Journal of Engineering and Applied Sciences 12 (3): 722-733, 2017
ISSN: 1816-949X

Context-Aware Security Policies: Model for Anti-Counterfeiting in RFID-Enabled Supply Chain Management (SCM)

Irene Anastasia Patric and Manmeet Mahinderjit Singh
School of Computer Sciences, Universiti Sains Malaysia (USM), 11800 Penang, Malaysia

Abstract: Radio Frequency Identification (RFID) applications bring a lot of benefits in Supply Chain Management (SCM). However, RFID still faces several challenges and issues while implementing and evaluating in Supply Chain Management technologies. Due to security concerns, the SCM data are exposed to active and passive attacks that lead to counterfeiting attacks: fraud and cloned attacks. For an organization data most treasured assets, information sharing between different companies become an issue. This is because different organizations have different role and responsibilities in data management and security policies in their environment. We propose testing and evaluating techniques for access control model policies. Based on findings, we have chosen Role Base Access Control (RBAC) most suitable candidate for an access control model. Furthermore, we have implemented RBAC and Event Condition Action (ECA) to context-aware security policy based RFID SCM in order to tackle counterfeiting attacks. The findings suggest the generation of five main security policies model in thwarting counterfeiting for any RFID-enabled supply chain.

Key words: Counterfeiting, Radio Frequency Identification (RFID), Supply Chain Management (SCM), access control, context aware policies

INTRODUCTION

Radio Frequency Identification (RFID) is one of most inspiring technology that has been used in the past few years. The main objective of this technology to tracks and identify the objects that attached with tags. In general, RFID systems consist of an antenna, tag and reader. In the past few year companies are incorporating RFID technologies in their system or services since it provides advantages in SCM. It makes the supply chain more precise and improves the efficiency and reliability of the entire chain.

RFID in supply chain management faces various challenges in term of security privacy issues, hardware and technology. The main concern is how the organization or companies is able to communicate and share protected data from unauthorized information leak. This is because different organization adopt different data managements and security policies within their own environment. In addition; the process in transferring of ownership between multiple supply chain partners and the existence of multiple roles and responsibilities in a single supply chain site need to be carefully designed and planned. This is because the occurrence of information leakage due to unprotected sharing. For instance, an employee without appropriate rights of responsibility is able to retrieve information share within or between the sites for their own unethical purpose.

In SCM; counterfeiting attacks deriving from fraud and tag cloning causes the loss of money and time in detecting the illegitimate tags. The reason why the counterfeiting attack occurs is due to the nature of the tags and the architecture of the supply chain which eliminate the sharing of sensitive information. The passive tag is the lack of any security measurement due to the space limitation. For example, RFID tag not embedded in products where it can easily remove from product and attached to another one (switching the price tag). A thief can switch tag form expensive product with cheaper one and pay less. Similarly; the architecture of the supply chain partners having different data management protocols and software makes it hard to detect the tag counterfeiting within the site. The current technique uses the Intrusion Detection System (IDS) to detect any form of attacks have been proposed. However, IDS causes extra infrastructure; manpower and frequent updating of engine which can be troublesome and can be costly. Thus, the need to plan a complete security policy of access control for all the supply chain partners which allow sharing without any attempt of malicious attack in

Corresponding Author: Irene Anastasia Patric, School of Computer Sciences, Universiti Sains Malaysia (USM), 11800 Penang, Malaysia

leakage of data is needed. As the importance of supply chain involves context parameters such as time, location, user-identity, event behaviors; it is important for us to propose the concept of context-based security policies access control in RFID supply chain management to solve this issue.

The main objectives of the study are to evaluates existing access control security policies based on the context in RFID based supply chain management and to propose a context based access control security policies in RFID enabled supply chain management. This research is focusing on RFID enabled supply chain management based on context-aware security policies. RFID Supply Chain Management (SCM) concepts are used as context-aware systems. This research is started developing a framework that can explore application or services in RFID supply chain management. The research scope to study the possible security threats and challenges that can occur in RFID SCM. This research is important since RFID technology has been used in every sector. Same concepts being used in supply chain management where RFID technology implemented so that it give benefits to the companies. One of important features today's is to protect their resources against unauthorized disclose and changes. Companies or organization has their own access control and security policies. This security policies are able to detect event that occurs to access to the system. This policy and model for access control should provide flexibility to authorized users to use whenever needed, at the same time control the data flows.

