Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

DESIGN AND IMPLEMENTATION OF VEHICLE DATA TRANSMISSION PROTOCOL BASED ON PRESENT ALGORITHM

S.SADDAM HUSSAIN PG Student, Dept of ECE, SITS, Kadapa.
G.LAKSHMI DEVI Assistant Professor, Dept of ECE, SITS, Kadapa.
R.L.B.R.PRASAD REDDY Associate Professor, Dept of ECE, SITS, Kadapa.

Abstract –

In order to monitor the operating status of vehicles, it is necessary to collect vehicle operating data in real time through IoT devices and analyze these data. However, the collected data has the characteristics of multi-source heterogeneous, network resources are limited and server performance is poor. It is difficult to truly realize data processing in real time. In addition, data needs to be transmitted over the network, it is particularly important to ensure the safety of data transmission. Considering the above problems, it is necessary to structure the data and define a unified data format to facilitate data transmission and analysis. At the same time, improve the server communication program and improve the server's concurrent processing capabilities. In addition, considering that data needs to be transmitted over the network, in order to ensure that the data is not stolen or tampered with, the PRESENT lightweight encryption algorithm is adopted to ensure the safety of data transmission. Compared with encryption algorithms such as AES, this algorithm has much lower hardware requirements. This article combines the characteristics of the project and uses the number of communication between the device and the server to achieve the dynamic key update which is approximately one-time pad, and greatly improves the security of the data.

I. INTRODUCTION

The vehicle's transmission range includes US patents issued and a US application to collect and verbally exchange vehicle sensor data easily. The sensors detect the vehicle's condition, speed, braking action, mileage, and neighbourhood. The collected statistics are protected by encryption and are automatically uploaded to a server using the mobile network after the event has propagated. The uploaded vehicle information can be used to decorate the vehicle's motion recognition. The rapid improvement of mobile networks and the slow decline in the prices of IoT devices have provided anincredible basis for developing the IoT industry. The development of the Internet of Things industry brings new forces to traditional industries and provides the beginning of some new industries, including bicycle sharing. However, with the rapid increase in the range of IoT devices, the data volume has also increased geometrically, and better requirements are found in statistical data processing, transmission, storage, and protection. Now, IoT technology has been widely used in many industries. However, it has also added several issues, including device-to-device conversation, access to the device, and device management. Given the problem of heterogeneous records from more than one source, it is extremely important to standardize the format of the information, standardize the design and content of the information and, instead, adapt well to existing technologies. It will not only facilitate the effective collection, processing, and transmission of information but also reduce the problem of log analysis and facilitate database storage. In addition, it is necessary somehow. Therefore, some protection measures must be taken to ensure that the

information is not stolen or tampered with. However, data encryption will devour some hardware assets. For low-power IoT devices, we want to meet the low power requirements, and at the same time, we need to ensure that the encryption algorithm used can ensure data security in a certain volume. Furthermore, ensure the protection of information in transmission. With the unexpected turn of the age of computers, statistics and a lot of technology are finding their way into cars. As a result, there are exciting practical adjustments to their skills and how they interact with drivers. Although some cars have the hardware to learn how to issue warnings to a human driver or control the vehicle independently, they usually have to make these decisions in real-time with only incomplete records. So, it is very important for human drivers to still have some control over the vehicle. Advanced in-vehicle recording structures provide cars with different types and levels of intelligence to aid the driving force. The advent of automotive design enabled an almost symbiotic relationship between driver and vehicle with the help of presenting a complex and judicious interface between the driving force and the vehicle through an intelligent information network. This paper discusses improving the vehicle's control framework known as virtual driving behaviour, a shared mechanism between the driver and the vehicle for belief, decision-making, and control. This article is based on the PRESENT algorithm and combines the features of the task. A dynamic coding system is discovered, a single-use notebook, which greatly improves the certainty of the facts. It will greatly increase the difficulty of theft, tampering, and counterfeiting. The advantage of the lightweight encryption algorithm is that the hardware performance requirements are much lower than the requirements for encryption algorithms that include AES, and the CPU consumes less power to organize the set of cipher rules, which greatly increases the time use of IoT devices. In addition, it reduces the frequency of battery replacement. Finally, this document creates a vehicle tracking system that efficiently collects and classifies records from the engineering position and performs functions including vehicle positioning, personnel control, authority management, system management, and position tracking.

