Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 2, pp. 751–759, DOI 10.12694/scpe.v25i2.2521

INTERFACE CONTROL AND STATUS MONITORING OF ELECTRONIC INFORMATION EQUIPMENT BASED ON NONLINEAR DATA ENCRYPTION

MIN YAN* AND HUA ZHANG†

Abstract. An advanced electronic information equipment interface control and status monitoring system is proposed to ensure the fairness, objectivity, and security of information while identifying responsibility for traffic accidents. Through an in-depth analysis of the system's security requirements and the current landscape of information security technology, a robust security strategy is developed for each crucial system stage. A PC-based platform is developed for efficient data acquisition, secure processing, reliable transmission, and fortified storage, focusing on implementing nonlinear data encryption methods. Performance evaluation of the system involved rigorous testing using files ranging from 3MB to 10MB. The results of the proposed system revealed a significant improvement in the system's overall speed and efficiency, showcasing an average performance enhancement of one quarter compared to the original platform. The proposed system demonstrated an impressive 15% to 30% increase in processing speed, establishing its capability to ensure data integrity protection during information transmission, facilitate accurate identification of data recording equipment post-accident, and safeguard the security of stored data. The developed electronic information equipment interface control and status monitoring system effectively addresses critical challenges associated with ensuring data integrity and security in traffic accident investigations.

Key words: Traffic accidents; Data encryption; Information security; Fairness; Objectivity

1. Introduction. In the current era of rapid economic growth, the exchange of information has become increasingly crucial. However, certain factors, such as the propagation of connecting cables and space saturation, significant challenges to efficient information transmission. To tackle these issues, scientists have developed various short-range wireless communication technologies. These technologies involve communication distances of less than 200 meters and employ radio technology for data transmission among different devices. Notable examples of such technologies include Bluetooth, Wireless Fidelity (WiFi), IrDA, UWB, Near Field Communication (NFC), ZigBee, WLAN, Ad Hoc, WMN, and ANT, each occupying distinct wireless frequency bands and offering unique performance, technical advantages, and application environments [123].

The significant advancements in Bluetooth's technical specifications, particularly with the release of the Bluetooth 4.0 specification in 2010, the competitiveness of Bluetooth products in the market has surged, leading to an expanding scope of applications. Statistical data indicates a rapid upsurge in the production of Bluetooth technology products since 2007, with global sales surpassing 1 billion units in 2008, reaching 1.6 billion units in 2011, and nearly 2 billion units in 2012. According to ABI's market tracking report on the Internet of Everything (IoE) in the second quarter of 2015 (MD-IOE-104), the worldwide count of Internet of Things interconnection devices is projected to exceed 45 billion by 2020, with at least 14 billion of these devices utilizing Bluetooth specifications. Bluetooth technology products are anticipated to account for at least one-third of Internet of Things interconnection devices by 2020. The widespread application and integration of Bluetooth products within the increasing Internet of Things landscape have made them ubiquitous in everyday life [456].

Despite being the primary wireless communication technology acknowledged by the industry, concerns regarding the security of Bluetooth technology have persistently echoed throughout the external sphere and the extensive user community. With the continuous evolution of network technology and the substantial enhancement of computer processing capabilities, Bluetooth's conventional encryption algorithm mode has become inadequate to meet the security demands of the contemporary application landscape. Presently, the utilization of Bluetooth applications has witnessed consistent spread. Notably, not only traditional sectors such as medical, commercial, financial, defense technology, aerospace, and the military, characterized by high information value and stringent

*XinXiang Vocational and Technical College, School of Information Engineering, 453006, China (minyan298@163.com)
†Xinxiang Vocational and Technical College, Xinxiang, Henan, 453621, China (huazhang58@126.com)

security prerequisites, impose fresh security requisites on Bluetooth, but also various mass industries, including the automotive sector, security, automated control, environmental monitoring, smart home technology, urban management, modern architecture, and the Internet of Things, have thrust Bluetooth security concerns to the forefront. Consequently, Bluetooth technology's current data security performance is causing significant apprehension [7, 8].

