iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82266

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Vehicle Access System Using UWB and Key Fob

Sahaj Sisodiya, Saniya Sheikh, Shubha P L, Sanjana H N
UG Student, Dept. of Electronics and Communication Engineering, Vemana Institute of Technology, Bengaluru, India

Abstract: ***This paper presents a comprehensive analysis of Vehicle Access Systems based on Ultra-Wideband (UWB) technology integrated with secure digital key fobs. With the rapid advancement of intelligent transportation systems and connected vehicles, the demand for highly secure, reliable, and user-friendly vehicle access mechanisms has significantly increased. Conventional Remote Keyless Entry (RKE) systems, which primarily rely on radio frequency communication, are increasingly susceptible to security threats such as relay attacks, signal interception, and spoofing techniques, thereby compromising vehicle safety and user privacy. To address these limitations, UWB-based vehicle access systems have emerged as an advanced solution capable of providing precise distance estimation and robust authentication between the vehicle and the authorized key fob. By utilizing time-of-flight (ToF) measurements and secure ranging techniques, UWB technology enables accurate localization and ensures that access is granted only when the authenticated user is physically present within a defined proximity. This significantly enhances protection against unauthorized access while simultaneously improving operational convenience for users.***

The paper discusses the overall architecture and operational workflow of UWB-enabled vehicle access systems, including communication protocols, authentication procedures, ranging mechanisms, and system integration. Furthermore, it examines the technical implementation aspects, performance advantages, security enhancements, and practical challenges associated with deploying UWB technology in modern automotive applications. The study also highlights emerging developments and future research directions, emphasizing the role of UWB in shaping next-generation secure and intelligent vehicle access solutions.

I. INTRODUCTION

Vehicle security and access control technologies have undergone substantial transformation over the past few decades, evolving from conventional mechanical locking systems to sophisticated wireless and intelligent authentication mechanisms. The increasing adoption of smart vehicles and connected automotive systems has created a growing demand for secure, efficient, and user-friendly vehicle access solutions. Traditional mechanical keys, although simple in operation, offer limited convenience and are vulnerable to physical theft or duplication.

To overcome these limitations, manufacturers introduced Remote Keyless Entry (RKE) systems, enabling users to lock, unlock, and start vehicles wirelessly through radio frequency (RF) communication.

Despite their convenience, conventional RF-based keyless entry systems face several security challenges. Attack techniques such as relay attacks, signal amplification, spoofing, and replay attacks can exploit the communication between the vehicle and the key fob, allowing unauthorized individuals to gain access without physically possessing the original key. Furthermore, traditional systems often lack precise localization capabilities, making it difficult to accurately verify the physical proximity of the authorized user.

Ultra-Wideband (UWB) technology has emerged as a promising solution to address these security and accuracy limitations. UWB is a short-range wireless communication technology that utilizes low-power pulse transmission over a wide frequency spectrum, enabling highly accurate distance measurement and real-time localization. Unlike conventional RF systems, UWB technology can provide centimeter-level positioning accuracy through precise time-based ranging techniques, significantly improving the reliability and security of vehicle access systems. In a UWB-based vehicle access system, secure communication is established between the vehicle and the authorized key fob through encrypted pulse exchanges. By calculating the time-of-flight (ToF) of transmitted signals, the system accurately determines the distance between the vehicle and the key fob. Access to the vehicle is granted only when the authenticated key fob is detected within a predefined secure range, thereby minimizing the risk of unauthorized access and relay-based attacks. In addition to enhanced security, UWB technology also improves user convenience by enabling seamless passive entry and ignition functionalities.

This study focuses on the architecture, communication mechanisms, operational principles, implementation techniques, advantages, and challenges associated with UWB-enabled vehicle access systems. The paper further explores the future potential of UWB technology in next-generation intelligent and autonomous automotive security applications.

A. Objectives

1) To understand the fundamental working principles of Ultra-Wideband (UWB) communication technology and its application in modern vehicle access systems.
2) To examine the architecture and operational design of vehicle access systems that utilize secure digital key fobs for authentication and access control.
3) To analyze the secure ranging, distance estimation, and encryption-based authentication mechanisms employed in UWB-enabled automotive systems to prevent unauthorized access.
4) To evaluate the performance, security, reliability, and efficiency of UWB-based vehicle access systems in comparison with conventional Radio Frequency (RF)-based keyless entry technologies.
5) To investigate the advantages of UWB technology, including precise localization, enhanced anti-relay protection, and improved user convenience in intelligent transportation environments.
6) To explore potential future advancements, emerging trends, and broader automotive applications of UWB technology in connected, autonomous, and smart vehicle ecosystems.