II. REVIEW OF LITERATURE

An ordinary compressor with a control unit has an electronic fuel injection device, automatic transmission systems, an anti-lock brake system (ABS), airbag systems, etc. These devices are the basic additives in the device of a modern car. It is time-sensitive and locked into the reliability and protection of the entire system. Since each real-time requirement management module mainly depends on the data update fee and the control period varies, to meet the real time requirements of each subsystem, it is necessary to implement a general information exchange, including engine speed, wheel speed, and throttle position. The content consists of cadence-gauge finish, gas dimension, A/D conversion, calculation conditions, control trigger, and a series of methods. This way, the transmit and receive data must be completed in 1 millisecond in the electrical fuel control to obtain the requirements in real-time. Therefore, the stats trading community should be competitive based primarily on concerns and have a high-speed conversational style. Given that IoT devices have the characteristics of low power consumption and limited hardware assets, a lightweight symmetric packet cipher set of rules occupying fewer assets becomes a hot spot for studies. PRESENT, CLEFIA, MIBS, and LBlock algorithms laid the foundation for lightweight block cipher algorithms. In presents the current algorithm. The current rule set is a lightweight block cipher. It was proposed in 2007 and is now included in ISO/IEC 29192-2. The rule set requires that the block length be 64

bits and the key size be either 80 or 128 bits. In normal cases, the eighty-bit key already fulfills the appropriate desires. The rule set takes the form of an SP community, and the nonlinear layer is based on a 4-bit unpaired S container, A wide range of iterations is 31; hardware optimization is also considered. Implementing the PRESENT-80 hardware requires approximately 1,570 equivalent gates (GE), which apply to conditions requiring low power consumption and high performance. In describes the security architecture of the IoT within the possibilities of verbal exchange, computation, processing, and decision-making for constrained and low-help devices (related to electricity, processing capacity, and obstacles). And look for related solutions. In has proposed a new set of lightweight LBlock block cipher rules. The rule set requires that the block is 64 bits long and the key is 80 bits more. The Lblock hardware app calls the 1320GE round. In has proposed a new and advanced chat protocol to save electricity, protect privacy and security for smart homes to ensure data integrity and credibility. In has proposed a set of lightweight SIT ciphers with 64-bit block length and 64-bit block length. The algorithm requires only five times the encryption to provide a positive level of protection and can be implemented on a low-cost eight-bit microcontroller.

III. PROPOSED ARCHITECTURE

The common structure of a vehicle management system is shown in Figure 1. The architecture consists of the belief layer, the network layer, the platform layer, and the utility layer. The concept layer is the core component of the Internet of Things and is also an essential part of information collection, and is the direct channel for records. This layer consists of basic sensor addons, including RFID tags and readers, sensors, cameras, GPS, various sensor components, and a community of sensors, including the RFID network and sensor network. The community layer, in particular, consists of many private networks, local area networks, the Internet, cellular networks, and Wi-Fi sensor networks, which are responsible for information transmission and reliable transmission. The platform layer is primarily intended for packages in the cloud environment and features the core offerings required within usability optimization, testing, deployment, and mode of operation, including web and alerting servers, message servers, document storage, and administrative assistance offerings such as access control deployment and alerting, utility performance monitoring, and benchmarking Usage, billing, etc. Finally, the application layer is placed on top of the IoT model. Its characteristics are "information processing," that is, technical facts through a cloud computing platform. The utility layer is specifically used to compute, process, and extract statistics collected through the perception layer for dynamic tracking, real-time manipulation, proprietary control, and clinical decision-making of the physical world. The main functions of the public services layer of the Internet of Things are to end the control and processing of information while integrating this information with various applications in the industry.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