2. Literature review. In 1994, Ericsson's mobile communication department pioneered developing a cost-effective and energy-efficient wireless technology to facilitate the connectivity between mobile phones and nearby devices, eventually named Bluetooth. Subsequently, in February 1998, Ericsson, in collaboration with IT industry leaders including Intel, KM, Nokia, and Toshiba, established the "Bluetooth Special Interest Group" (Bluetooth SIG), formally solidifying its presence in the technological landscape. The consortium welcomed the participation of additional technology giants such as 3Com, Microsoft, Motorola, and Lucent, who joined the ranks of Bluetooth SIG as active proponents [9].

On July 26, 1999, Bluetooth SIG introduced Bluetooth specification 1.0, marking a significant milestone in the evolution of the technology. This was followed by the release of Bluetooth Specification 2.0 in November 2004, which proposed the Enhanced Data Rate (EDR) transmission mode. The latest Bluetooth specification, 3.0, was unveiled on April 21, 2009, incorporating the high-speed transmission mode, boasting a maximum 24 Mbps [10].

The concept of low-power Bluetooth, originally conceptualized by the Nokia Research Center, began its developmental journey in 2001 and was officially launched in October 2006 under the name Wi-Bree. Initially targeted at applications in personal medical and security domains due to its exceptional low-power Design and compatibility with traditional Bluetooth, Wi-Bree exhibited strong market potential in the medical and safety sectors. Consequently, the Wi-Bree Forum announced its incorporation into the Bluetooth Special Interest Group (SIG) on June 12, 2007, leading to its renaming as Ultra Low Power (ULP) Bluetooth [11].

In mid-2008, ULP was rebranded as Bluetooth Low Energy, with plans to introduce low-power Bluetooth specification products in mid-2009. Subsequent advancements led to the official launch of Bluetooth Specification 4.0 by the Bluetooth Special Interest Group on June 30, 2010, combining traditional, high-speed, and low-power Bluetooth capabilities, propelling Bluetooth technology to a new level. The Bluetooth Technology Alliance continued this trajectory with the introduction of the Bluetooth 5.0 specification on June 16, 2016, announcing substantial enhancements in transmission distance, speed, and data capacity, thereby setting the stage for a new generation of Bluetooth standards from the end of 2016 to the beginning of 2017 [12].

The author's primary focus centres on conducting an in-depth analysis of the system's security prerequisites and proposing comprehensive security measures for each system component, closely integrating insights from information security technology. Emphasizing the system design's pivotal aspects and pragmatic aspects, the author has developed a PC-centered platform dedicated to data gathering, secure processing, continuous transmission, and reliable storage. This platform validates the establishment of communication channels and the effectiveness of the data protection processes [13].

3. Research Methods.

3.1. Safety Demand Analysis. The primary risk to the secure transmission of data within the system during the data processing phase arises from potential transmission failures or wireless interferences during the data transfer between the front-end acquisition unit and the central unit. These challenges concerning data integrity, timely delivery, and the security of Bluetooth wireless connectivity. Furthermore, ensuring storage security involves verifying the freshness and integrity of data upon its arrival at the central unit. The goal is to guarantee the authenticity of device identity and data integrity, thus necessitating implementing the proposed storage process security measures. The safety structure diagram showing the data processing process within the system is presented in Figure 3.1 [14].

The fundamental security of the system is chiefly responsible for safeguarding the integrity and protection of the system's software and hardware elements, alongside the associated technologies utilized in their creation and operation. This entails implementing robust strategies to reinforce the inherent defenses of the system against potential vulnerabilities and threats. Notably, it emphasizes the deployment of dependable protocols and mechanisms to strengthen the system's flexibility against unauthorized access and breaches.

