Journal of Theoretical and Applied Information Technology
15th October 2017. Vol.95. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INSIDER RISK PROFILE MATRIX TO QUANTIFY RISK VALUE OF INSIDER THREAT PREDICTION FRAMEWORK

[1]ISZAIDA ISMAIL, [2]ROHAYANTI HASSAN, [3]MUHAMMAD RAZIB OTHMAN, [4]ASRAFUL SYIFAA' AHMAD, [5]NADA ELYA TAWFIQ

[1,2,3,4] Department of Software Engineering, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia

[5] Computer Science Department, Nawroz Univesity, Computer and I.T College, Duhok, Iraq

E-mail: [1]iszaida@gmail.com, [2]rohayanti@utm.my, [3]razib@ utm.my, [4]asrafulsyifaa.ahmad@gmail.com, [5]Nada.tawfiq@nawroz.edu.krd

ABSTRACT

An insider threat refers to the threat arising from an individual inside an organization that maliciously leverages his or her system privileges, and closeness and proximity in a computerized environment to compromise valuable information and inflict harm. This scenario is an example of system violation that decreases the degree of system trustworthiness. Most cases of system trustworthiness use a peer judgment formulation, which may involve bias sentiments towards document sensitivity values. Moreover, audit trails of risky document navigation paths are important as an alarm to indicate any violation. Therefore, this study presents a combination of the trust criteria and document sensitivity level of an insider to obtain a risk value, which will be used to predict the occurrence of an insider threat. This study begins by investigating the prominent attributes of insiders with a focus on their degree of experience and skill in line with system trust. Subsequently, these prominent attributes are used to construct an insider Trust Profile Matrix (TPM). From the TPM, the trust value is calculated and combined with the sensitivity value of each document to produce a Risk Matrix (RM). As a result, (i) risk value and (ii) prediction rate and risky path are then calculated and analyzed using an Insider Threat Prediction Framework as an alarm for violation occurrence.

Keywords: *Insider Threat, Insider Threat Prediction, Sensitivity Level, Trust Value, Risk Value*

1. INTRODUCTION

The security information is playing a crucial function in protecting confidentiality, integrity and availability of the data information system [1]. Nowadays, it is pointed where every organization attempt encounters serious information and network security threat that may cause to lose, changing and misuse of the data by internal or external users. Commonly, insider threat is categorized as a major contributor to increased risk and systems damage. The present of threats to the system became a huge problem in order to maintain the security management in the system.

The insider attack formed the biggest threat on database, system and network due to an authorized user had the bad behavior or revenge on someone. There are many possible issues of occurrence the increasing the system risk such as human behavioral factors. The availability of heterogeneous factors of insider threats in system application making it progressively ambiguity to identify which factors are contributed to be a significant attribute of attacking the system. As stated by Neuman [2] insider threat attributes are particularly relevant to potential insider misuse the system. Among the highlighted attributes in this study include insider knowledge, trust, privileges and risk assessment. According to Moyano *et al*. [3] indicated that a successful predicting threat depends on both technical and behavioral solutions of system user. Thus, an appropriate and constructive behavior by a system's users can enhance the effectiveness of information security while inappropriate and destructive behaviors can substantially inhibit its effectiveness [4].

Some of the insider threat prediction framework does not emphasize some important attributes that are able to predict the threat may attack the document. According to research by Yaseen and Panda [5], they extended the previous framework to investigate the problem of insider threats in relational database systems. A Constraint and Dependency Graph (CDG), and the Dependency Matrix were developed to represent dependencies and constraints of each table and introduce the Threat

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Prediction Graph (TPG) to predict and prevent an insider threat of each table. Their framework also did not implement experiments to establish the effectiveness of the models until they are extended their predicting framework to insider threat mitigation [6] using the same technique and enhance on evaluation phase to test the effectiveness of the framework. However, the percentage of the prevented threat ranges from 8 to 30 % depending on the number of transactions and the percentage of write operations in transactions. This shows that, the prevention range is still low.

A sensitivity of data item or document access is the document which insider may be interested in changing, due to the importance and secrecy of the information that it represents [5]. Besides that, releasing information about sensitive data carries serious risks to privacy. Therefore, priority of each sensitive document should be given to provide the highest levels to different insider who accesses the document. Frequently, an expert has a priority to assign the sensitivity level. However, judgment from an expert many unknown variables. According to Moyano *et al*. [3] and peer's judgment processes are crucial in the identification of insider vulnerabilities. In addition, due to bias of a peer assessment, judgment from the experts only is not sufficient. Meanwhile an expert is prone to a confirmation bias. There also no judgments are made as to the accuracy the expert opinion in predicting a threat. Therefore, this study has motivated to improve the insider threat prediction framework by combining the insider trust profile matrix with the sensitivity value of each document in order to produce the risk matrix.

The details of this paper are explained more details regarding the relate works, case study used, proposed framework and the result respectively in section 2, 3 and 4.

2. RELATED WORKS

Insider threat prediction refers to the effort to detect the existing threats that were exposed by a legitimate user in a systems development. The process of prediction insider attack in the information system can create a mechanism to mitigate and prevent the threat that contributes by the insider. According to the previous researches, most of the researcher have overcame a few issues regarding the threat, especially prediction of insider threats in the relational database.

Prediction insider threats are regularly presented by the researcher using the own techniques such as Kandias *et al*. [7] proposed algorithm to predict dangerous users. A formal methodology was implemented by Sengupta *et al*. [8], while Magklaras and Furnell [9] proposed end user sophistication model. Yaseen and Panda [5] also proposed insider threat prediction model.