II. LITERATURE SURVEY

Recent advancements in intelligent automotive security systems have led to significant research and industrial adoption of Ultra-Wideband (UWB) technology for secure vehicle access applications. Several automotive manufacturers, technology companies, and research organizations have investigated the integration of UWB communication to enhance vehicle security, improve localization accuracy, and provide seamless user access experiences.

Major technology companies such as Apple and Samsung have introduced advanced digital car key frameworks that combine UWB technology with Bluetooth Low Energy (BLE) communication. These frameworks enable smartphones and smart devices to function as secure digital vehicle keys while supporting precise proximity detection and encrypted authentication. The integration of UWB with BLE enhances both connectivity efficiency and secure ranging performance, thereby reducing the possibility of unauthorized access through relay-based attacks.

In the automotive industry, leading manufacturers including BMW, Volkswagen, and Mercedes-Benz have actively incorporated UWB modules into premium and next-generation vehicles. These implementations focus on enabling secure passive entry systems, intelligent authentication, and location-aware vehicle interaction. The adoption of UWB technology in commercial automotive platforms demonstrates its growing importance in modern vehicle security infrastructures.

Several research studies and technical investigations have highlighted the advantages of UWB-based access systems over conventional Radio Frequency (RF)-based keyless entry solutions. Existing literature indicates that UWB technology offers centimeter-level localization accuracy through precise time-of- flight (ToF) measurements and secure ranging mechanisms. Researchers have also demonstrated that UWB systems are significantly more resistant to relay attacks, signal spoofing, and replay attacks due to their accurate distance verification capabilities and encrypted communication protocols.

Furthermore, academic studies emphasize that UWB technology contributes to improved operational reliability, reduced false authentication events, and enhanced user convenience in smart transportation environments. Researchers continue to explore advanced algorithms, hybrid communication models, and low-power implementations to further optimize the performance and scalability of UWB-enabled automotive access systems. The findings from existing literature confirm that UWB technology represents a promising and effective solution for next-generation secure vehicle access and intelligent mobility applications.

III. METHODOLOGY

A. Ultra-Wideband (UWB)

Ultra-Wideband (UWB) is an advanced short-range wireless communication technology that transmits information using extremely low-power pulses distributed across a wide frequency spectrum. Unlike conventional narrowband communication systems that operate within limited bandwidth ranges, UWB utilizes very short-duration pulses, enabling highly accurate time-based measurements and secure wireless communication. The wide bandwidth characteristics of UWB significantly improve localization precision, reduce interference, and enhance resistance to signal spoofing and relay attacks.

One of the most important features of UWB technology is its ability to perform precise Time-of-Flight (ToF) measurements, which enable centimeter-level distance estimation between communicating devices. In vehicle access systems, this capability allows the system to accurately determine the physical proximity of the authorized key fob relative to the vehicle, thereby enhancing both security and operational reliability.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

B. Key Fob Operation

The proposed vehicle access system utilizes a smart key fob integrated with multiple hardware components, including a UWB transceiver, microcontroller unit (MCU), antenna module, secure cryptographic element, and battery management circuitry. These components collectively enable secure communication, signal processing, authentication, and low-power operation.

When the authorized user approaches the vehicle, the vehicle control unit periodically initiates encrypted ranging requests through UWB communication. Upon receiving the request, the key fob generates a secure authentication response containing encrypted ranging information. The bidirectional communication process allows the vehicle system to verify the legitimacy of the key fob while simultaneously estimating the exact distance between the user and the vehicle.

If the calculated distance falls within a predefined secure threshold range, the vehicle grants access to authorized functions such as door unlocking, passive entry, and engine ignition. Otherwise, access is denied to prevent unauthorized entry attempts.