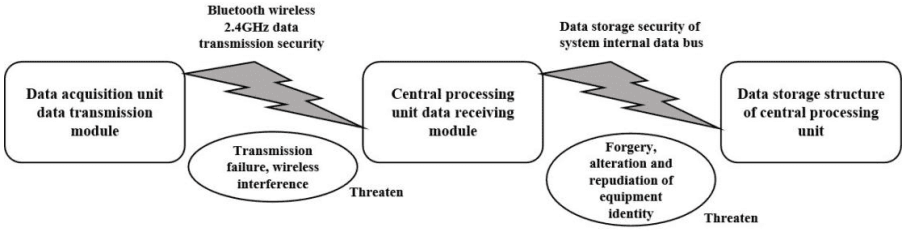

Fig. 3.1: Safety structure of system data process

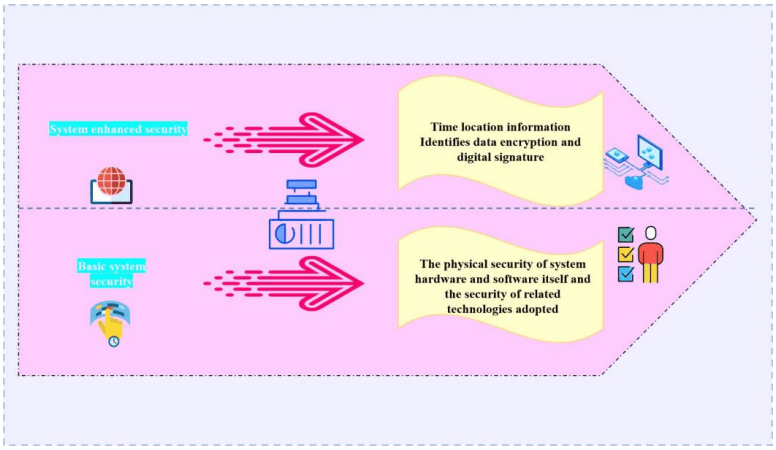

Fig. 3.2: Schematic of system security

Conversely, the heightened security dimension of the system primarily revolves around the meticulous management of data, incorporating sophisticated information security protocols and cryptographic methodologies to establish an additional layer of defense. The system uses sophisticated cryptographic techniques to encrypt and decrypt sensitive data, reinforcing its capacity to resist potential cyber threats and unauthorized breaches.

The system's security framework, encompassing both the foundational and advanced security layers, is concisely represented in Figure 3.2. This visual representation underscores the comprehensive structure of the system's security architecture, highlighting the pivotal interplay between foundational security measures and state-of-the-art technical procedures for ensuring robust data protection and overall system integrity.

3.2. System security design and implementation.

3.2.1. Data integrity design and implementation. Within this system, the preservation of data integrity pertains to the seamless transmission of data from the front-end unit to the back-end unit via Bluetooth communication. Additionally, it ensures the perpetual authenticity of the recorded information before and after the back-end unit ultimately stores the data. This entails guaranteeing that the data remains unaltered throughout these two critical data transmission and storage stages [15].

In the area of cryptography, the concept of the hash function is intricately intertwined with safeguarding data integrity. Typically employed to generate concise data "fingerprints," the hash function aids in distinguishing data through its distinctive characteristics. Notably, any alterations to the data trigger corresponding changes in its associated "fingerprint." Consequently, in cases where data integrity is potentially compromised during transmission or storage, data integrity verification can be facilitated by recomputing the data's fingerprint and cross-verifying it against the original data fingerprint. This process effectively ensures the continual authenticity of the data [16].

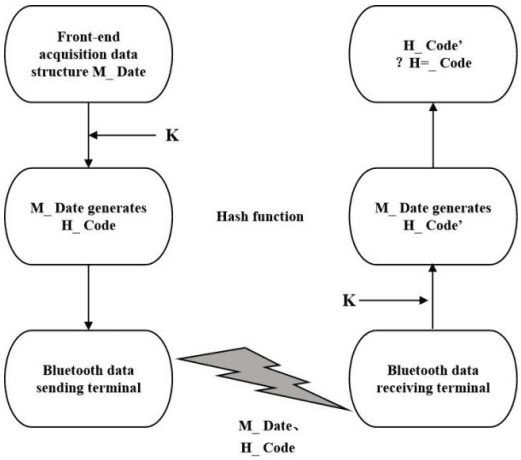

Fig. 3.3: Process for Ensuring Data Integrity

Let's consider the data structure M_Image, which encompasses both temporal and spatial information stored within the system. The hash function, denoted as H, is employed in the context of the security mechanism implemented within the front-end unit. Notably, the processor within the front-end unit undertakes the hashing operation, as depicted in the following Equation 3.1.