Althebyan and Panda [10] has suggested a knowledge-base model in order to predict insider threat. The researchers had developed a Knowledge Graphs that able to track knowledge of each insider accumulates thus able help in predict the malicious act that insider going to implement. Once the knowledge of insider has gained, then clustering document based on insider request to access document is initiated. Then, insider threat prediction algorithm insider threat prediction algorithm is implemented in which in this proses, involved risk value and attack probability calculation.

Althebyan and Panda [10] and Paci *et al*. [11] as well has brought up insider trust factors in their prediction framework. However, the framework did not briefly discuss the detail elements of insider trust attribute. Besides that, weighted calculations of sensitive documents is solely dependent on expert judgment that could lead bias.

3. THE CASE STUDY

E-Plantation System (ePS) has been used as a case study. ePS is a web-based, integrated information system that is centralized and geographically-distributed that allows users remotely access operation sites using the virtual private network (VPN). ePS is organized under three different levels of operation which are headquarters (HQ), region and branch. In this paper, only payroll module is used as a focus for this study. Under payroll module there are 7 sub modules/documents which are Set Earning (PY1), Set Deduction (PY2), Set Productivity- Harvester (PY3), Set Productivity- Tapper (PY4), Payroll Sheet- Salary (PY5), Payroll Sheet- Cash Denomination (PY6) and Payroll Checking (PY7).

Those documents can be accessed by multiple insiders which are the developer, system administrator, system support, and end user. Table 1 shows an insider access matrix, in which insider can access the following system function such as create (C), update (U), read (R), view (V) and process (P). Insider access matrix is the important element in order to assign the sensitivity value of each document.

Figure 1 shows a structure of payroll document that motivated by [10] who are presented the system access path using graph based representation. The tree representation is able to demonstrate the authorized traversal path for different insider roles.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Furthermore, it is extended to action including create, update, read, view and process that can be performed by each insider. Thereby, tree is easy to quantify the sensitivity value of each document and its action that has been accessed by an insider. Payroll structure consists of 4 layers where layer number 1 represented the insider developer, system support, system administrator or end user. Layer 2 refers main module of the system, while layer 3 is a list document of a selected module. Layer 4 refers to the function of each document module.

4. ENHANCEMENT ON RISK VALUE QUANTIFICATION

Insider threat prediction framework has been presented as shown in Figure 2 in order to predict the violation occurrence performed by system insider based on their risky score when navigating documents. However, this paper had made improvement on insider risk profile matrix as per illustrated on Figure 3, this procedure consist of four main processes which focuses on combining trust component and document sensitivity in order to predict the insider violation occurrence. This framework embodies Trust Profile Matrix (TPM) that specifically designs to characterize the knowledge of system insider which is self-feeding information. TPM is attributed to skill and experience degree of system insider.

On the other hand, Fung *et al*. [12] has claimed that trust is an important criterion to predict the system violation occurrence and they formulated trust based on peer judgment. However, trust is subjective and peer judgment may bias due to human emotions and error prone. Conversely, our framework presents that trust value can be formulated based on the degree of skill and experience of system insider. The details of processes are described in the following section.

Table 1: Function and Action of Payroll Module

Function	User Role	Create (C)	Update (U)	Read (R)	View (V)	Process (P)
Set Earning (PY1)	Developer	√	√	√	√	x
	System Administrator	x	x	x	√	x
	System Support	√	√	√	√	x
	End User	√	√	√	√	x
Set Deduction (PY2)	Developer	√	√	√	√	x
	System Administrator	x	x	x	√	x
	System Support	√	√	√	√	x
	End User	√	√	√	√	x
Set Productivity-Harvester (PY3)	Developer	√	√	√	√	x
	System Administrator	x	x	x	√	x
	System Support	√	√	√	√	x
	End User	√	√	√	√	x
Set Productivity-Tapper (PY4)	Developer	√	√	√	√	x
	System Administrator	x	x	x	√	x
	System Support	√	√	√	√	x
	End User	√	√	√	√	x
Payroll Sheet-Salary (PY5)	Developer	x	x	x	x	√
	System Administrator	x	x	x	x	√
	System Support	x	x	x	x	√
	End User	x	x	x	x	x
Denomination (PY6)	Developer	√	√	√	√	x
	System Administrator	√	√	√	√	x
	System Support	√	√	√	√	x
	End User	√	√	√	√	x
Payroll Checking (PY7)	Developer	x	x	x	√	x
	System Administrator	x	x	x	√	x
	System Support	x	x	x	√	x
	End User	x	x	x	x	x

Journal of Theoretical and Applied Information Technology
15th October 2017. Vol.95. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

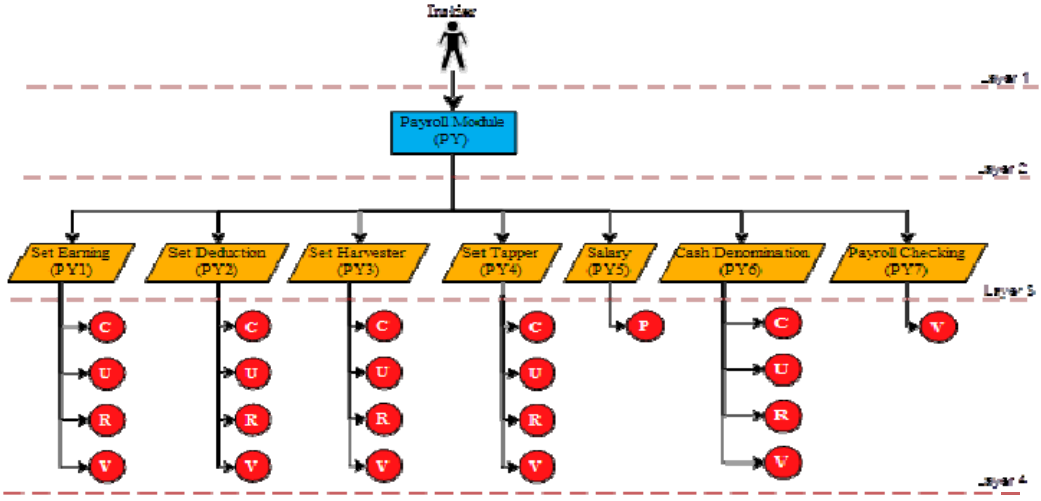

Figure 1: Structure of Payroll Document

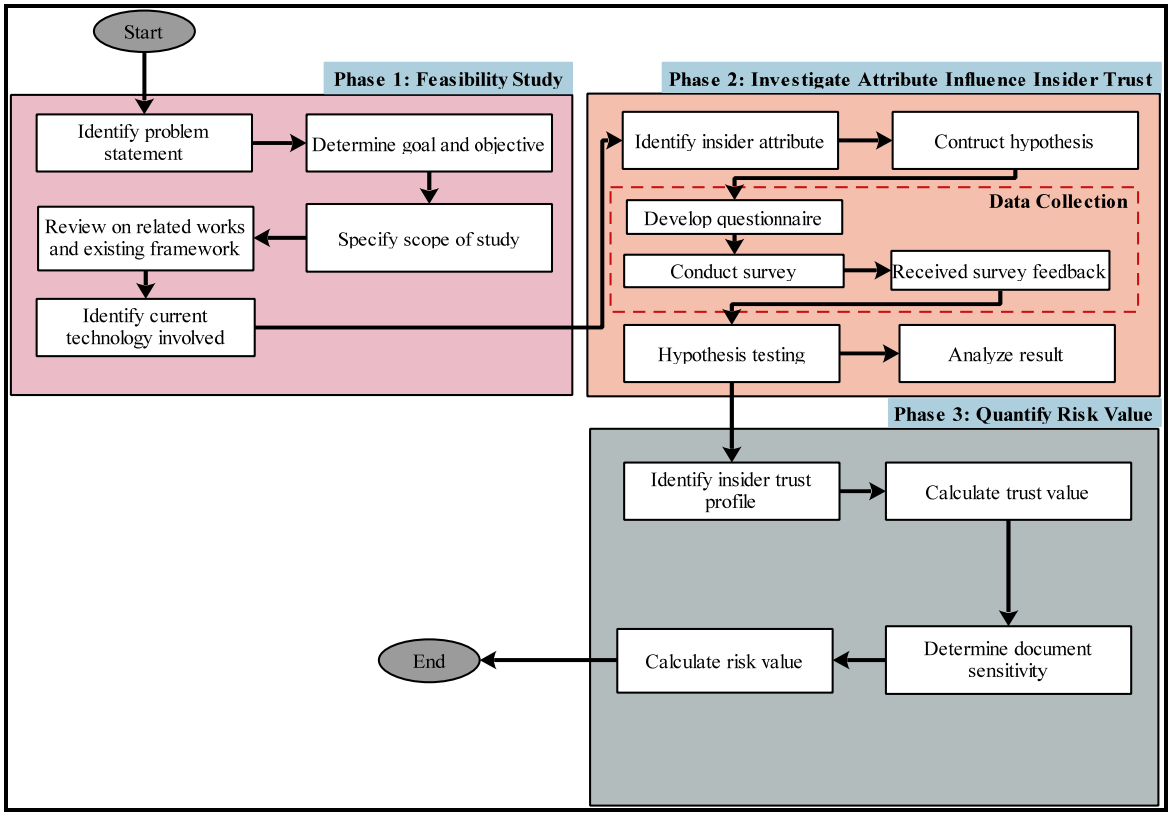

Figure 2: A Framework of Insider Threat Prediction

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

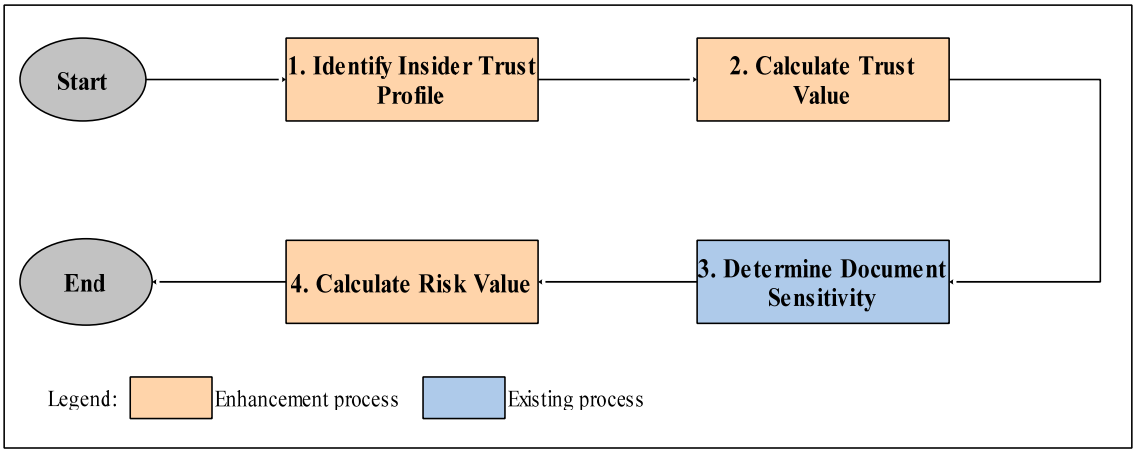

Figure 3: Procedures to Quantify Risk Value

4.1 Identify Insider Trust Threat Profile

Table 2 summarizes the trust characteristics that emphasize two attributes which are experience and skill. The insider with high or low skill and experience could tend to some issues including; i) system handling; ii) bugs/errors; iii) security policy; iv) fine tuning server and network; and v) computer usage. For insider respondent, they have to answer several questions in order to generate insider threat profile. As per illustrated in Figure 4 is a sample of questionnaire that later on, the result of the questionnaire will be used to get the value of experience and skill of an insider as based on scoring as shown in Table 3 and 4 respectively. Answers from the questionnaire are converted into experience and skill scoring, in which these value will be used to get the trust value. An answers are based on roles and the component. Table 5 shows an example of experience and skill rating for one of an insider role, S1.

Table 2: Description of Trust Characteristics

Component	Skill Description	Experience Description
Computer usage	Insider that has high skill on computer usage are positively associated to low expose in data leakage.	Insider that has a good experience on computer usage are positively associated to low expose in data leakage.
System handling	Insider with low skill in handling the system are positively associated to low expose in data leakage.	Insider with poor experience in handling system are positively associated to low expose in data leakage.
Solving bugs	Insider with high skill in solving error or bug are positively associated to low expose in data leakage.	Insider with poor experience in solving error or bug are positively associated to low expose in data leakage.
Security policy	Insider with low skill on security policy are positively associated to low expose in data leakage.	Insider with good experience on security policy are positively associated to low expose in data leakage.
Server and network fine tune	Insider with low skill on fine tuning server and network are positively associated to low expose in data leakage.	Insider with good experience on fine tune server and network are positively associated to low expose in data leakage.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

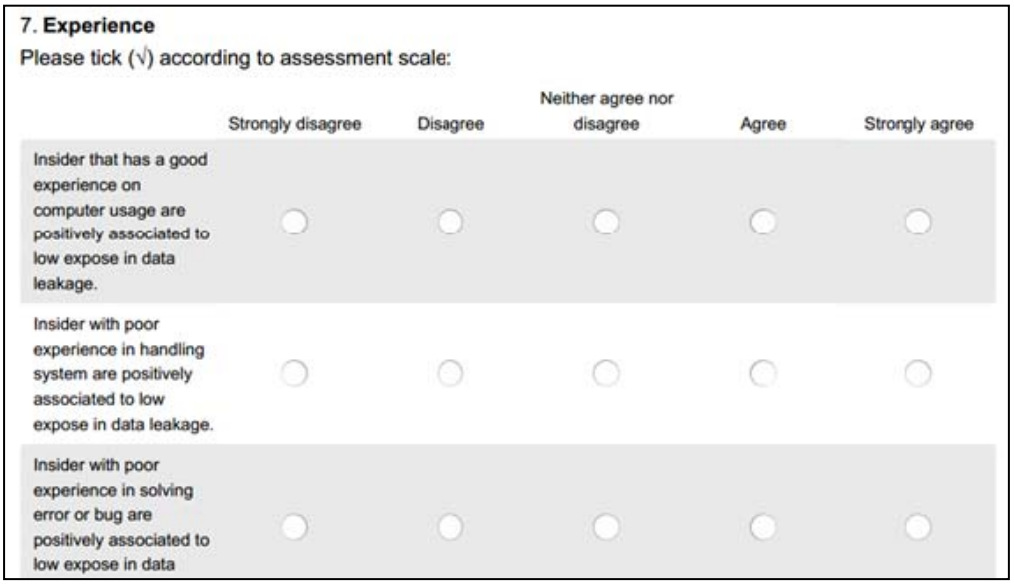

Figure 4: Sample of Questionnaire

Table 3: Scalar for Experience Scoring Value

ID	Questionnaire rating	Experience rating
1	Strongly Disagree	Very Poor
2	Disagree	Poor
3	Neither Agree nor Disagree	Neutral
4	Agree	Good
5	Strongly Agree	Very Good

Table 4: Scalar for Skill Scoring Value

ID	Questionnaire rating	Skill rating
1	Strongly Disagree	Very Low
2	Disagree	Low
3	Neither Agree nor Disagree	Medium
4	Agree	High
5	Strongly Agree	Very High

Table 5: Example of Experience and Skill Scalar

Roles	Component	ID Questionnaire Skill Rating		ID Questionnaire	Experience Rating
S1	Computer usage	5	Very High	5	Very Good
	System handling	5	Very High	5	Very Good
	Solving an error/bugs	5	Very High	5	Very Good
	Security policy	4	High	5	Very Good
	Fine tuning server and network	5	Very High	5	Very Good

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2 Calculate Trust Value

On the other hand, Paci *et al*. [11] have claimed that trust is an important criterion to predict the system violation occurrence and they formulated trust based on peer judgment. However, trust is subjective and peer judgment may bias due to human emotions and error prone. Conversely, this study presents that trust value can be formulated based on the degree of skill and experience of system insider. Thus, Trust Profile Matrix (TPM) that specifically designs to characterize the knowledge of system insider which is self-feeding information. TPM is attributed to skill and experience degree of system insider.

Table 6 represents Trust Profile Matrix in Scoring Value that are used to calculate the trust value. Table 7 illustrate the example of predetermined trust value based on component and roles of the system user using the TPM provided.

Based on the example on the table below, S1 is represent as a system developer, S2 represent system administrator, S3 and S4 represented as a system support and end user of an ePS system respectively. S1 has a very high skill and very good experience in system computer usage, system handling and solving error/bug. Therefore, the trust value of those 3 components is very trusted. However, S2 has low skill and poor experience regarding system fine tune server and network, thus, his trust towards the system is classify as untrusted. Thus, Using TPM can summarize that insider with good experience and high skill can be delegated to a trusted person.

Table 6: Trust Profile Matrix in Scoring Value

Experience	Skill				
	Very Low [1]	**Low [2]**	**Medium [3]**	**High [4]**	**Very High [5]**
Very Poor [1]	U	U	U	N	N
Poor [2]	U	U	N	N	T
Neutral [3]	U	N	N	T	T
Good [4]	U	N	T	T	VT
Very Good [5]	N	T	T	VT	VT

Note: VU: Very Untrusted [1], U: Untrusted [2], N: Neutral [3], T: Trusted [4], VT: Very Trusted [5]

Table 7: Example of Trust Value Determination

Roles	Component	Skill Rating	Experience Rating	Trust Value
S1	Computer usage	Very High	Very Good	Very Trusted
	System handling	Very High	Very Good	Very Trusted
	Solving an error/bugs	Very High	Very Good	Very Trusted
	Security policy	High	Very Good	Very Trusted
	Fine tuning server and network	Very High	Very Good	Very Trusted
Total Trust				**Very Trusted**
S2	Computer usage	High	Very Good	Very Trusted
	System handling	Medium	Very Good	Trusted
	Solving an error/bugs	Medium	Neutral	Neutral
	Security policy	High	Neutral	Neutral
	Fine tuning server and network	Low	Poor	Untrusted
Total Trust				**Neutral**
S3	Computer usage	High	Good	Trusted
	System handling	Medium	Good	Trusted
	Solving an error/bugs	Medium	Poor	Neutral
	Security policy	High	Neutral	Trusted
	Fine tuning server and network	Medium	Very Poor	Untrusted
Total Trust				**Neutral**

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Roles	Component	Skill Rating	Experience Rating	Trust Value
S4	Computer usage	Medium	Neutral	Neutral
	System handling	Low	Neutral	Neutral
	Solving an error/bugs	Low	Very Poor	Untrusted
	Security policy	Low	Neutral	Neutral
	Fine tuning server and network	Very Low	Very Poor	Very Untrusted
Total Trust				**Untrusted**

4.3 Determine the Document Sensitivity Value

Sensitivity value is classified as a weightage value of document that accessed by an insider. A rate for sensitivity value is in accordance with the scale from 1 to 5 which is very less sensitive to very sensitive. This scale weightage is adopted by Althebyean and Panda [10]. A sensitivity value of document is also given by an expert based on a predetermined scale. As previously described, for ePS case study, expert from Prodata Basis has been assigned the sensitivity value of each document function for different rows as tabulated in Table 9. The sensitivity of sensitivity document is based on type of user role in the system and the document accessed type either the document is sensitive or nor. The guideline can be referred to Table 8. A grant value of sensitivity document by the expert includes system document function. Subsequently, Figure 5 shows example of an insider S1 accessing possible document and function in payroll module. If developer access for path PY1, C, U, R and V, the sensitivity value of the document is very less sensitive, less sensitive, neutral, very less sensitive and neutral respectively.

Table 8: Sensitivity Scoring

ID	Sensitivity
1	Very Less Sensitive
2	Less Sensitive
3	Neutral
4	Sensitive
5	Very Sensitive

Table 9: Sensitivity Value of Documents

Role	Action & Sensitivity				
	C	U	R	V	P
Developer	LS	N	VLS	N	N
System Administrator	LS	N	LS	S	VS
System Support	N	S	LS	VS	S
End User	N	S	S	VS	VS

Note: VLS: Very Less Sensitive [1], LS: Less Sensitive [2], N: Neutral [3], S: Sensitive [4], VS: Very Sensitive [5]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

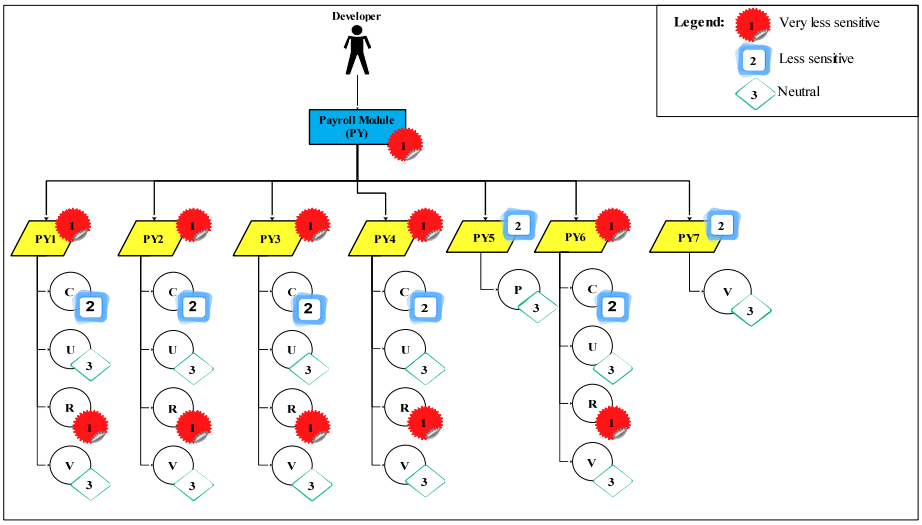

Figure 5: Example of Document Sensitivity for S1

4.4 Determine the Navigation Document Path and Risk Value

Table 10 shows an example of the predetermined document path navigation for insider role, S1 (system developer). This prediction has been extracted from business process of system requirement specification. Later on, having this path navigation is used as input to calculate risks value.