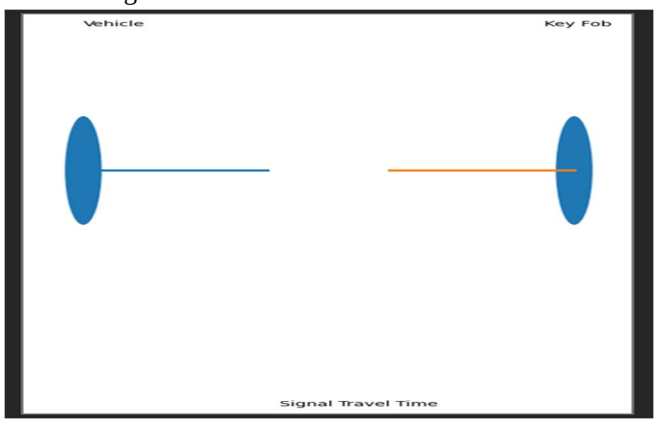
C. Distance Measurement Using Time-of- Flight (ToF)

The distance estimation process in the proposed system is based on the Time-of-Flight (ToF) principle. In this method, the system measures the time required for UWB radio pulses to travel between the vehicle and the key fob. Since electromagnetic waves propagate at approximately the speed of light, the travel time can be used to calculate the precise physical distance between the communicating devices.

The distance is determined using the following mathematical expression:

$$\text{Distance} = \frac{\text{Speed of Light} \times \text{Time Delay}}{2}$$

The division by two accounts for the round-trip travel time of the transmitted and received UWB signals. This precise ranging mechanism enables the system to accurately authenticate user proximity and significantly reduces vulnerabilities associated with conventional RF-based vehicle access technologies.



IV. RESULT

The proposed Ultra-Wideband (UWB)-based Vehicle Access System was successfully implemented and tested using a hardware prototype consisting of DWM1000 UWB modules, ESP32 microcontrollers, CAN bus communication interfaces, LEDs for status indication, and supporting circuitry assembled on a breadboard platform. The experimental setup was designed to demonstrate secure two-way ranging, authentication, and communication between the vehicle unit and the authorized digital key fob.

The developed system establishes communication between the UWB-based DWM1000 modules and the CAN bus network through the ESP32 controller. The ESP32 acts as the central processing and communication unit, handling signal interpretation, ranging operations, authentication processing, and LED-based status indication. The prototype validates the ability of the system to securely exchange ranging information and determine the proximity of the authorized user before granting vehicle access.

A. Prototype Implementation

The hardware implementation consists of the following major components:

1) DWM1000 UWB modules for secure ranging and distance estimation
2) ESP32 microcontroller for communication control and processing

3) CAN bus interface for vehicle communication simulation
4) LED indicators for real-time system status monitoring
5) Breadboard-based experimental circuitry for prototype testing

The system performs secure two-way ranging between two DWM1000 modules. When communication is initiated, encrypted ranging signals are exchanged between the transmitter and receiver units to verify proximity and authenticate the authorized key fob. Based on the ranging result and authentication status, the ESP32 controller activates different LEDs to visually indicate the current operational state of the system.

B. *LED Status Indication*

The implemented prototype uses multiple LED indicators to represent different states of the vehicle access system:

1) Red LED – Locked State: Indicates that the vehicle remains in a secure locked condition due to failed authentication, absence of an authorized key fob, or invalid ranging results.
2) White LED – Unlock State: Indicates successful authentication and secure proximity verification. The system grants vehicle access only when the authorized key fob is detected within the predefined secure range.
3) Blue LED – Waiting/Connection State: Represents the initialization and synchronization phase where the system waits for successful two-way ranging communication between both DWM1000 modules.

The LED-based monitoring mechanism provides a simple and effective method for observing real-time communication and authentication status during experimental testing.