$$H\_Code = H(M\_Image) \tag{3.1}$$

Consequently, the resultant output is the fingerprint of the recorded data, often referred to as the message digest of the data. Subsequently, during the transmission of the data structure package within the system via Bluetooth or upon the data's entry into memory through the system bus, it becomes necessary to re-execute the hashing operation exclusively at the receiving end of the transmission channel or when retrieving the data structure from memory. This operation is demonstrated as follows:

$$H\_Code' = H(M\_Image) \tag{3.2}$$

This results in the new condensed message representation of the data. Comparing H_Code and H_Code' for equality signifies the data's integrity. It is crucial to note that this determination relies significantly on the security attributes of the hash function. Moreover, given the embedded nature of the system components and the inherent constraints on data transmission and processing capacity, adopting a relatively uncomplicated and convenient hash function is imperative.

Specifically, the hash functions can be categorized into those without keys and those with keys. In cases where hash functions without keys are utilized, it is essential to ensure the secure storage or transmission of the message digest (H_Code). Consequently, a hash function with a key to generate the condensed message summary is recommended. The outlined process is as follows:

(1) H_Code=H(M_Image) and H_Code'=H(M_Image)

(2) H_Code?=HCode

Here, K represents the key of the HMAC function. In the practical data communication framework of the system, K functions as a provisional key solely dedicated to upholding the integrity of data transmission. Its primary objective is to secure the successful exchange of validation data between the front-end and back-end through the HMAC function. Consequently, the session key can be designated for both communicating parties during data transmission. It is crucial to securely store K within the system, ensuring its confidentiality and safeguarding its integrity. Figure 3.3 illustrates the design process for data integrity protection [17].

Within the data integrity mechanism framework, if the newly computed message digest differs from the initial message digest dispatched by the front-end unit, the system will discard the data. To ensure data integrity, the system utilizes a retransmission strategy to compensate for any discarded data.

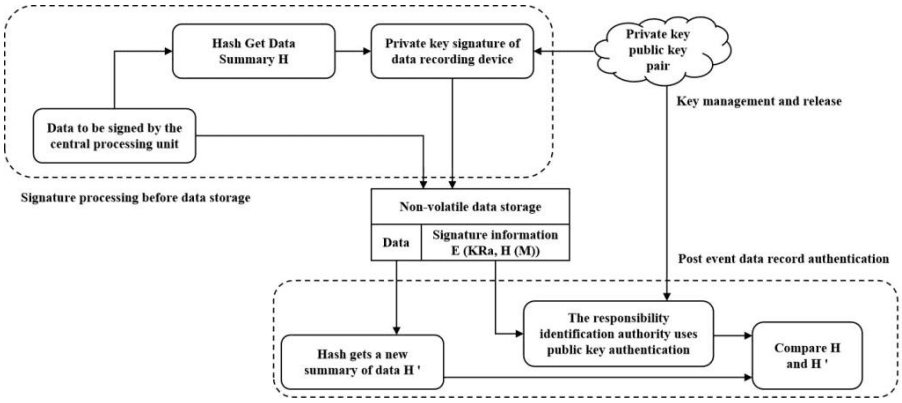

Fig. 3.4: Model for Implementing Digital Signatures using Public Key Cryptosystems

3.2.2. Design and implementation of non-repudiation of data records. Non-repudiation prevents the originator of a message from disowning the disseminated or transmitted message. In the system context, the vehicle monitoring data pertains to the information captured by the onboard equipment installed within the vehicle. As this data constitutes authentic records of the accident scene, it may contain information not in favour of certain parties. Consequently, to uphold the principle of impartiality, when the "evidence" is subsequently presented to the accident responsibility adjudication authority, the authority must verify the identity of the data recorder, i.e., the vehicle equipped with the monitoring system, and ascertain the origin of the evidence data. This verification is essential to prevent any evasion of unfavourable records. The non-repudiation mechanism within the system ensures the accountability of the data recorder and the data, thereby safeguarding the integrity and reliability of the entire process.

