International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 6, Issue 4 (April 2017), PP.01-07

Android-Based Secure Monitoring System for Industrial Power Plants

Joonhyuck Choi[1], Myungchul Kang[2], Yungho Lee[2], Jayung Gi[2], Dongik Lee[1,*]
[1] *School Of Electronics Engineering, Kyungpook National University, Daegu, Republic Of Korea*
[2] *EGT Co. Ltd, Daejeon, Republic Of Korea*

ABSTRACT: This paper presents a secure remote monitoring system for industrial gas turbines. By adopting remote monitoring techniques, not only can the human resources required for supervising the turbines around the clock be reduced, but also the reliability in detecting faults with the turbine can be improved. In this work, the proposed system supports the remote monitoring of the gas turbine status with an android-based smart phone. Also the proposed system utilizes the well-known RSA algorithm with a 512-bit encryption to protect the sensitive information of turbines from unauthorized access including hackers. The level of security is further enhanced by prohibiting the users from saving the received turbine data on their devices. The performance of the resulting system is evaluated with an experimental setup including a virtual data generator.
Keywords: Android, Monitoring system, Gas turbine, Security, RSA algorithm

I. INTRODUCTION

Power plants are the fundamental facility for producing electric energy which is very vital for many people and industry. Hence, power plants require an extremely high level of stability and safety. The failure to monitor the power plant may cause critical accidents resulting in massive economic and environmental losses, such as the cases of the Chernobyl and Fukushima nuclear power plants [1]. In particular, since it is inevitable to operate the power plant pauselessly, condition monitoring on the primary system, such as gas turbines, should be carried out 24-hour a day in order to respond to any abnormal situation before it develops into a serious secondary damage. However, condition monitoring relying on human resource is inefficient because not only it requires huge cost, but also it may result in inaccurate monitoring due to lack of concentration and accumulated fatigue.

This work presents a real-time remote monitoring system that allows system operators to monitor the key state variables without having to reside in the power plant. Considering the fact that more than 83% of people in the nation use smart mobile devices [2], the proposed system is developed using an Android-based smart phone. The remote monitoring system can be vulnerable to cyber attacks because the data is transmitted to the personal device through a wireless commercial network [3]. Researchers highlighted that the hacking attack on the nuclear power plant would be dangerous when the internal operation data has been leaked [4]. In this work, hence, the well-known RSA algorithm is applied to ensure the security of the remote monitoring system. In general, the secure transmission with RSA algorithm requires a 1024-bit encryption. However, in this work, a 512-bit encryption is applied to ensure the real-time processing capability with a smart phone. The decreased level of security due to 512-bit encryption is compensated by prohibiting the users from storing the turbine data on their devices. A set of experiments are performed using a data generator to verify the performance and effectiveness of the proposed remote monitoring system and security techniques.

II. DESIGN OF REMOTE MONITORING SYSTEM

2.1 System overview

Most of smart phones in the market are based on either Android or IOS. According to the recent market survey [5], the domestic market share of Android-based smart phones being used in the country accounts for 76.7%. Therefore, this work implements the remote monitoring system based on the Android operating system.

Fig.1 shows the configuration of the entire monitoring application using the JAVA socket communication. Client devices transmit and receive the information about log-in, permission, and gas turbine status with the socket server through the application. The MySQL database, which is primarily provided by the Android operating system, performs the data management [6].