Literature review

Security attacks in RFID and SCM: RFID systems are vulnerable to attack and can be compromised at various stages of their use. Attacks against a RFID system can be categorized into four major groups: authenticity, integrity, confidentiality and availability. Besides being vulnerable to common attacks such as eavesdropping, man-in-the-middle and denial of service. RFID technology is, in particular, susceptible to spoofing and power attacks. Figure 1 shows attacks that happen in RFID SCM.

Figure 1 explain that there is two type of loop in categorization concern. First closed loop that happens in a single organization and open loop happen in multiple organizations. There are many type attacks occur during the data transfer example eavesdropping, physical attacks and skimming can cause information leakage. The occurrence of these attacks causes financial loss and lack of trust among business partners.Man in the middle attacks, steal information happen when unauthorized party impersonates as a real reader and communicate with tags. The RFID reader and tag are falsely pretending to be the authentic reader or tag that lead to attacks happen. For example, eavesdropping attack which

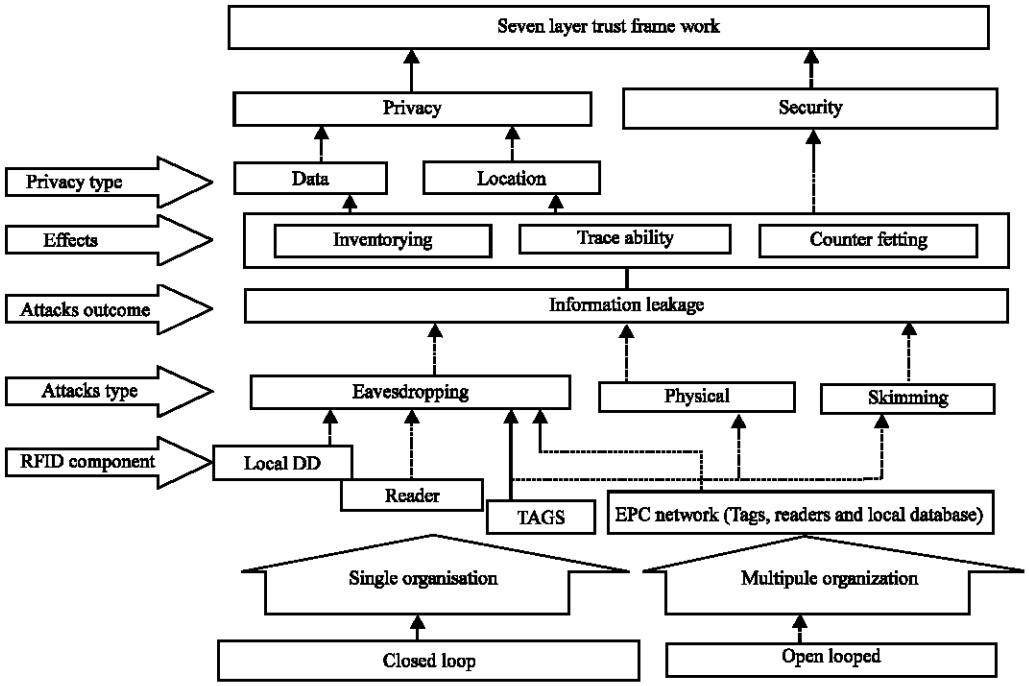


Fig. 1: RFID privacy concerns categorization

happens during transmission between tag and reader, the attacker sniffs the data during transfer of data.

RFID counterfeiting: RFID counterfeiting attacks can be categorized into two which clone and fraud. Counterfeiting makes an organization loss intern of financial, less trust and confidence to implement the RFID in their services.

Fraud attacks create fake RFID tags not exist in database and cloning attacks refer to copying same identification number into empty tags. Lack of technology hardware storage and memory makes the systems not able provide higher security capabilities. The absence of trustworthiness between partners in SC has caused problems such as counterfeiting issues. The researcher used data mining approaches such as classification and clustering methods in detecting RFID counterfeiting attacks in SC.

The researchers design an RFID-enabled supply chain simulator to generate data that able to track and trace the movements of RFID tagged items in the supply chain from manufacturer to distributor and then to the retailer. To generate the dataset techniques Monte Carlo and using that dataset for counterfeiting attacks. In order to protect against counterfeiting, verification needs to be done whether the product is authenticated or not. There are two important components that need secure: physical protection and cryptography protection. Example the digital signature and fingerprints. The scenario of counterfeiting attack.