More specifically, the system's data security protection entails ensuring the security of the data both before and after storage. This comprehensive security measure is augmented by implementing a sophisticated digital signature scheme, representing an advanced level of protection within the system.

The data information the system captures incorporates the timestamp associated with the data recording process. In this context, verifying the consistency between the data generation time and the time of the recorded events is instrumental in ensuring the data's current state. However, this verification guarantees the data's chronological accuracy and does not provide comprehensive assurance of its authenticity. The system must employ a digital signature mechanism to guarantee non-repudiation of the data's origin [18].

In the system, attaining non-repudiation through digital signature for data relies on applying public key cryptography as an encryption algorithm. This technique employs a pair of keys, where one key is used for encryption, and another distinct yet related key is employed for decryption. Its notable advantage lies in the computational infeasibility of determining the decryption key solely based on knowledge of the encryption algorithm and key. When the public key encryption is utilized for digital signatures, the private key is initially employed for encryption, a process known as signing. To enhance efficiency, it may process either a segment of the message or the message summary.

As previously discussed, following the wireless transmission of data via Bluetooth and its verification for integrity, the data is stored in the temporary memory of the central control and data centralized processing unit. Before direct storage, the original data, which is currently devoid of any association with the recorder's identity, requires further security processing. The message digest of the original data, generated during the integrity verification, serves as the security hash code output by the corresponding data hash function. In this scenario, the system's private key encrypts this hash code to create a signature. Consequently, the recorded data concerning vehicle accidents and the accompanying signed information are stored in the non-volatile memory of the central control and data centralized processing unit. Concurrently, the system's signature represents the public key generated with the private key and disseminated through alternative channels such as the Public Key Infrastructure (PKI) system [19].

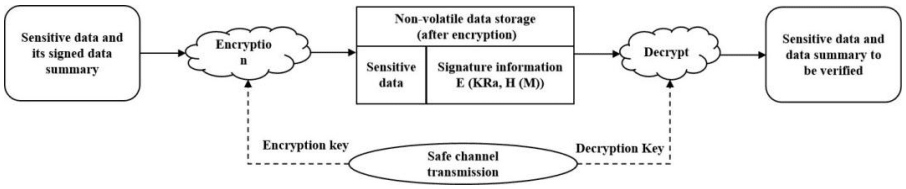

Fig. 3.5: Schematic diagram of data confidentiality processing

When the system's data necessitates submission to the certification authority for verification, the certifying entity extracts "evidence" data from the system's non-volatile storage. It validates it using the data record claimant's public key. This process verifies the authenticity and validity of the data recorder's identity, thereby facilitating the objective of responsibility identification. Figure 3.4 illustrates the schematic diagram of the implementation model, demonstrating the application of public key cryptography as a digital signature within the system. To verify the identity of the digital signature to the data recording device, here we use the RSA algorithm based on the mathematical problem of large prime number decomposition.

3.2.3. Data confidentiality requirements. Based on the preceding examination of the system's security requisites, it is evident that the comprehensive security framework for monitoring vehicle operation and accident data primarily emphasizes the integrity of wireless data transmission and the authentication of the data storage device. Typically, the data stored within the system is either inaccessible under normal circumstances or possesses minimal confidentiality demands. However, considering potential functional expansions, sensitive data such as GPS coordinates can be subjected to encryption.

In practice, the information logged by the onboard system doesn't require confidentiality measures for external parties. Even if the data is intercepted, the integrity of the key data recording information and the originating equipment remains unchanged. Consequently, the data retains the authentic details of the involved parties and upholds its legal validity as "evidence" for the responsibility identification authority.

In light of this, we establish the system's data confidentiality requirement as an extended security mechanism. The fundamental implementation concept involves the nonlinear data encryption after the signing process before its storage. Conversely, before its use as "evidence," the data undergoes decryption to eliminate the confidentiality shield, followed by public key verification. This approach is depicted in Figure 3.5.

In the data security design, we employed the AES symmetric encryption system. While ensuring the system's security demands, we have considered the performance criteria on the embedded hardware platform. Encrypting specific, limited-sensitive data fulfils the security needs and alleviates the functional strain on the system.

4. Result analysis and Discussion.

4.1. Test platform for Bluetooth transmission and data security processing. Two key technological facets underpin the wireless Bluetooth vehicle safety monitoring system conceptualized by the project. Firstly, Bluetooth wireless data transmission's implementation and security technology facilitates data integrity protection, signature verification of data publishing devices, and encrypted storage of data message digests. To demonstrate the efficacy and practicality of these technologies within the system, the author has established a test environment on a PC platform, emphasizing Bluetooth wireless transmission and data security processing. This initiative has preliminarily actualized the research objectives and key technologies outlined in the system design.

To underscore the realization of Bluetooth communication and data security processing, the embedded control PC in the test platform has been substituted with a PC. The Bluetooth module is connected to COM1 and COM4, respectively. The software environment for the test platform has been compiled using Visual C++v6.0 and is executed accordingly. The two Bluetooth devices within the test platform adhere to the agreed-upon protocols for seamless communication.

Main equipment address: 00 80 38 14 3c CC COM1

Slave address: 00 80 38 14 3d 0f COM4

4.1.1. Test platform software. The testing software employs the Visual C++v6.0 serial port control, MSComm, to regulate the serial data communication interface. It effectively manages the Bluetooth module and facilitates data transmission via the HCI interface of the Bluetooth host.

4.1.2. Bluetooth communication function realization. Initialize the slave device (00 80 37 14 3d 0f): Select the function reset by chip, set the authentication enable, set the event filter, read the device address and query enable.

#define HCI_RESET "01 03 0C 00"
#define HCI_WRITE_AUTHENTICATION_ENABLE "01 20 0C 01 00"
#define HCI_SET_EVENT_FILTER "01 05 0C 03 02 00 02"
#define HCI_READ_BDADDR "01 09 10 00"
#define HCI_WRITE_SCAN_ENABLE "01 1A 0C 01 03"

Bluetooth module reply time grouping.

At this time, the slave device has entered the waiting query state.

Main device initialization (00 80 37 14 3c cc): select the function by chip reset, set authentication enable, set event filtering, read device address and search device in sequence.

#define HCI_RESET "01 03 0C 00"
#define HCI_WRITE_AUTHENTICATION_ENABLE "01 20 0C 01 00"
#define HCI_SETEVENT_FILTER "01 05 0C 03 02 00 02"
#define HCI_READ_BDADDR "01 09 1000"
#define HCI_INQUIRY "01 01 04 05 33 8B 9E 06 00"

Subsequently, the primary device yields the search outcomes, identifying a nearby Bluetooth device as the target slave device. Upon selecting the "create ACL link" function by the primary device, both the master and slave devices confirm the successful establishment of the link, denoted by the event group comprising the other device's address. The command structure for transmission is as follows: m_StrAddress represents the location of the Bluetooth device's address, specifically the slave device address.

HCI_CREATE_CONNECTION1+m_strAddress+HCI_CREATE_CONNECTION2

Following the successful establishment of the ACL, the master-slave device events are synchronized accordingly.

Post ACL link establishment, the transmission of data files becomes feasible. The sender showcases the time and location details of the file's record and transmits it to the receiving end. Concurrently, the HMAC function is utilized to compute the summary of the data file. The function for calculating the data file summary is as follows:

void CBluetoothDlg:Mac(CByteArray & data, CByteArray & mac)

Assuming the HMAC function key is: "01234567890123456789," the data file information slated for transmission aligns with the information obtained by the receiving end.

