International Journal of Engineering & Technology, 7 (4.38) (2018) 105-108

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security between Dehumidify Dryers and a Monitoring Server in Plastic Manufacturing Control

Byung Mun Lee

Dept. of Computer Engineering, Gachon University, Korea
**Corresponding author E-mail: bmlee@gachon.ac.kr*

Abstract

When moisture over an allowable range is included in material during the plastic manufacturing process, a defective product might be produced, hence management of the dehumidifying dryer process is needed. Therefore, to maintain the material's optimal humidity, a dehumidify dryer measures data in real time and transfers the data to a server; based on the measurement results, it suggests a smart factory model for appropriate control. However, even if the data is accurately measured, if its integrity and confidentiality are not maintained during the transfer process, control data sent to a dehumidify dryer can cause unintended malfunctions. Therefore, this study suggests an overall encryption mechanism that can maintain the integrity and confidentiality of data at the same time during the transfer process. We confirmed through an experiment with this mechanism that when data is damaged or altered during a transfer process, a person can check this. We expect that the method suggested in this paper will help the productivity of the plastic manufacturing process to increase and defective product rate to decrease.

Keywords: *Security, Smart Factory, Dehumidify Dryer, Manufacturing, Control*

1. Introduction

A smart factory provides efficiency and intellectualization of processes by combining IT technology with the manufacturing business, and increases productivity [1-2]. Smart factory technology can be used in the process of injection molding to produce the plastic.

Generally, the injection molding of plastic involves a three-step process, as follows: transferring plastic synthetic resin material, dehumidify the material, and injection molding [3]. In the injection molding step, if moisture is included in the material over an allowable range, tiny water drops can be formed, and the product will have bubbles, which makes it defective. Therefore, a dehumidify dryer is necessary [4]. This device measures the moisture quantity, and when that value is high, the heater inside the dehumidify dryer needs to be operated to reduce the moisture quantity. On the other hand, when the moisture quantity is low, the operation of the heater needs to be stopped, and it needs to be controlled to increase the moisture quantity [5]. Like this, a dehumidify dryer measures the moisture content data that changes frequently in real time and needs to transfer it to the monitoring server.

About 10-100 dehumidify dryers are usually operated in one factory building, and when they are operated at the same time in many buildings, the number increases accordingly [6-7]. Because many facilities and devices, including overhead cranes, are installed inside a factory, stable data transfer over a wireless network is difficult. However, if the immediacy and stability of measured and controlled data are not guaranteed, the defective product rate will increase, while productivity decreases at the same time [8-11].

To solve this issue, this study analyzes the disruption of integrity that can happen during data transfer between dehumidify dryers and monitoring servers. Wrongly measured data or damaged data can make wrongly controlled data; therefore, a serious malfunction problem may be caused. This study suggests an encryption mechanism to solve these kinds of issues. The encryption mechanism considers all confidentiality and integrity and can check if transferred data is damaged or altered in the middle of the network. To confirm the usefulness of this method, we did an experiment. We tried to verify if the suggested method was applied effectively with a disruption of integrity experiment.

2. Drying process for plastic injection molding system

Figure 1 is a picture image of a plastic manufacturing factory (A) and the processes of dehumidify drying and injection molding (B).

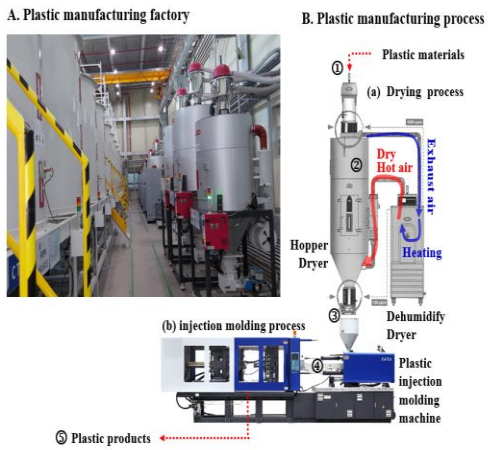

Fig. 1. Plastic manufacturing factory and process

When synthetic resins which are plastic materials are inserted into a hopper dryer (①), a dehumidifying process occurs where dry hot air inside takes moisture out of the material (②). Due to this process, exhaust air with moisture is sent to a dryer, which gets rid of the moisture through the drying process. Dry hot air is emitted to the hopper dryer again and continuously dries the material. The dry material goes into the injection molding machine (③) and is injected into the plastic product (④⑤). The material is different according to the plastic product that is to be produced [5]. The suitable drying temperature for dehumidification and moisture quantity are different for each material, as shown in Table 1. This fact means that the controlled heater temperature is different for each material in a dehumidify dryer.