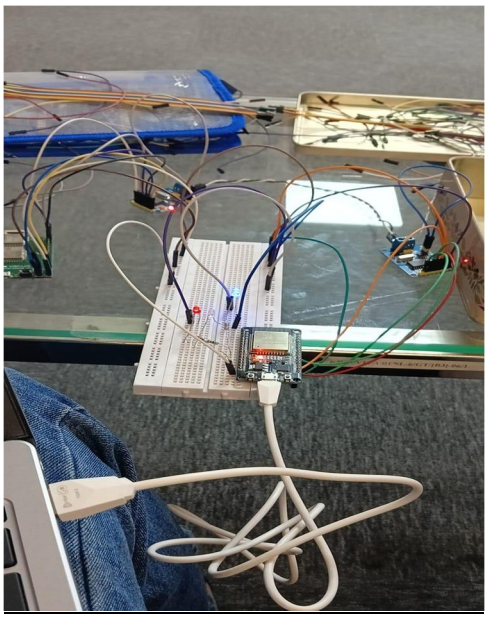
C. *Experimental Observation*

During testing, the system successfully established secure communication between the DWM1000 modules and accurately detected proximity using UWB-based ranging techniques. The CAN bus interface enabled efficient communication between the ESP32 controller and the simulated vehicle network environment. The prototype demonstrated stable operation with reliable state transitions between locked, waiting, and unlocked conditions.

The experimental results confirm that UWB technology provides accurate ranging performance and secure authentication capabilities suitable for next-generation automotive access systems. Compared to traditional RF-based systems, the implemented prototype exhibited improved resistance to unauthorized access attempts due to its precise distance verification mechanism.

Furthermore, the integration of UWB communication with CAN bus architecture demonstrates the feasibility of deploying such systems within modern intelligent vehicle platforms. The prototype validates the practical implementation of secure passive entry systems using low-power wireless communication and embedded automotive networking technologies.

D. *Performance Analysis*



The developed system achieved the following functional outcomes:

1) Successful two-way ranging communication between DWM1000 modules
2) Reliable LED-based status indication for system monitoring
3) Secure authentication using proximity-based verification
4) Stable CAN bus and ESP32 integration
5) Improved localization accuracy compared to traditional RF systems
6) Enhanced resistance against relay attack scenarios

The results demonstrate that UWB-based vehicle access systems can significantly improve automotive security, operational reliability, and user convenience in intelligent transportation applications.

V. FUTURESCOPE

The future of vehicle access systems is expected to be significantly influenced by the integration of Ultra-Wideband (UWB) technology with emerging intelligent and secure digital technologies. As the automotive industry continues to move toward connected, autonomous, and software-defined vehicles, UWB-based access systems are likely to evolve into more advanced, adaptive, and highly secure authentication platforms.

One of the major future developments involves the integration of UWB technology with Artificial Intelligence (AI). AI-driven algorithms can enhance localization accuracy, predict user behavior, and optimize secure access decisions based on environmental conditions and movement patterns. Intelligent access systems may automatically recognize authorized users, adjust vehicle settings according to user preferences, and improve overall operational efficiency through real-time data analysis.

Biometric authentication mechanisms such as facial recognition, fingerprint scanning, voice recognition, and behavioral authentication are also expected to be integrated with UWB-enabled vehicle access systems. Combining biometric verification with precise UWB ranging can provide multi-layered security, significantly reducing the possibility of unauthorized access and identity spoofing attacks.

Another promising advancement is the implementation of blockchain-based authentication frameworks for secure digital key management. Blockchain technology can provide decentralized and tamper-resistant storage of authentication credentials, enabling secure sharing, revocation, and management of digital vehicle keys without compromising user privacy or system integrity.

Smartphone-based digital key systems are anticipated to become a standard feature in next-generation vehicles. By integrating UWB, Bluetooth Low Energy (BLE), and Near Field Communication (NFC), smartphones and wearable devices can function as fully secure digital keys, eliminating the need for traditional physical key fobs. This advancement will improve convenience, remote accessibility, and seamless interaction between users and vehicles.

Furthermore, UWB technology is expected to play a critical role in autonomous vehicles and intelligent transportation systems (ITS). Its high-precision localization and secure communication capabilities can support vehicle-to-vehicle (V2V) communication, automated parking systems, collision avoidance mechanisms, and smart mobility infrastructure. As research and development continue, UWB-based systems are likely to become a fundamental component of future intelligent automotive ecosystems, offering enhanced security, automation, and user-centric mobility solutions.

VI. CONCLUSION

Vehicle access systems based on Ultra-Wideband (UWB) technology and secure digital key fobs represent a significant advancement in modern automotive security, authentication, and user convenience. The integration of UWB technology into vehicle access mechanisms addresses many of the limitations associated with conventional Radio Frequency (RF)-based keyless entry systems, particularly vulnerabilities related to relay attacks, signal spoofing, and inaccurate proximity detection.