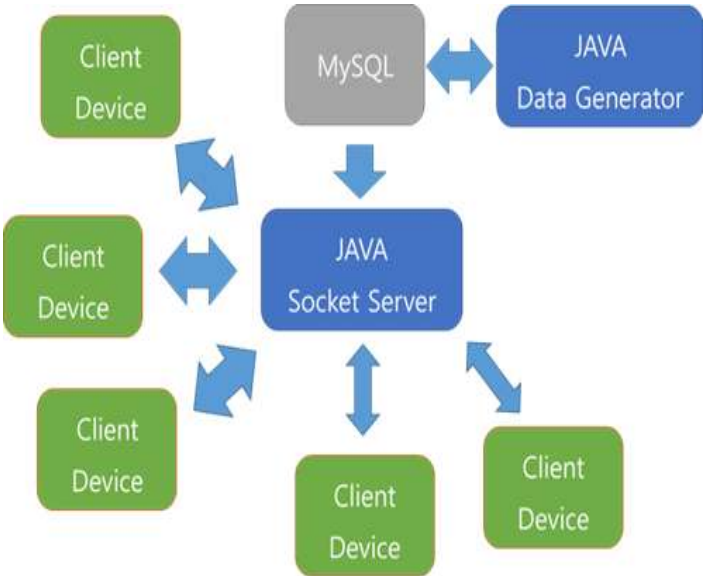

Figure 1. Configuration of remote monitoring application.

2.2 Remote monitoring application

The remote monitoring application, in conjunction with the existing condition monitoring equipment attached to the gas turbine, provides the functionality of client devices to access the gas turbine status information. As shown in Fig. 2, the user interface of the application is made up with a main screen and a few detailed screens. The main screen displays the system schematic and operational values for users to easily identify the status of the gas turbine. The detailed screens are configured to display the operating values of each subsystem in real time.

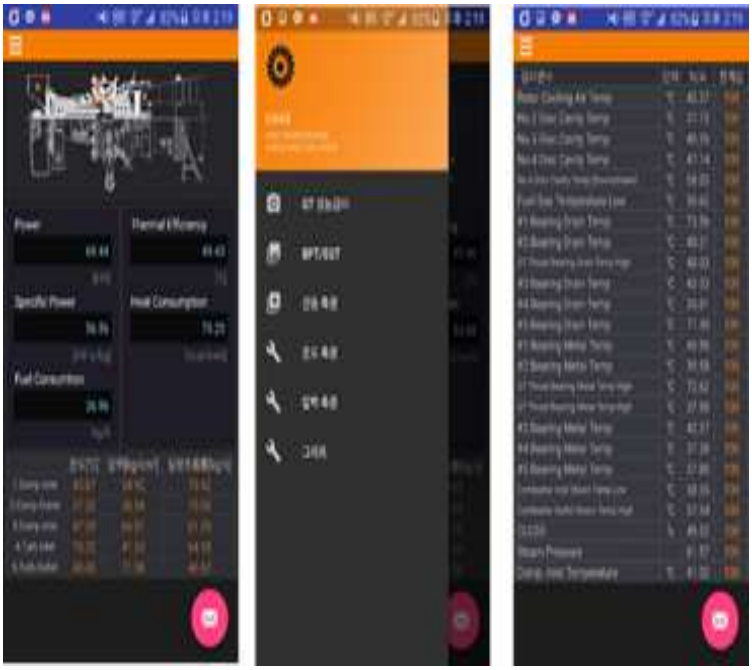

Figure 2. User interfaces for remote monitoring application.

2.3 Differential authorizing algorithm

Since the different level of authorities is granted to the users for data access, the server checks whether the user's identification (ID) is valid for logging-in and accessing the data. The differential authorization function depending on the user's grade is implemented using the algorithm described in Fig. 3. A different level of authority is given to the user depending on his/her position, and accordingly a different user interface is provided corresponding to the verified authority level.

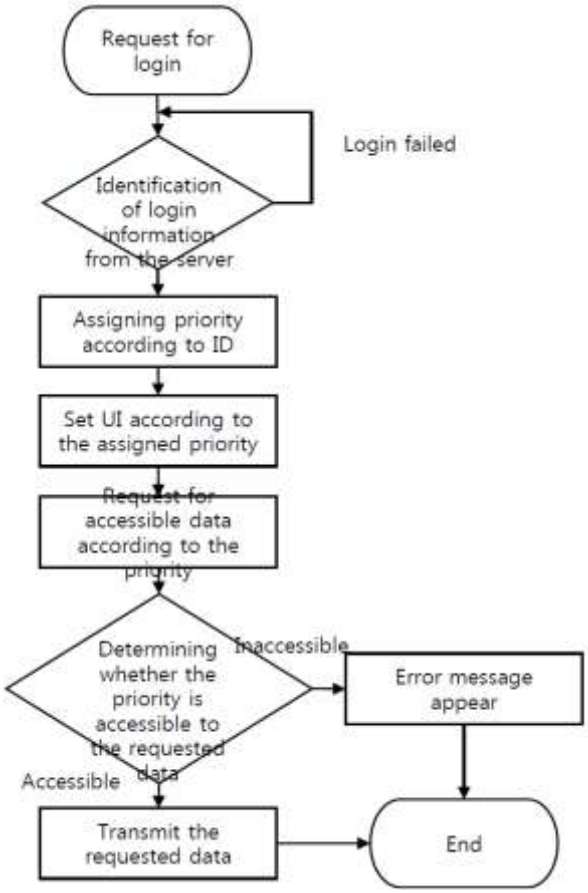

Figure 3. Differential authorizing algorithm.

2.4. Notification service based on GCM

The main function of the remote monitoring application is to alert the responsible system operators to quickly identify a malfunction with the gas turbine. However, it is not possible that users are always paying attention to the monitoring system and responding to the abnormal situation immediately. Therefore, it is necessary to provide the users with alarm signals when abnormal situation is detected.

In this work, an alarm service based on the Google Cloud Message (GCM) [7] is realized and added into the remote monitoring application for promptly notifying abnormal condition to the users. The procedure to generate an alarm is shown in Fig. 4. The server that controls the GCM service detects abnormal situation in the gas turbine facility. However, alarming messages can be duplicated if the push messages are transmitted whenever abnormal data is generated. To deal with this problem, it is designed to generate push messages based on the edge at which the data transits from normal to abnormal. In this work, it is set to determine an abnormal situation when the value of critical status data exceeds 95% of the predefined threshold as shown in Fig. 5.

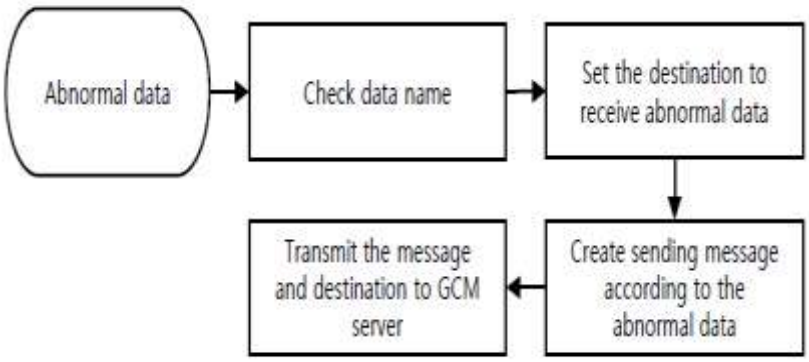

Figure 4. Algorithm for generating push messages.

Figure 5. Implemented function for abnormal status alarms.

III. SECURITY OF REMOTE MONITORING SYSTEM

3.1. RSA algorithm

Since the remote monitoring system uses a personal smart device and wireless communications, it is difficult to physically restrict the access from unauthorized persons. The most vulnerable aspect of the remote monitoring system is the leakage of confidential information during the sending and receiving process. The leakage of confidential data of gas turbine can lead to a serious social and economical damage.

In this work, to achieve the security of remote monitoring system, we exploit the existing RSA algorithm with a 512-bit composite number for data encryption. According to the report [8], the data encrypted using a 512-bit RSA composite number was deciphered through the experimental attempt for five months with a hundred of computers. Consequently, security experts now recommend the use of RSA composite number more than 1024 bits. However, in the case of the remote monitoring system proposed in this paper, it is difficult to use a 1024-bit RSA composite number due to the limit of real-time computing power with a smart phone.

To overcome this problem, the proposed system exploits a 512-bit RSA composite number for effective real-time processing, while it prohibits the users from storing the received turbine data on their smart devices in order to compensate for the reduced level of security with a low-bit RSA number. Hence, the smart device used for remote monitoring can only display and print the data continuously, but dispose past data without storing on it. This approach is based on the fact that a monitoring system requires a large amount of data obtained for a period of time to accurately analyze the gas turbine status. The risk of large information leakage from continuously deciphering the 512-bit encrypted data in real time is extremely low. By taking this approach, the unauthorized access can only get part of data, from which meaningful information about the gas turbine cannot be obtained.

3.2. Security coding algorithm

Considering the fact that Android applications are generally developed on the basis of JAVA programming language, the security technique used in this work is also implemented in JAVA. The RSA algorithm contains several functions that produce random prime numbers, perform modular arithmetic, and generate a public key and a private key. The data to be transmitted is encrypted and decoded using these functions. But, considering the computational power of a smart phone, the minimum operation in encryption and decryption is realized. The device generates a public key and a private key to request data from the server, and sends a data request message with the public key to the server. The server encrypts the data using the public key and sends the encrypted data back to the requesting smart device. Then the smart device decodes the encrypted data using the private key. The algorithm for implementing the security function is presented in Fig. 6 and Fig. 7.

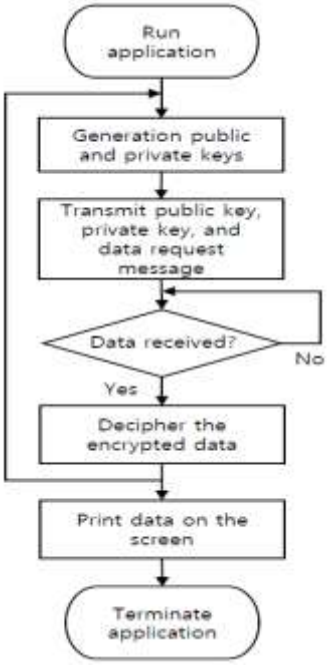

Figure 6. Flowchart of encryption algorithm for client.

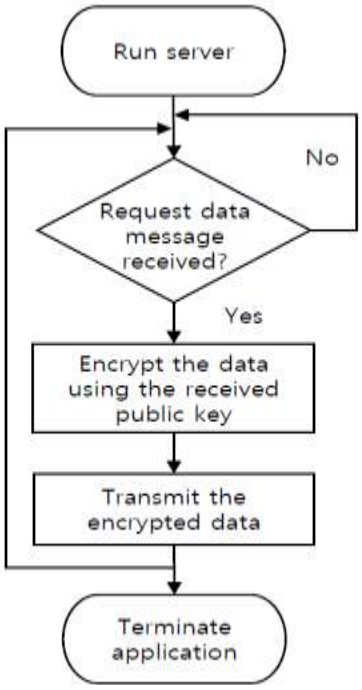

Figure 7. Flowchart of encryption algorithm for server.

IV. EXPERIMENTAL RESULTS

4.1. Verification of remote monitoring system

In order to verify the performance of the remote monitoring system presented in this paper, a data generator based on JAVA is produced. Fig. 8 shows the test environment for verifying the remote monitoring system. The data generator produces a series of random data and sends them to a personal smart device. The generated data A, B,…, N are assumed to be the sensor data and the status data. It has been seen that appropriate user interface could be displayed according to the different ID of the personal smart device. When the server generated some abnormal data, the effectiveness of the remote monitoring system has been verified by producing an appropriate notification with alarms.

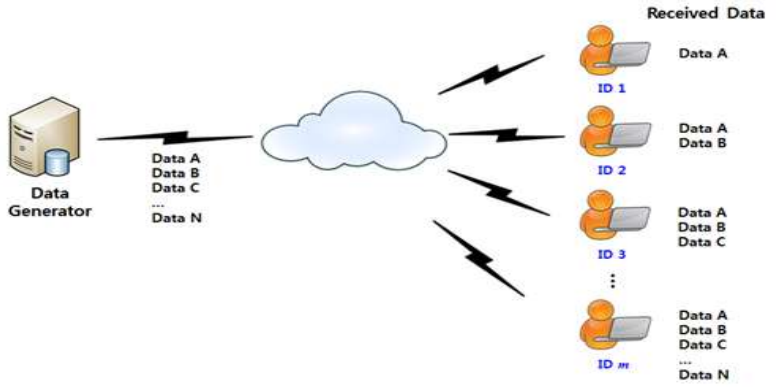

Figure 8. Concept for verifying remote monitoring system.

4.2. Verification of RSA security algorithm

The stability of the RSA algorithm has already been verified over decades [10][11]. Hence, this work focuses on the verification of real-time processing with the RSA algorithm implemented in the remote condition monitoring application. The update interval of the real-time status data is set to 0.25s to 1s, and the effect of RSA algorithm on real-time data transmission is assessed by measuring the executing time of encryption and decryption. The measured execute time for RSA algorithm is shown in Fig. 9. From the experimental results, the mean time of encryption and decryption process is around 20ms. This result is short enough time which is equal to 1/12 to 1/50 of the data update cycle, 0.25s to 1s. Therefore, the proposed security method seems suitable for real-time data transmission of the remote monitoring system, even considering the response time for data transmission time and application execution time.

Figure 9. Measurement of processing time for encryption algorithm.

V. CONCLUSION

In this paper, a remote monitoring system that allows real-time monitoring on the state of industrial gas turbines has been proposed. The proposed system was implemented using an Android-based smart phone and wireless communications. Since the purpose of the remote monitoring system is to enable an external operator immediately recognize the abnormal status in the gas turbine, an alarm service has been implemented using the push message technique. Different user interfaces were provided according to the corresponding authority for data access. In addition, the real-time security technique using the RSA algorithm has been applied to achieve the secure operation of the remote monitoring system. Finally the performance and efficiency of the proposed system have been verified through a set of experiments.

ACKNOWLEDGEMENTS

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20151120200070).

REFERENCES

[1]. Jai Wan Cho and Kyung Min Jeong, "Remote Controlled Robots Used for the Mitigation of the Fukushima Nuclear Power Plant Accident," Journal of Institute of Control, Robotics and Systems, pp. 148-151, 2011.

[2]. Connecting Lab, Mobile Trend 2015, Window of Future, 2014.

[3]. Sung-tae Kang and In-june Jo, "Individual Users based Smart Phone Remote Management System Design and Implementation," Journal of the Korea Institute of Information and Communication Engineering, pp. 2675-2681, Vol. 16, No. 12, 2012.

[4]. Ho-Jun Ko and Huy-Kang Kim, "A Study on Vulnerability Analysis and Incident Response Methodology based on the Penetration Test of the Power Plant's Main Control Systems," Journal of The Korea Institute of Information Security and Cryptology, Vol. 24, No. 2, 2014.

[5]. StatCounter, available: http://www.statcounter.com/

[6]. Y.H.Shin and J.C.Ryu, "Study on Adoption of Suitable Encryption Scheme According to Data Properties on MySQL Database," Proc. Korea Computer Congress 2010, Vol. 37, No. 1, 2010.

[7]. "Google Cloud Messaging for Android - Android Developers," available: http://developer.android. com/google/gcm/index. html.

[8]. Thomas. H. Cormen, Foundations of Cyptography: Algorithms Unlocked, MIT Press, 2013.

[9]. Robert D. Silverman, "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths," RSA Laboratories, Bulletin #13, April, 2000.

[10]. T. Fujita, K. Kogiso, K. Sawada, and S. Shin, "Security Enhancement of Networked Control Systems Using RSA Public-key Cryptosystem," Proc. 10th Asian Control Conference (ASCC), 2015, pp. 1-6, 2016.

[11]. A. Selby and C. Mitchel, "Algorithms for Software Implementations of RSA," IEE Proceedings, Vol. 136E, 1989, pp. 166–70.