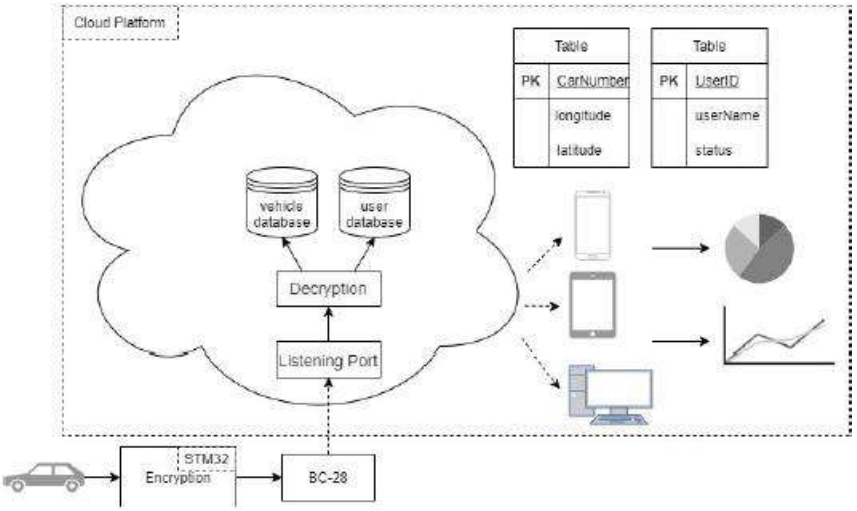

Fig.1 System architecture

In the vehicle management machine, various sensors collect various records of vehicle popularity consisting of temperature, time, latitude, longitude, and personnel statistics in real-time. After encoding and processing by a single-chip STM32 microcomputer, the statistics are sent to the cellular voice exchange network through the BC-28 voice exchange module. The software layer complements information control and data processing, which provides a basis for dynamic monitoring, realtime processing, precision processing, and data mining. It can help enterprises with specific control and scientific selection. Also, the temperature of the device. Supervision, people control, equipment management, and proximity management are also implemented in the application layer. The platform is mainly implemented based on the
MVC design pattern, which can reduce coupling. Between structures, facilitating subsequent maintenance and expanding functionality. Spring, SpringMVC, and Mybatis framework understand the separation of business features, Mysql database achieves data survival strength, Ajax achieves fact interaction, and Json format unifies records. HTML5 framework, CSS, JavaScript, Bootstrap, and rendering plug-in integration, including Charts achieve fact rendering and vehicle location rendering implementation based on Baidu Map API.

IV. SYSTEM IMPLEMENTATION

The single-chip STM32 microcomputer calls the PRESENT algorithm to encrypt the records collected through the vehicle-mounted sensors and then sends the records to the cloud platform server through the BC-28 module. The server software will decrypt the obtained data. Ciphertext The ciphertext and the corresponding plain text are shown in Figure IV. This data can be transferred to the application layer to finish control and data processing, which provides a basis for dynamic tracking, real-time manipulation, management in particular, and record extraction. They can help companies with accurate control and medical selection. In addition, functions such as instrument temperature monitoring, consumer control, device management, and zone control are also implemented in the software layer, providing a more comprehensive medical control technology.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

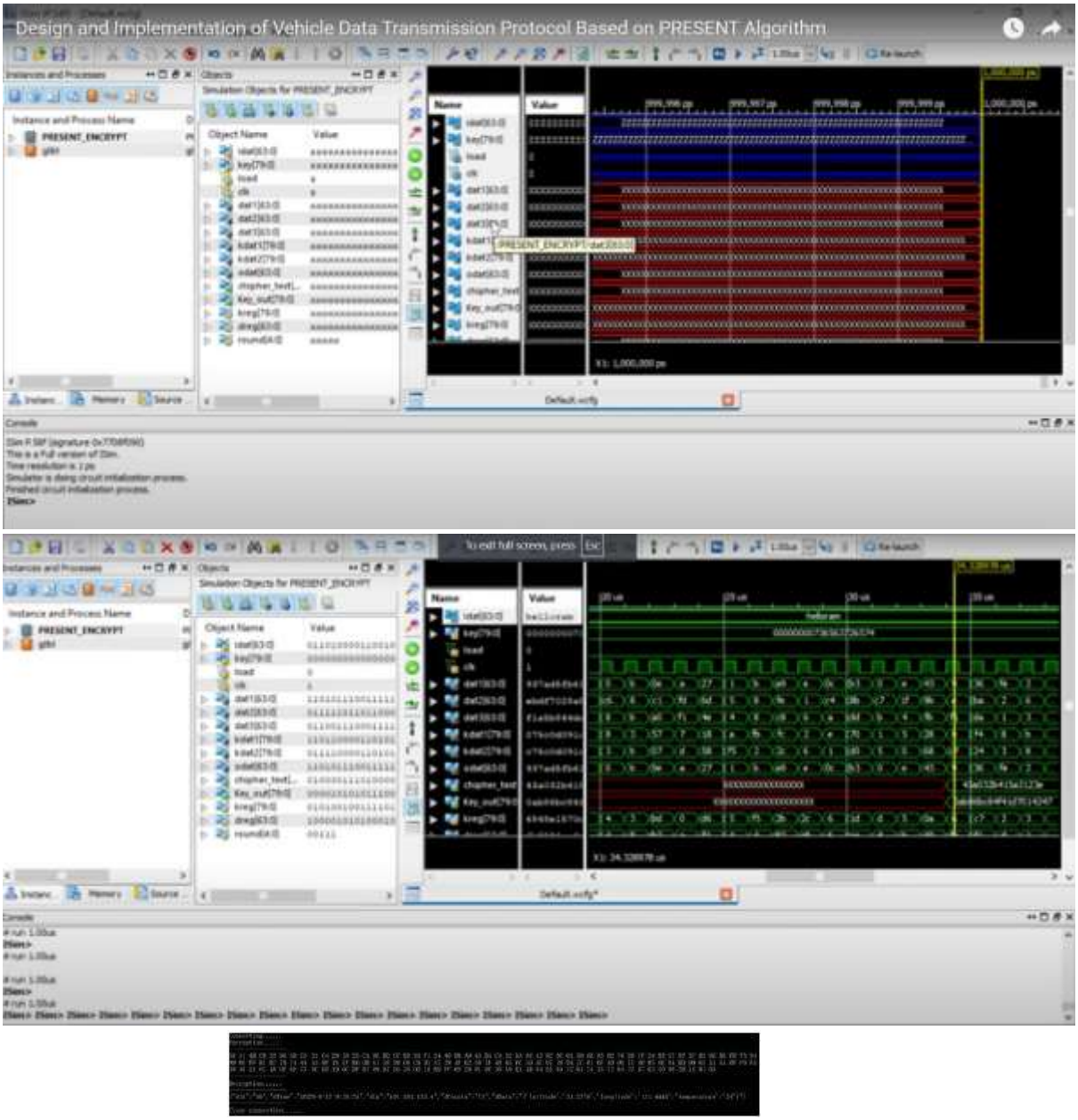

Fig.2 Dynamic encryption process

V. ENCRYPTION ALGORITHM DESIGN

The PRESENT algorithm uses the SP community model. Variety of iterations 31 rounds. Each round passes through SP Road. Each field consists of 3 operations: add round key, sBoxLayer and pLayer

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

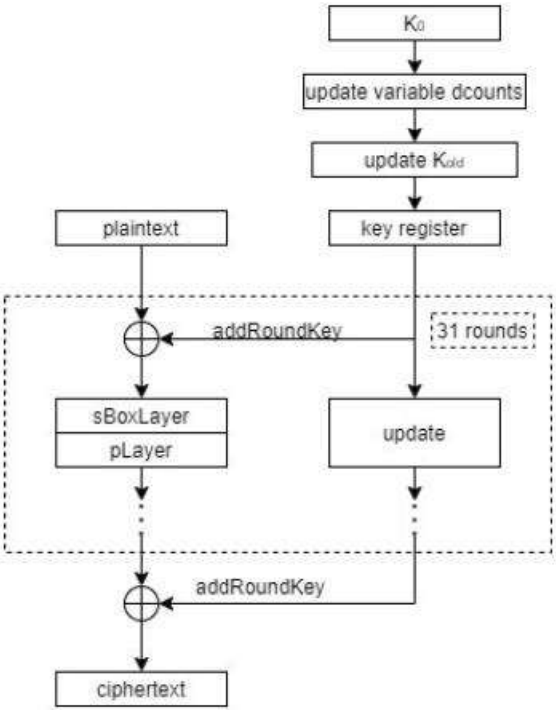

Fig.3 Description of present algorithm

Based on the PRESENT-80 algorithm combined with real engineering emergencies, this bulletin updates a dynamic switch, achieving almost a one-time effect. Compared to using static keys for encryption, this will increase the hacking problem and prevent information from being properly encrypted, stolen, and tampered with. The encryption technology is implemented as follows: an initial key K is stored in the IoT tool and the server, and the number of variable discounts is stored to maintain regular communication between the tool and the server. The process is illustrated in Figure 3.

VI. CONCLUSION

This paper designs and implements a fully auto logger security transfer protocol based on the CURRENT algorithm, collects relevant logs with the help of GPS and various sensors, and encrypts the data using the stm32 single-chip microcomputer by calling the existing rule set, and communicates with the server through the BC-module 28. The utility layer that meets the actual needs of the enterprise is built on the cloud platform. The functions of device temperature monitoring, user control, instrument management, proximity monitoring, and abnormal alarm are implemented by processing the accumulated data through the perception layer. Based on the current algorithm, the number of conversations between the machine and the server is used to achieve dynamic key updating. It is a unique classifier that greatly improves the security of data transmission and achieves convenient, practical effects.

REFERENCES

1. Christoffer Dharma, Vijaya Saradhi Dommeti, “Optimization of Layer Thickness to Yield Predetermined Shielding Performance of Multilayer Conductor Electromagnetic Shield”, International Conference ACCT-2011, ISBN: 978-981-08-7932-7.

2. Vijaya Saradhi Dommeti, Hemambaradhara Rao, 2020, “Some Investigations on Shielding Effectiveness of Multilayered Conductor Electromagnetic Shield” , National Conference on advances in communication Technologies.
3. Bogdanov A. et al. (2007) PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg.
4. Singh, S., Sharma, P.K., Moon, S.Y. et al. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Human Comput (2017).
5. Wu W., Zhang L. (2011) LBlock: A Lightweight Block Cipher. In: Lopez J., Tsudik G. (eds) Applied Cryptography and Network Security. ACNS 2011. Lecture Notes in Computer Science, vol 6715. Springer, Berlin, Heidelberg.
6. T. Song, R. Li, B. Mei, J. Yu, X. Xing and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1844- 1852, Dec. 2017.
7. Usman M , Khan S . SIT: A Lightweight Encryption Algorithm for Secure Internet of Things[J]. International Journal of Advanced Computer ence & Applications, 2018, 1(1).
8. Partha Pratim Ray,A survey of IoT cloud platforms,Future Computing and Informatics Journal,Volume 1, Issues 1– 2,2016, Pages 35-46.
9. Prasadu Peddi (2019), Data Pull out and facts unearthing in biological Databases, International Journal of Techno-Engineering, Vol. 11, issue 1, pp: 25-32.
10. MehaboobMujawar, D. Vijaya Saradhi, “Design and performance comparison of arrays of circular, square and hexagonal meta-material structures for wearable applications” Journal of Magnetism and Magnetic Materials,
11. D. Vijaya Saradhi, Swetha Katragadda, Hima Bindu Valiveti , 2021,“Hybrid filter detection network model for secondary user transmission in cognitive radio networks” International Journal of Intelligent Unmanned Systems, ISSN: 2049-6427.