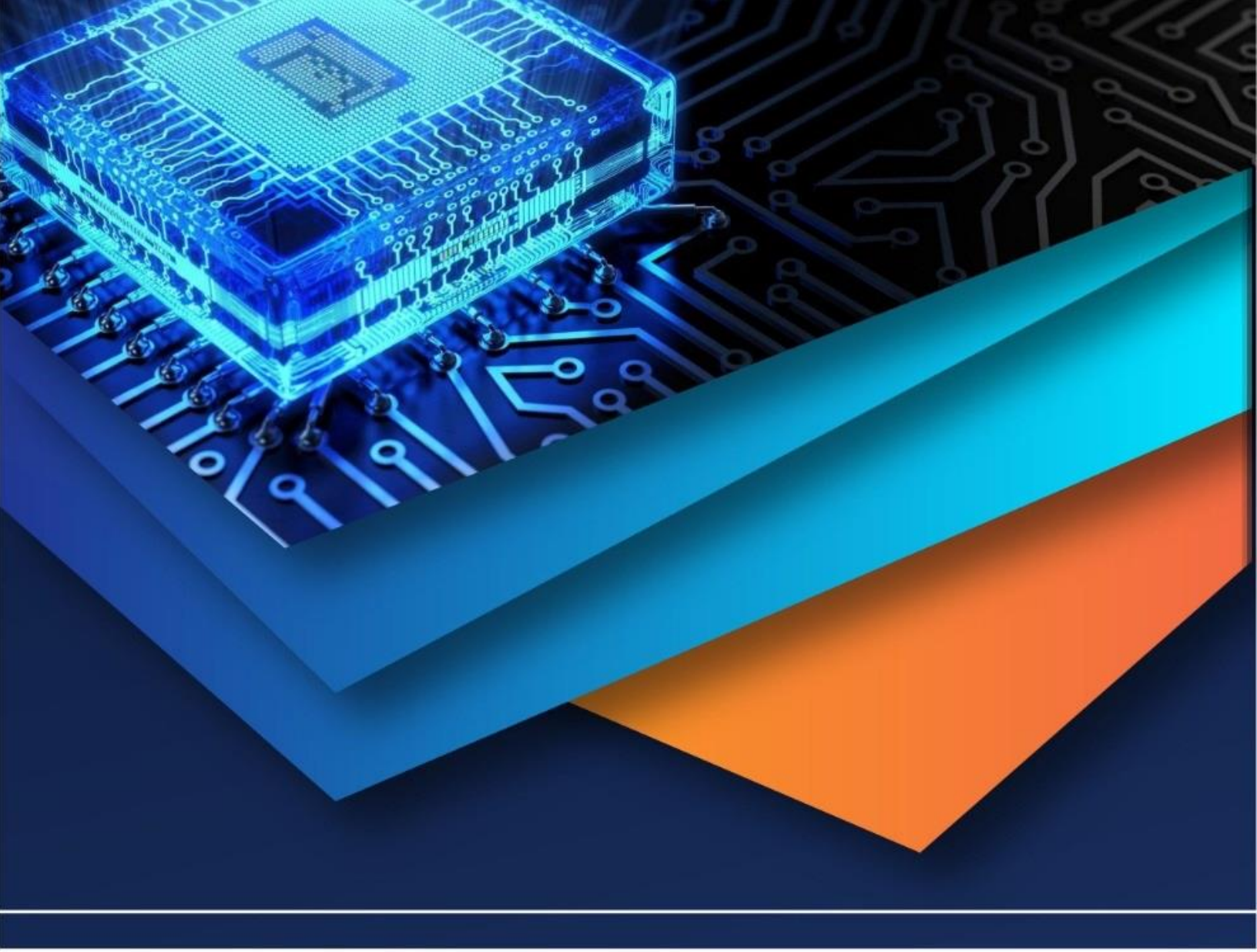
By utilizing precise ranging techniques and Time-of-Flight (ToF) measurements, UWB technology enables highly accurate localization and secure communication between the vehicle and the authorized key fob. This ensures that vehicle access is granted only when the authenticated user is physically present within a predefined secure range, thereby substantially improving protection against unauthorized access attempts. In addition to enhanced security, UWB-based systems provide seamless passive entry functionality, faster authentication, and improved user experience in smart automotive environments.