Based on this, we can deduce that the sequence of message digests computed by the identical hash function with the key remains consistent before and after the file transmission. This consistency serves as a verification of the file's integrity throughout the transmission process.

4.1.3. Implementation of digital signature and verification. This section primarily includes two key functions: data security processing and security verification, enabling private key signature, data encryption and decryption, and public key verification. Depending on specific test requirements, signature and encryption can be independently chosen.

The public key information is manually inputted for device verification during the test without a Public Key Infrastructure (PKI) system for providing public key release. Furthermore, to ensure the security of the signature private key, the USBeKey facilitates the private key signing in the RSA public key encryption algorithm.

The electronic key eKey is the "electronic key and ID card" within the client (i.e., the signatory). This USB-based product features a smart chip and a read-write controller, exhibiting a sleek design for convenient portability across various computers equipped with USB interfaces. It functions as a tool for digital signatures, identity authentication, secure information and data encryption, and the storage of personal certificates within a network environment. With a user storage space of 64K, it enables personal information, passwords, keys, certificates, and more storage. Additionally, it supports the RSA 1024-bit public key cryptography algorithm, allowing direct generation of RSA key pairs within the chip and facilitating functions such as signature/authentication and encryption/decryption. It provides an API dynamic library for streamlined programming.

Table 4.1: Comparison Results of Speed Test

File type	File size	Processing time(s)	
		Original platform	Author's text platform
MP3	3.10MB	7	7
EXE	6.35MB	13	9
ZIP	10MB	400	340

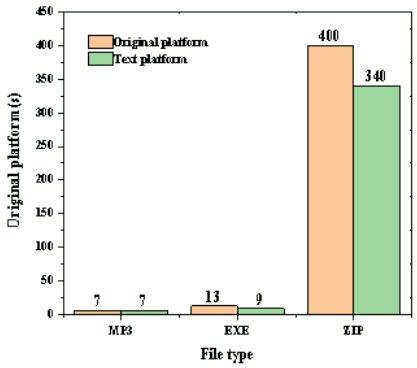

Fig. 4.1: Comparison of Processing Times between Original and Author's Platforms

During security processing, the initial step involves selecting the desired file for processing. If encryption is necessary, the encryption key must be entered. After selecting "Execute," the program prompts the user to store the file following security processing for verification purposes.

4.2. Speed test. Files within the range of 3MB to 10MB were chosen for testing purposes, and the outcomes of the tests are presented in Table 4.1 and Figure 4.1.

The Table 4.1 presents the processing durations for various file types on both the original and author's platforms. It offers insights into the processing time in seconds for MP3, EXE, and ZIP files, along with their corresponding sizes. The data emphasizes the superior efficiency of the author's platform, showcasing reduced processing times compared to the original platform for all file types. As indicated in Table 4.1, the author's platform demonstrates an average speed improvement of one-quarter over the original platform, resulting in an increased speed of 15% to 30%.

5. Conclusion. The integration of wireless Bluetooth technology with advanced data security processing, including data signature, encryption, and decryption, has led to the development model for a vehicle-mounted monitoring system. With the support of embedded control technology, this model maintains data integrity during information transmission, safeguarding against breaches and tampering for dependable data transfer. Furthermore, the system's ability to identify data recording equipment post-incident supports its security infrastructure, ensuring a robust mechanism for secure data storage. This contributes significantly to maintain the integrity of critical information providing credible evidence for post-incident analysis and investigations. Through the whole integration of these technologies, the system supports data transmission against potential vulnerabilities and establishes a strong foundation for ensuring data credibility and security in vehicle safety monitoring. As a robust tool, it guarantees sensitive information's accuracy, authenticity, and confidentiality, significantly enhancing safety and security standards within vehicle monitoring and surveillance.

REFERENCES

[1] Al-Absi, M. A., Al-Absi, A. A., & Lee, H. J. (2020, February). Comparison between DSRC and other short range wireless communication technologies. In 2020 22nd International Conference on Advanced Communication Technology (ICACT) (pp. 1-5). IEEE.

[2] Zekavat, P. R., Moon, S., & Bernold, L. E. (2014). Performance of short and long range wireless communication technologies in construction. Automation in construction, 47, 50-61.

[3] Vidakis, K., Mavrogiorgou, A., Kiourtis, A., & Kyriazis, D. (2020, June). A comparative study of short-range wireless communication technologies for health information exchange. In 2020 International conference on electrical, communication, and computer engineering (ICECCE) (pp. 1-6). IEEE.

[4] Joh, H., Yang, I., & Ryoo, I. (2016). The internet of everything based on energy efficient P2P transmission technology with Bluetooth low energy. Peer-to-Peer Networking and Applications, 9, 520-528.

[5] Nusrat, T., Dawod, F. S., Islam, T., Kunkolienker, P., Roy, S., Rahman, M. M., ... & Braaten, B. D. (2022). A comprehensive study on next-generation electromagnetics devices and techniques for internet of everything (IoE). Electronics, 11(20), 3341.

[6] Tyagi, A. K., & Nair, M. M. (2020). Internet of Everything (IoE) and Internet of Things (IoTs): Threat Analyses, Possible Opportunities for Future. Journal of Information Assurance & Security, 15(5).

[7] Rege, K., Goenka, N., Bhutada, P., & Mane, S. (2013). Bluetooth communication using hybrid encryption algorithm based on AES and RSA. International Journal of Computer Applications, 71(22).

[8] Albahar, M. A., Olawumi, O., Haataja, K., & Toivanen, P. (2018). Novel hybrid encryption algorithm based on aes, RSA, and twofish for bluetooth encryption.

[9] Decuir, J. (2014). Introducing bluetooth smart: Part ii: Applications and updates. IEEE Consumer Electronics Magazine, 3(2), 25-29.

[10] Zanella, A. (2009). A mathematical framework for the performance analysis of Bluetooth with enhanced data rate. IEEE Transactions on Communications, 57(8), 2463-2473.

[11] Abdelatty, O., Chen, X., Alghaihab, A., Wentzloff, D. (2021). Bluetooth Communication Leveraging Ultra-Low Power Radio Design. Journal of Sensor and Actuator Networks, 10(2), 31.

[12] Lin, J. R., Talty, T., & Tonguz, O. K. (2015). On the potential of bluetooth low energy technology for vehicular applications. IEEE Communications Magazine, 53(1), 267-275.

[13] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.

[14] Huang, L., Wu, C., Wang, B., & Ouyang, Q. (2018). Big-data-driven safety decision-making: a conceptual framework and its influencing factors. Safety science, 109, 46-56.

[15] Wang, H., Zu, B., Zhu, W., Li, Y., & Wu, J. (2022). On the Design and Implementation of the External Data Integrity Tracking and Verification System for Stream Computing System in IoT. Sensors, 22(17), 6496.

[16] Hsiao, H. I., & Lee, J. (2015). Fingerprint image cryptography based on multiple chaotic systems. Signal Processing, 113, 169-181.

[17] Garg, N., Bawa, S., & Kumar, N. (2020). An efficient data integrity auditing protocol for cloud computing. Future Generation Computer Systems, 109, 306-316.

[18] Inam, S., Kanwal, S., Zahid, A., & Abid, M. (2020). A novel public key cryptosystem and digital signatures. European Journal of Engineering Science and Technology, 3(1), 22-30.

[19] Khan, S., Luo, F., Zhang, Z., Rahim, M. A., Ahmad, M., & Wu, K. (2022). Survey on issues and recent advances in vehicular public-key infrastructure (VPKI). IEEE Communications Surveys & Tutorials, 24(3), 1574-1601.

Edited by: Venkatesan C
Special issue on: Next Generation Pervasive Reconfigurable Computing for High Performance Real Time Applications
Received: Aug 17, 2023
Accepted: Nov 2, 2023