Table 10: Document Path Navigation

No	Path
1	PY, PY1, PY2, PY3, PY4, PY5, PY6, PY7
2	PY, PY1, C, U, R, V
3	PY, PY2, C, U, R, V
4	PY, PY3, C, U, R, V
5	PY, PY4, C, U, R, V
6	PY, PY5, P
7	PY, PY6, C, U, R, V
8	PY, PY7, V

4.5 Calculate Risk Value of Document Access

Risk Matrix (RM) by Paci *et al*. [11] has been adopted in study to calculate the risk value for document access by an insider otherwise known as path navigation as shown in Table 11. The determination value of risk is associated with the threat initiated based on trust value in section 4.2 and sensitivity value in section 4.3. Paci *et al*.[11] claimed that risk associated with a threat is given by the probability that a threat occurs and the severity of the threat. Thus, sensitivity was represented as quantifies the cost of the threat, whereas the trust value represented as quantifies the tendency that the threat occurs. Supposedly, higher the sensitivity value, higher the damage to the system. Same as a higher level of insider trust, lower the probability of insider misuse the authorization.

Table 11: Scalar for Risk Value

ID	Risk Value
2	Low
3	Medium
4	High
5	Extreme

RM as shown in Table 12, sensitivity value is depicted in the column of the table, while the trust value is represented in rows. The used to speculate the value of risk is low, moderate, high and extreme and represent as 2, 3, 4 and 5 respectively as shown in Table 12. In addition, Table 13 shows an example result of risk value that was determines using RM based on sensitivity value and trust value. One sample of navigation path was selected. Each document of the path was determined the sensitivity value and developer role is chosen to assign the trust value. Then, risk value for the document of the path navigation is calculated by using RM. After that, the risk of the path navigation is determined based on average of the total document of the path.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 12: Risk Matrix of Document Access

Trust	Sensitivity				
	Very Less Sensitive [1]	Less Sensitive [2]	Neutral [3]	Sensitive [4]	Very Sensitive [5]
Untrusted [2]	M	M	H	H	E
Neutral [3]	L	M	M	H	E
Trusted [4]	L	M	M	M	H
Very Trusted [5]	L	L	M	M	H

Note** L: Low [2], M: Moderate [3], H: High [4], E: Extreme [5]

Table 13: Example of Risk Value Calculation

Role	Developer						Path Risk Average
Path Access	**PY**	**PY1**	**C**	**U**	**R**	**V**	
Sensitivity Value	VLS (1)	VLS (1)	LS (2)	N (3)	VLS (1)	N (3)	
Trust Value	VT (5)	VT (5)	VT (5)	VT (5)	VT (5)	VT (5)	
Risk Value	L (2)	L (2)	L (2)	M (3)	L (2)	M (3)	Low(2)

Note: VLS: Very Less Sensitive [1], LS: Less Sensitive [2], N: Neutral [3], S: Sensitive [4], VS: Very Sensitive [5]

5 RESULT AND ANALYSIS

This section describes the evaluation and analysis regarding insider threat risk profile. The analysis is divided into three sub-sections which are trust scoring analysis, sensitivity value analysis and risky path analysis.

5.1 Analysis on Trust Score

In business system development, certain level of trust is required amongst user roles such as bosses and staff. This is to ensure that security policies are irrefrangible at first place they are not compromised between trust and personal relations. Beside, lack of oversight also can raise the level of a negligent insider risk, such as when a third party uncovers the staff members that had no knowledge of widespread illegal or risky activities. Thus in this study, trust score obtained through a survey answered by the system users (insider) before they start using the system as describe in section 4.2. Figure 6 shows the results of the trust value based on different type of user role. As per stated by Li *et al.*[13] trust management is necessary in order to create stability and flexible access control in a system.

According to a graph of a developer demonstrated that each of criterions in the system is trusted especially in fine tuning server and network. This is because a developer has a high expertise and knowledge regarding overall system including network and server in order to develop a system. Besides, a developer is categorize as a trusted person because of his capabilities to manage the system overall. Neumann [2] stated that in the existing commercial systems, developers and vendors have considerable latitude in making surreptitious system changes if there is any problem and issues of the system. Then, the developer also should have these trusted credentials.

While, refers to graph of system administrator, and shows that his experience in security policy is highest. As an administrator, he should understand more on security policy because any organizational policy is influence and determine employees' course of action [14]. Therefore, result shows that system administrator has a high experience and skill in handling the system because, after system is delivering to the client side, any issue and error is goes to administrator. He is responsible for all upcoming problems. However, system support has a medium skill and experience in system handling and security policy but high skill in solving bug. This shows that, a system support is assigned to test the usability and functionality of the system module. Thus, his expertise is required on development phase and the probability the system is attacked by system support is less and can be overcome because still in development phase.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Next, in end user graph, from the calculation of the trust value, end user tend to the lowest score of skill and experience in which led to a trust value are below optimum which is an untrusted person. It is supported by Stanton *et al*. [4] where he state that end user as an untrusted system because, end user consist of different kinds of behavior different level of education and intention to the system in which might harm to the system. Graph also shows end user has a less skill in computer usage, solving bugs and security policy. This can be proving that, end user mostly is a public users consist of low level education, besides if system is problem, surely they do not has a skill to solved an error.

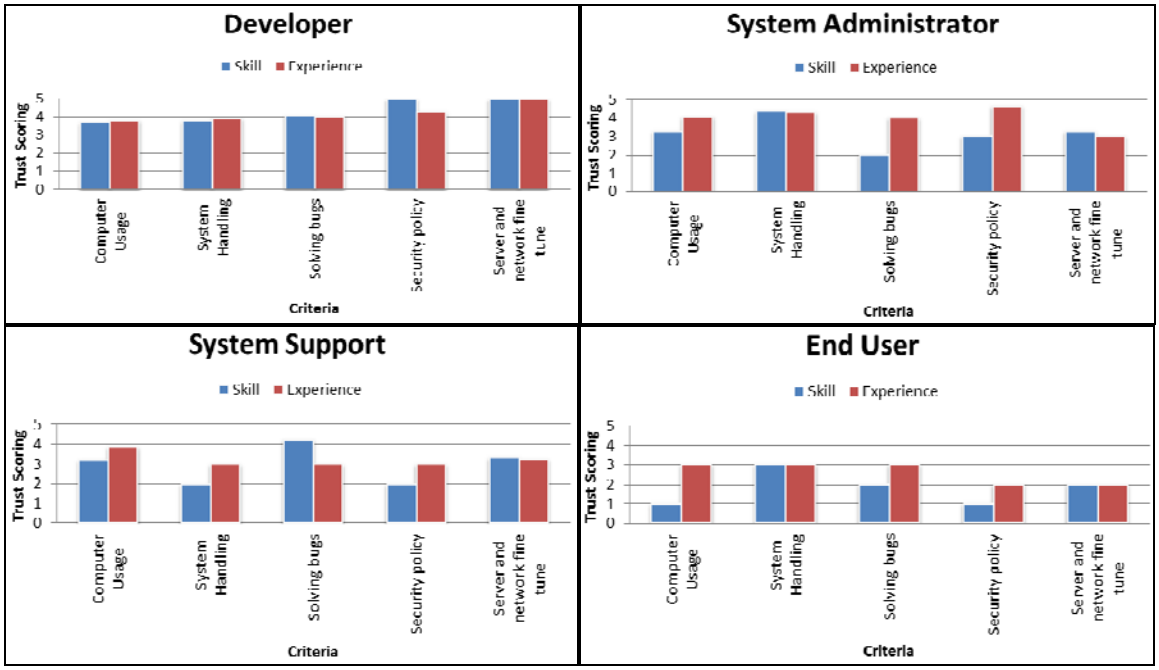

Figure 6: Trust Score based on Role

5.2 Analysis on Sensitivity Value

According to Table 14 shows an example of three document path that was access by different insider. Based on first path, for document C, U, R and V is sensitive or has high level accessibility for system support and end user. While for developer and system administrator to access to the document is less sensitive. However, on path second shows the ability for developer, system administrator and system support to achieve the document is neutral, very sensitive and sensitive respectively. This is show that different weighted is given to different role. This is because, if the same sensitivity or weightage of document is assigned for each role, will help an insider easily access to those document.

5.3 Analysis on Risk Value

Risk value can be determined in different method or technique. For example, method that was proposed by Althebyan and Panda [10]where they do not consider trust value into their proposed method. Their risk value calculation is using graph tree and the value is depending on the document weightage and using a formula to get the value. However, in our method is also considered a graph tree to determine the path navigation. Then, trust value was added in this proposed method where the value of trust is retrieving from self-input survey that insider has been key-in. The trust value is retrieved from the value of skill and experience of the system user. Thus, the same case study has been applied for both methods in order to compare the result obtained. Table 15 shows the differences of risk value for both methods.

As per illustrated in the table below, a developer and system support showed no significant differences risk value between these two methods. However, the difference occurs only on

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

path 6 and 8. This difference is due to the value of document weightage that has been assigned for insider being accessed is too sensitive. Besides that, the major difference is on system administrator and end user. The differences risk value shows the increment in this study compare to method by Althebyan and Panda [10]. Even though the difference is small and has an increment, it proved that trust value that was added in this study is to help to improve the risk value for each document path that is being accessed by different roles.

The benefit of added trust value that proposed by this study is where it assists system owner to determine the risk of the confidential document or information if it was accessed by internal users. Besides, as per stated by Paci *et al*. [11] that insider threat can be identified using the advantages of level of trust associated with the permissions granted to the insider, as well as the sensitivity of the document to which access is granted. The risk value later on will be used to calculate an insider threat prediction in this system using a real data.

Table 14: Sensitivity Value Based on Number of Accessed

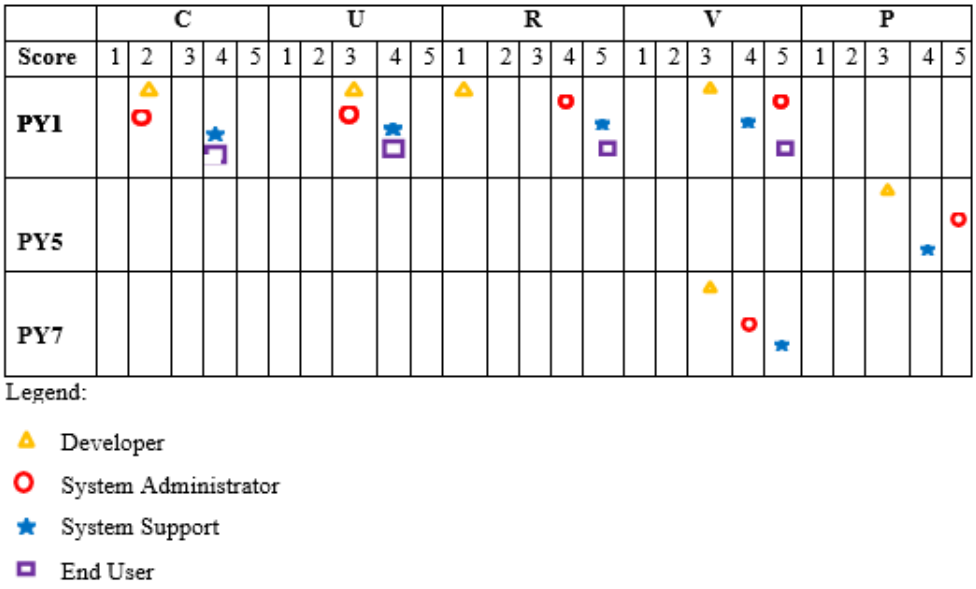

Table 15: Risk Value

Roles	Path	Risk Value	
		Risk Value without Trust [10]	Risk Value with Trust (This Study)
Developer	PY, PY1, PY2, PY3, PY4, PY5, PY6, PY7	Low	Low
	PY, PY1, C, U, R, V	Low	Low
	PY, PY2, C, U, R, V	Low	Low
	PY, PY3, C, U, R, V	Low	Low
	PY, PY4, C, U, R, V	Low	Low
	PY, PY5, P	Low	Moderate
	PY, PY6, C, U, R, V	Low	Low
	PY, PY7, V	Low	Moderate
System Administrator	PY, PY1, PY2, PY3, PY4, PY5, PY6, PY7	Low	Low
	PY, PY1, C, U, R, V	Low	Moderate
	PY, PY2, C, U, R, V	Low	Moderate
	PY, PY3, C, U, R, V	Low	Moderate
	PY, PY4, C, U, R, V	Low	Moderate
	PY, PY5, P	Low	High
	PY, PY6, C, U, R, V	Low	Moderate
	PY, PY7, V	Low	High
System Support	PY, PY1, PY2, PY3, PY4, PY5, PY6, PY7	Low	Low
	PY, PY1, C, U, R, V	Moderate	Moderate
	PY, PY2, C, U, R, V	Moderate	Moderate
	PY, PY3, C, U, R, V	Moderate	Moderate

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Roles	Path	Risk Value	
		Risk Value without Trust [10]	Risk Value with Trust (This Study)
	PY, PY4, C, U, R, V	Moderate	Moderate
	PY, PY5, P	Moderate	High
	PY, PY6, C, U, R, V	Moderate	Moderate
	PY, PY7, V	Moderate	High
End User	PY, PY1, PY2, PY3, PY4, PY5, PY6, PY7	Low	Moderate
	PY, PY1, C, U, R, V	Moderate	High
	PY, PY2, C, U, R, V	Moderate	High
	PY, PY3, C, U, R, V	Moderate	High
	PY, PY4, C, U, R, V	Moderate	High
	PY, PY5, P	Moderate	Extreme
	PY, PY6, C, U, R, V	Moderate	High
	PY, PY7, V	Moderate	Extreme

6 CONCLUSION

As a conclusion, we introduce an insider risk profile matrix in which able to quantify risk value of insider threat prediction framework. This new insider risk profile was proposed whereby as improvements of the framework by considering trust value of system user. The trust value is obtained by carrying out a survey based on the experience and skill of system users. The enhancement of this framework is on the (i) identify insider trust threat profile, (ii) calculation trust value and (iii) calculation of risk. Each insider possesses a different trust profile. The profile that was selected in this study is insider skill and experience.

7 ACKNOWLEDGEMENT

This research was funded by GUP UTM grant, Vot No: 11H84. Also many thanks to collaborative sponsor which are GATES Scholars Foundation of GATES IT Solution Sdn. Bhd. Company, MyMaster Scholarship of the Ministry of Education Malaysia.

REFRENCES:

[1] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," in *Journal of Computer and System Sciences*, 2014, vol. 80, no. 5, pp. 973–993.

[2] P. G. Neumann, "Combatting insider threats," *Adv. Inf. Secur.*, vol. 49, pp. 17–44, 2010.

[3] I. J. Martinez-moyano, E. Rich, S. Conrad, D. F. Andersen, and T. R. Stewart, "A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach," *ACM Trans. Model. Comput. Simul.*, vol. 18, no. 7, 2008.

[4] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers and Security*, vol. 24, no. 2. pp. 124–133, 2005.

[5] Q. Yaseen and B. Panda, "Predicting and preventing insider threat in relational database systems," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6033 LNCS, pp. 368–383.

[6] Q. Yaseen and B. Panda, "Insider threat mitigation: Preventing unauthorized knowledge acquisition," *Int. J. Inf. Secur.*, vol. 11, no. 4, pp. 269–280, 2012.

[7] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, "An Insider Threat Prediction Model," *Trust. Priv. Secur. Digit. Bus.*, vol. 6264, pp. 26–37, 2010.

[8] A. Sengupta, C. Mazumdar, and A. Bagchi, "A formal methodology for detection of vulnerabilities in an enterprise information system," in *Post-Proceedings of the 4th International Conference on Risks and Security of Internet and Systems, CRiSIS 2009*, 2009, pp. 74–81.

[9] G. B. Magklaras and S. M. Furnell, "A preliminary model of end user sophistication for insider threat prediction in IT systems," *Comput. Secur.*, vol. 24, no. 5, pp. 371–380, Aug. 2005.

[10] Q. Althebyan and B. Panda, "A knowledge-base model for insider threat prediction," in *Proceedings of the 2007 IEEE Workshop on Information Assurance, IAW*, 2007, pp. 239–246.

[11] F. Paci, C. Fernandez-Gago, and F.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Moyano, "Detecting insider threats: A trust-aware framework," in *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, 2013, pp. 121–130.

[12] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Robust and scalable trust management for collaborative intrusion detection," in *2009 IFIP/IEEE International Symposium on Integrated Network Management, IM 2009*, 2009, pp. 33–40.

[13] W. Li, B. Panda, and Q. Yaseen, "Malicious Users' Transactions: Tackling Insider Threat," Springer, Berlin, Heidelberg, 2012, pp. 211–222.

[14] T. Herath and H. R. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, May 2009.