Table 1. Characteristics of plastic materials

Plastic material	Initial moisture quantity	Drying moisture quantity	Drying temperature
ABC Acrylonitrile	0.3%	0.07%	80°C
PA6 Polyamide	0.5%	0.07%	70~80°C
PPD	0.1%	0.07%	120°C
PMMA Polyoxymethylene	0.4%	0.05%	80°C

3. Threat of Data Inconsistency between Dehumidify Dryer and Server

I suggest a smart factory network for plastic injection molding in figure 2. It is composed of many dehumidify dryers, a mobile alarm controller, large dashboard, and real-time monitoring server.

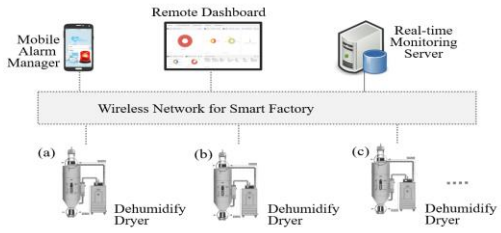

Fig. 2. System configuration for dehumidifying dryers in a smart factory

For the safety of workers and facility management in the factory, wireless LANs are mainly composed, with a server and a cable network. When the plastic manufacturing process is under way, the dehumidify dryer mainly measures and collects the data of drying temperature and dew point temperature, and transfers those to a server in real time. Typically, many kinds of injection molding products are produced in one factory at the same time. The material fed to a hopper dryer is different, and the dehumidifying condition becomes different at each time. Therefore, each controlled data that is transferred to a dehumidify dryer in a server is different. For example, because the optimal drying temperature of the fed material in (a), which is 70°C ~ 80°C, and the optimal drying temperature of the fed material in (b), which is 120°C, are different, the control command to stop or operate the heater is different for each one.

In this situation, data has to be accurately transferred and has to be safe for a production process not to have a problem. If an unapproved transfer or unexpected command is permeated or flowed into a smart factory network, there is a possibility of damaging the data and threatening stability. To safely protect the system from this, data confidentiality, availability and integrity have to be satisfied.

A. Data Confidentiality

The data that is mainly transferred from a system is application data that is distributed between the dryer and monitoring server. Generally, even if it has a security function provided in respect to a network or operating system, confidentiality can be breached because of data being eavesdropped from an application's malfunction or intentional man-in-the-middle attack. To maintain confidentiality, encryption before transferring and a decoding process after reception has to be done. However, because it is not personal information or medical data that should never be exposed, it is less important than other breaching factors

B. Data Availability

Data availability is important because it is related to the instantaneity of data in a smart factory. This is because proper control can be formed right away when drying temperature data measured in a dehumidify dryer is sent immediately. The solution to this problem is that secondary safety is necessary by considering a factory's site, although it is appropriate to compose a smart factory LAN with a cable network rather than a wireless network

C. Data Integrity

When data for drying temperature or dew point temperature from a dryer is transferred to a monitoring server, there can be a breach attack on integrity that counterfeits that value. As shown in figure 3, when a drying temperature of 160 and dew point temperature of 80 degrees are counterfeited to 167 and 75 degrees, respectively, with a spoofing tool and transferred to a monitoring server, they have a weak point to be used in a server as they are. In this case, a defective product can be produced when a dehumidify dryer is operated poorly as faked control data is transferred. Therefore, because the dryer embedded application generates transfer data in the form of text inside an http protocol packet, the content may easily be counterfeited or altered. This is a problem that can happen in the process of introducing an open platform to a smart factory, which is the current trend.

Fig. 3. Scenario for the violation of data integrity.

This problem does not guarantee integrity with the encryption method used in keeping confidentiality. Therefore, the next chapter will suggest an integrated security mechanism for this

4. Secure Data Transfer for Data Integrity

To guarantee the integrity of data, the signature code is needed to guarantee that encrypted contents are not counterfeited or altered. By using the MD5 hashing function (HF), figure 4 suggests a safe data transfer mechanism to achieve this.

In figure 4, transferred data acquires encrypted results, $E(data_i)$ with a Spritz algorithm by using the key, K. Acquired information is coded with the MD5 algorithm and finds $MD5(E(data_i))$, and locates it in front of encrypted $E(data_i)$ and composes a transferring message. The reason for locating the MD5 code in front of $E(data_i)$ is because a hashing code value is generated with lengths that are always constant, parsing is convenient for deciphering. Also, as this method pursues safety in the process of encryption, it is a method of using MD5 and a Spritz encryption algorithm that was made lightweight to decrease the burden on the function.

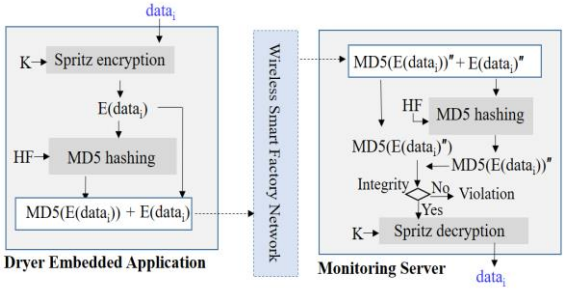

Fig.4. Scenario for the violation of data integrity.

5. Experiment and Evaluation

By applying the suggested encryption mechanism, encryption and a combined transferring algorithm that can be performed in a dehumidify dryer are realized on a Node.js platform. The monitoring server achieves the decryption algorithm by using MySQL and Node.js, and stores received data in a DB. When the received data goes out of normal value, the encrypted message is transmitted to the mobile alarm manager in real time. Figure 5 shows a confirmation message by capturing an encrypted message with the Burp Suite Tool.

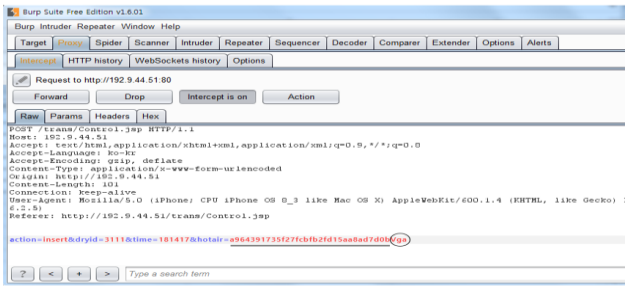

Fig. 5. Captured message from dryer to mobile application via server using Burp Suite Tool.

As shown at the bottom of figure 5, the stored value in the hot air parameter is a hash code value obtained with the MD5 method, and the 3 bytes at the very end is the actually encrypted drying temperature value. We confirmed that confidentiality and integrity could be maintained by using this value on the reception side.

6. Conclusion

To decrease the defect rate of plastic products, real-time dehumidifying management is needed. Even if a measurement is accurate, the defective product rate can increase if integrity and confidentiality are breached in the data transfer process. This study suggests a security mechanism to send measured data and controlled data safely and confirmed its usefulness through an experiment.

7. Acknowledgements

This work was supported by the technology development program (Grants No. S2598497) funded by the Ministry of SMEs and Startups (MSS, Korea).

8. References

[1] J. Kurosz, and A. Milecki. The idea of "industry 4.0" in car production factories. Proceedings of the 2nd International Conference on Intelligent Systems in Production Engineering and Maintenance, **(2018)** October 17-18; Wroclaw, Poland.

[2] A. Rojko. Industry 4.0 concept: Background and overview, International Journal of Interactive Mobile Technologies, 11, 5, pp. 77-90, **(2017).**

[3] J.C. Ferreira, and A. Mateus. Studies of rapid soft tooling with conformal cooling channels for plastic injection moulding, Journal of Materials Processing Technology, 142, 2, pp. 508-516, **(2003).**

[4] S.H. Tang, Y.M. Kong, S.M. Sapuan, R. Samin, and S. Sulaiman. Design and thermal analysis of plastic injection mould, Journal of Materials Processing Technology, 171, 2, pp. 259-267, **(2006).**

[5] R. Moretto, Method and plant for dehumidifying material in granular form. U.S. Patent 879,390, 0B2, Oct 16 **(2010)**.

[6] X. Li, and J. Wan. Proactive caching for edge computing-enabled industrial mobile wireless networks, Future Generation Computer Systems, 89, pp. 89-97, **(2018).**

[7] J. Wan, S. Tang, Z. Shu, D. Li, S. Wang, M. Imran, and A.V. Vasilakos. Software-Defined Industrial Internet of Things in the Context of Industry 4.0, IEEE Sensors Journal, 16, 20, pp. 7373-7380, **(2016).**

[8] M. Shin, J. Woo, I. Wane, S. Kim, and H. S. Yu. Implementation of Security Mechanism in IIoT Systems. Proceedings of the Sixth International Conference on Green and Human Information Technology, **(2018)** Jun 30; Chiang Mai, Thailand.

[9] J. Lopez, C. Alcaraz, and R. Roman. Smart control of operational threats in control substations, Computers & Security, 38, pp. 14-27, **(2013).**

[10] W.D. Yu, L. Davuluri, M. Radhakrishnan, and M. Runiassy. A Security Oriented Design (SOD) Framework for eHealth Systems. Proceedings of international workshop on Computer Software and Applications Conference, **(2014)** Jun 20; Vasteras Sweden.

[11] K. Knorr, and D. Aspinall. Security testing for Android mHealth apps. Proceedings of IEEE 8th International Conference on Software Testing, Verification and Validation Workshops, **(2015)** Apr 13-17; Graz, Austria.