The study demonstrates that UWB technology offers superior reliability, localization accuracy, and operational efficiency when compared to traditional RF-based vehicle access solutions. Furthermore, the growing adoption of UWB by leading automotive manufacturers highlights its increasing importance in the development of next-generation intelligent transportation systems.

As the automotive industry continues to evolve toward connected, autonomous, and software-defined vehicles, UWB-enabled secure access systems are expected to become a standard component of future vehicle architectures. The integration of UWB with emerging technologies such as Artificial Intelligence (AI), biometrics, digital smartphones, and intelligent mobility platforms will further enhance vehicle security, automation, and user-centric functionality. Consequently, UWB technology holds strong potential to shape the future of secure and intelligent automotive access systems**.**

REFERENCES

[1] "Vehicle Positioning Based on UWB Technology," Journal of Physics: Conference Series, vol. 1827, no. 1, 2021.
[2] "CAN Protocol Based Vehicle Monitoring System," International Advanced Research Journal in Science, Engineering and Technology (IARJSET), vol. 11, no. 4, 2024.
[3] "Mitigating Relay Attacks in Vehicle Access Systems Using BLE and UWB," Engineering, Technology & Applied Science Research (ETASR), vol. 15, no. 1, 2025.
[4] "Bluetooth Based Smart Vehicle Access System," International Research Journal of Engineering and Technology (IRJET), vol. 8, no. 6, 2021.
[5] IEEE, "IEEE Standard for Low-Rate Wireless Networks," IEEE Std 802.15.4 UWB Communication Standard, 2020.
[6] M. Z. Win and R. A. Scholtz, "Ultra-Wide Bandwidth Time-Hopping Spread-Spectrum Impulse Radio for Wireless Multiple-Access Communications," IEEE Transactions on Communications, vol. 48, no. 4, pp. 679–689, 2000.
[7] D. Dardari, A. Conti, U. Ferner, A. Giorgetti, and M. Z. Win, "Ranging With Ultra-Wide Bandwidth Signals in Multipath Environments," Proceedings of the IEEE, vol. 97, no. 2, pp. 404–426, 2009.
[8] F. Zafari, A. Gkelias, and K. K. Leung, "A Survey of Indoor Localization Systems and Technologies," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2568–2599, 2019.
[9] J. Decawave, "DWM1000 Ultra-Wideband Transceiver Module Datasheet," Decawave Technical Documentation, 2020.
[10] Bosch Automotive Electronics, "CAN Bus Communication Protocol for Intelligent Automotive Systems," Bosch Technical White Paper, 2019.
[11] Espressif Systems, "ESP32 Series Microcontroller Technical Reference Manual," Espressif Documentation, 2023.
[12] S. Brands and D. Chaum, "Distance-Bounding Protocols," in Workshop on the Theory and Application of Cryptographic Techniques, Springer, pp. 344–359, 1993.
[13] A. Alkhateeb and G. Leus, "Secure Localization and Authentication in UWB-Based Systems," International Journal of Wireless Information Networks, vol. 27, no. 1, pp. 45–57, 2020.
[14] Apple, "Digital Car Key Security Using Ultra-Wideband Technology," Apple Developer Documentation, 2023.
[15] Samsung, "Secure Smartphone-Based Vehicle Access Using UWB and BLE," Samsung Research Publications, 2022.
[16] BMW, "Ultra-Wideband Technology for Secure Passive Vehicle Entry Systems," BMW Technical Report, 2021.
[17] "Secure Smart Key System Using Ultra-Wideband Communication," International Journal of Automotive Technology, vol. 23, no. 5, pp. 1152–1163, 2022.
[18] "Relay Attack Prevention in Keyless Vehicle Entry Systems Using Distance Bounding," IEEE Access, vol. 9, pp. 102345–102357, 2021.
[19] "Implementation of UWB-Based Localization for Intelligent Transportation Systems," International Conference on Smart Mobility and Communication Technologies, 2023.
[20] "Advanced Vehicle Access Control Using Embedded Systems and CAN Communication," International Journal of Engineering Research and Applications (IJERA), vol. 12, no. 2, pp. 55–61, 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY