Enhanced Approach of Risk Assessment for Insider Threats Detection in Smart Manufacturing

N A Hashim¹, Z Zainal Abidin¹*, Z Abal Abas¹, N A Zakaria¹, R Ahmad¹ and E Mardaid¹

¹Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka 76100 Durian Tunggal Melaka Malaysia

E-mail: zaheera@utem.edu.my

Abstract. The smart manufacturing integrates Internet of Things (IoT), cloud systems, data analytics and machine learning for autonomous implementation particularly in the factory’s supply chain. The additional components from Information Technology (IT) gives convenience accessibility in spike of welcomed threats from inside or outside the boundary to do harmful events. The valuable information in smart manufacturing consists of intellectual property (IP), assets (hardware and software) data and human talent that lead to data theft and illegal activities due to its monetary values. However, little work is done on assessing risks invaluable information particularly threats from inside. In fact, studies on risk assessments are focusing on financial profit, supply chain production and IT assets. Therefore, an enhanced approach of risk assessment for insider threat detection (RAFITD) is introduced. The proposed approach contributes to a log monitoring of the log on and log out activities, based on the role of employee on a software dashboard. From the result, the log monitoring produces two scenarios, which is the ideal and non-ideal. For the ideal scenario, a balanced ratio between log on and log out is accomplished. Meanwhile, a non-ideal scenario performs an imbalance ratio. The impact of the study brings an insider threat detection for better analysis.

1. Introduction

Each year the smart manufacturing is facing new challenges and changes that must be realized to ensure the sustainability of a business. In actual fact, smart manufacturing is at a high risk of danger due to the condition in the supply chain and vulnerabilities exist in the manufacturing components towards Industry 4.0 [1]. A risk assessment approach for smart manufacturing is highly in demand [2] and provides greater agility to prevent disruptive and catastrophic incidents to the manufacturing industry. Common problems occurred in smart manufacturing are minimizing risk [3] and unappreciated risk [4].

The minimizing risk factor requires a very dynamic nature of current age demand and supply balance and put the companies on high business risk. To minimize risk is gradually becoming a difficult call. Any stone unturned in decision making will cost a huge impact. On the other hand, unappreciated risk involves insider threat, which originates from person who misuse authentic access to smart manufacturing factory’s cyber assets for unlawful and malicious goals or who carelessly create vulnerabilities. They might be permanent workers, contractors, or suppliers and programmers [5]. With this misuse authentic access, they can steal, interrupt, or damage the computer systems and crucial information without discovery by ordinary perimeter-based security resolutions and controls which emphasis on points of entrance instead of what or who is currently inside. In fact, a number of insider threats and attack cases have been reported to national cybersecurity and it is arising [6]. Section II
explains related works. Section III describes methods and shows the results and findings on the risk assessment for insider threats. Section IV concludes the study on risk assessment for insider threat detection.

2. Related Works

The weaknesses of the entity's systems, facilities, products or services potential threat in smart manufacturing allow threats from inside or outside of the factory to damage the system. The current model for risk assessment the potential threat in smart manufacturing is illustrated as in Figure 1.

![Figure 1. Risk Assessment for Potential Threats in Smart Manufacturing [7].](image)

2.1 General Settings: Abstraction of Basic Structures and Relation.

Machines in smart manufacturing are equipped with embedded systems, sensors and IT hardware and software components, which allows autonomous operation over traditional manufacturing. The implementation of an information system consists of cloud-based solutions and client-server application that provides instant customer-supplier interactions, which infrastructure and its IT assets risks are assessed accordingly.

2.2 Modeling and Formalizing Smart Factory.

The smart factory is designed to perform production based on the capacity of the assigned components. IT assigned components in the production line are relying directly or indirectly on IT components and the information network services without changing the overall approach. For direct functional dependency on production components of the IT component, there is a high power usage else there is a redundancy of information network.

2.3 Risk Quantification Approach.

The non-availability of IT components limits the output of dependent production components due to interference and failure in IT component. Thus, the failure in IT assets leads to risk evaluation of identified risk at the critical nodes and decision making is determined for better solutions.

On the other hand, Figure 1 explains on risk assessment of performing risk values (i.e.: High, Medium or Low) for all IT assets and arrange IT assets in terms of their threat possible to the production network [7], [8]. For example, Email Server is (High Risk). However, the privileged information and level of user permission who access IT assets in the smart factory, still not be observed and analyzed. For instance, why is user A accessing to Email Server in network B? Why is user Z accessing at the same time to Email Server and Node D? This crucial information could be obtained from the log file but the log file only contains node number, node name, event, timestamp, and activity of the node. Therefore, the log file monitoring [9] is important in insider threat detection since it observes the activities at the various levels of the organization especially at the access events system [10], which motivates the researcher to include log monitoring process into the proposed model. The enhanced approach of risk assessment for insider threat detection is illustrated in section 3 in Figure 2.

3. Risk Assessment For Insider Threat Detection (RAFITD)

RAFITD monitors log files from the authentication level in the access control system. The log file contains huge and various types of events, thus we concentrate on the event situation of log on and log out from the computer access based on the role of employee in the smart factory.
3.1 General Settings on Authentication.

The architecture of smart manufacturing is developed according to general settings in Figure 1. Nonetheless, using RAFITD, the log file is configured at the authentication process that is log on and log out. The authentication process is done at each employee’s computer, cloud, client-server application, smartphone application, Internet-of-Things device and sensor, which involve a huge amount of logs.

3.2 Formalization.

The production line with direct relation to IT component and network services shows a high amount of energy usage, which is $f_E$ is energy usage in the production line as stated in equation 1.

$$f_E > \sum IT \text{ component} + \sum network \text{ services}$$  

(1)

Conversely, the production line without implementation of IT component and network services produces a low power consumption in Equation 2 but redundancy occurred in performing the same task.

$$f_E < \sum IT \text{ component} + \sum network \text{ services}$$  

(2)

Thus, any high consumption of energy use in the production line indicates that there is an employee who accesses to the line to start the machine or any network node in the smart factory.

3.3 Log Monitoring

In the proposed log monitoring algorithm is a procedure for governing equations to monitor the computer access log data according to each employee’s role. Role, $i = \{1, 2, \ldots, n\}$ where $n$ is the number of roles in the company, which $f_i$ calculates the number of computer access log data based on the number of roles of the employee in the organization as given in equation 3.

$$f_i = \sum log \text{ on} + \sum log \text{ off}$$  

(3)

For an ideal scenario, the summation of log on is equal to log out that gives equation 4.

$$f_{ii} = \sum log \text{ on} = \sum log \text{ off}$$  

(4)

For the non-ideal scenario, the summation of log on is not equal to log out as shown in equation 5.

$$f_{ii} = \sum log \text{ on} \neq \sum log \text{ off} \Rightarrow \forall_i$$  

(5)

3.4 Risk Quantification

The risk quantification evaluates the probability of scenarios of ideal and non-ideal based on the ratio of a balance event in log on and log out. If the summation of log is ideal, then, there is a probability of non-insider threat exist in the smart factory that given in equation 6.

If $P(f_i) = P(f_{ii})$ then non-insider threat  

(6)
If the summation of the log is non-ideal, then, a probability of insider threat exist as given in equation 7 and also other factors occurred such as equations of network failure (8), hardware damage (9) and power outage in (10).

If \( P(f_i) = P(f_{in}) \) then insider threat is likely exist \hspace{1cm} (7)

If \( P(f_i) = P(f_{in}) \) then network failure is likely exist \hspace{1cm} (8)

If \( P(f_i) = P(f_{in}) \) then hardware damage is likely exist \hspace{1cm} (9)

If \( P(f_i) = P(f_{in}) \) then power outage is likely exist \hspace{1cm} (10)

The RAFITD model develops using R programming codes to achieve a software dashboard in monitoring every log on and log out at the computer accessed by each employee based on the role or work position in the smart manufacturing factory.

4. Results and Discussion

Figure 3 illustrates the software dashboard to monitor log on and log out activities in one month based on the role of the employee. The user interface of the dashboard named RAFITD consists of the left side menu of the selection, for instance, main page, employee data, log file, and graphs and right side of the interface to show the results. RAFITD dashboard is useful for security administrative person in charge at the security center. The security administrative person monitors the log activities at the dashboard and inspect the log. Any ideal or non-ideal scenarios are documented and recorded either in softcopy or hardcopy. The security administrative person sends a report to a higher level of management for further action. The general manager of the department gives a warning or in worst case a warrant if the employee has committed to crime.

Figure 4 shows a graph of several access computer log on and log off based on the role of employee. As we can see that the VP, unknown, senior manager, security, technician, project manager, janitor, engineer, council, loading dock, foreman, IT Admin, director and administrative assistant log on and
log off as usual. The blue bar is log on and the red bar indicates log out. Most of the bar produces a balanced ratio between blue and red bars. This means most of the employee is non-insider. However, the technician is log on all the time since the technician produces an ignorant attitude to log off the computer.

Therefore, the technician has the probability of intention to perform illegal activities and create an opportunity to violate access to permission. On the other hand, there is a probability that the technician is on shift for maintenance or down-time operation. Based on our findings, these results suggest that the risk monitoring process needs to be a continuous process to detect insider threats in terms of frequencies.

A possible assumption from this result shows that the probability of new employees using new devices or mobile phones may lead to the status of unknown user. On the other hand, the campaign on awareness about password and username among employees helps to reduce the ignorance attribute in the access log on and log off activity. Seminar and sharing sessions among employee for all levels assist the management to have a better control and security in preventing the cyber crime from happening.

**Figure 4.** Graph of log on and log out versus role of employee

### 5. Conclusion

This paper presented an enhanced model of risk assessment for insider threat detection in smart manufacturing. As industries are moving towards the industrial revolution, cyber-crimes and threats are reported to increase as business growth. The findings of this study contribute to a RAFTID model and a dashboard to detect log file computer access based on the role of an employee at an authentication level. The current investigations have shown insider threats in terms of scenarios in ideal and non-ideal. The unknown user has been detected among employees who successfully gain access to the computer.

Future research should, therefore, concentrate on the investigation of event and log information of insider threats using risk assessment from mobile phones and Internet-of-Things devices.

**Acknowledgment**

Thank you and appreciation to Ministry of Higher Education Malaysia for sponsor a research grant for project TRGS/1/2016/FKP-AMC/01/D00005 under program TRGS/1/2016/UTEM/01/3. Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka.
References
[1] Nilufer T and Stephen H 2018 Journal of Manufacturing Systems 47 pp 93-106
[2] Avlijaš G 2019 Management: Journal of Sustainable Business and Management Solutions in Emerging Economies 24 pp 11-23
[3] Bayer E and Bustad G O 2012 Introducing Risk Management Process to a Manufacturing Industry
[4] Brandis H G 2015 A Personnel Security Handbook pp 24
[5] Department of Homeland Security and Homeland Infrastructure Threat and Risk Analysis 2013 National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat
[6] US Homeland Security NCCIS 2015 Seven Strategies to Defend ICSs
[7] Häckel B, Hänsch F, Hertel M and Übelhör 2019 Business Research. Springer 12 pp 523-558
[8] Schmidt G and Proske 2015 Proceedings of the 6th International Probabilistic Workshop
[9] Gheyas I A and Abdallah A E 2016 Big Data Analytics 1 pp 1-29
[10] Amruta A and Narendra S 2015 Procedia Computer Science 45 pp 436 – 445