About 1000 cases of wines with each case containing 100 bottles was produced by Bordeaux. The cases are then sent to the distributor. An employee named Bob from distributor steals information EPC information of 100 wine cases and send it to Carol, the attacker. Then Carol copies the EPC tag numbers into empty tags and tags, fake cases of wines. These wines are later shipped to different retailers within the country.

Reagan corp, a shipping company, is plotting to steal a bulk load of wines during transporting. Each wine has attached with passive RFID tags. Reagan creates fake cheaper wine bottles and clones the associated passive EPC tags. Reagan exchanges the fake wine bottles with real ones. An unknown reader belonging to Carol (an attacker) was placed in the warehouse belonging to Alice.

When the Cabernet Sauvignon wines transported by Suiko Corp reached the warehouse, Carol eavesdrops on the communication channel, actively performs a man in the middle attack and records messages exchanged between the genuine reader and the trusted local database. Carol's reader communicates with the database based on encrypted EPC data. Database side no authenticated needed for the reader, the encrypted key is exchanged by the database.

Carol now uses this received key information and execute a brute force attack on other EPC tags tagged on the cases. This attack able to reveal the key used for all the EPC tags scanned. Carol now sells this information to Alex, Alice's competitor who insert the data into cloned EPC tags and tags them on to cheaper goods and sends the goods to other retailers.

The second method which is data mining technique: Data mining is a process of analyzing data, by molding the data and summarize it into useful information. Alerts that produces by IDS contain attributes and data not detection of counterfeiting. System administrator able to determine the relationship between alert data attributes like Time To Live (TTL) and also flow of RFID tag movement in SCM. This technique able to detect whether counterfeiting occurs or not. There is two type of data mining that is classification and clustering.

Context-aware computing: Context is any information that able to detect and adapt the changes environment where it characterizes the situation of entity. Time, location, activity and behavior are context that used by researchers (Dey *et al*., 2001). A system is context aware if it able to interact to context information and react accordingly on current situation. This condition events are known as context. The term context-aware was used by Schilit and Theimer which define a context-aware systems as one that can adapt according to its context. Context user as the user's emotional state, focus of attention, location and orientation, date and time, objects and people in the user's environment (Dey *et al*, 1998). Schilit claim that the important aspects of context are: where the user is, who the user is with and what resources are nearby. They define context to be the constantly changing execution environment: Computing environment, user environment and physical environment. Context created by using 'five W's: who (identity of users what (what is work) when (time information) where (location of information) and why (user's preferences) (Hong *et al*., 2009). There is a great division among context-aware researchers as to whether context should only include automatically acquired information, or both manually and automatically acquired information (Dey *et al*., 2001). Context can define many different ways. There are four types of context: identity, location, time and activity (Dey *et al*., 2001). Active badge location system which is considered to be one of the first context-aware applications

Table 1: Comparison chart of access control methods

Models	DAC	MAC	RBAC	ABAC	Clark-wilson
Advantage	The owner of the file who controls other user's accesses to the file-flexible (government and commercial)	Access control policy decisions are made by a central authority not by object owner Implement military sector System must enforce the protection decision No read up and no write down (Bell-La Padula confidentiality) Biba (integrity)	Encapsulates privileges into roles and user are assigned to role which make simple Reflected on the permissions available if there is changes in a role	More flexible Commercial RBAC intern of contexual attributes	Used to protect commercial information Different approach to ensure data integrity
Disadvantage	Two weakness Granting user read access is transtive Vulnerable to Trojan horse attacks (programs inherit the identity of the invoking user)	Restriction on user access The oprating sysytem and associated utilizes outside the access control framwork	Authorization complex as decision may depend on context Permission are specified in term of object identifier	More complax then RBAC intern policy review analysing reviewing or changing are difficult task	Nill

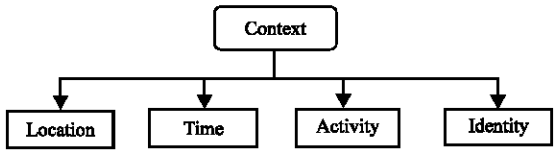


Fig. 2: Sensor-based context parameters

System is about how to determine user's current location via telephone that close to user by infrared technology.

Figure 2 shows parameters of contexts. Location and time have been used in RFID-enabled supply chain in EPC global network as context. Whenever, products with tag move from one place to another place there will changes in term context such as time and location.

Security policy model and authorization: One of most important features of today's technology is protect or secure their resources (data or services) against unauthorized persons, alteration and accessibility when the resources needed by authorized user (Ausanka-Crues, 2001). Security policy is set of rules that used by company information security. The security policy identify assets that need to protected in system and control flow of access (Belokosztolszki, 2004). In context e-services system, security policies should adapts context users, location, application and resources. In context of e-service system, security policies should adapt adopt behavior based on user context, location, application and resources (Hwang *et al*., 2009). To provide security, two conditions should be satisfied; first language for express policies based on standard technologies and secondly the protocol to dispatch security policies on based technologies (Hwang *et al*., 2009). Access control are used as security mechanisms. Access control is mechanism which control users or processes access the resources in the system. Access control services provided by systems should be flexible and expensive so that it able fit or fulfill all requirements. This is because different organization, users have different roles and responsibilities. Early methods to authorization specification can be associated with the conditions. Conditions refer to whether the content of the objects can be access or no. Another features refers users of group example employees, consultants, administration. Access depends on hierarchy where only group of set privileges "write privileges". There are several existing access control mechanism different in technology, complexity and infrastructure and so on (Table 1).

MATERIALS AND METHODS

This proposed research can be summarized into five steps (as shown in Fig. 3):

Step 1 (Investigation problem): In this phase where the problem statement is defined. The current security issues that happen in RFID supply chain management are identified and investigated through literature review. Access control and security models are compared and choose suitable for the experiment.

Step 2 (Design): Based on literature review we choose three suitable access model and security model. Testing the model by creating policies based RFID SCM. Access Control Policy Testing (ACPT) tools are used to create and verifies the policies. Three access control selected that are RBAC, ABAC and MAC.

Step 3 (Choose best model): Based on the result of verification and testing evaluate the result, choose

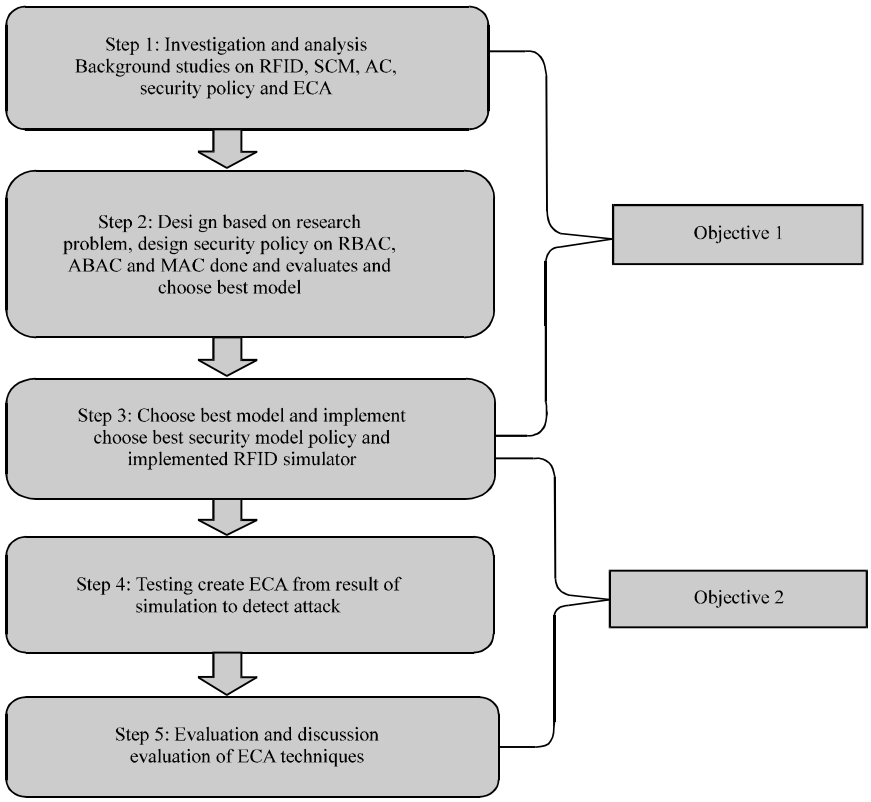


Fig. 3: Research framework

which model show the best result for this research to be implemented on RFID SCM Simulator.

Step 4 (Testing): This phase the simulation RFID SCM Simulator. Generate RFID dataset using Monte Carlo method.

Step 5 (Evaluation and Discussion): Based on result, data is validated to ensure the correctness of policies. Access control model will be evaluated using security metric. Figure 4 shows that the Monte Carlo algorithm that used in this research to generate datasets and to calculate reader ID, timestamp and EPC of cloned tag.

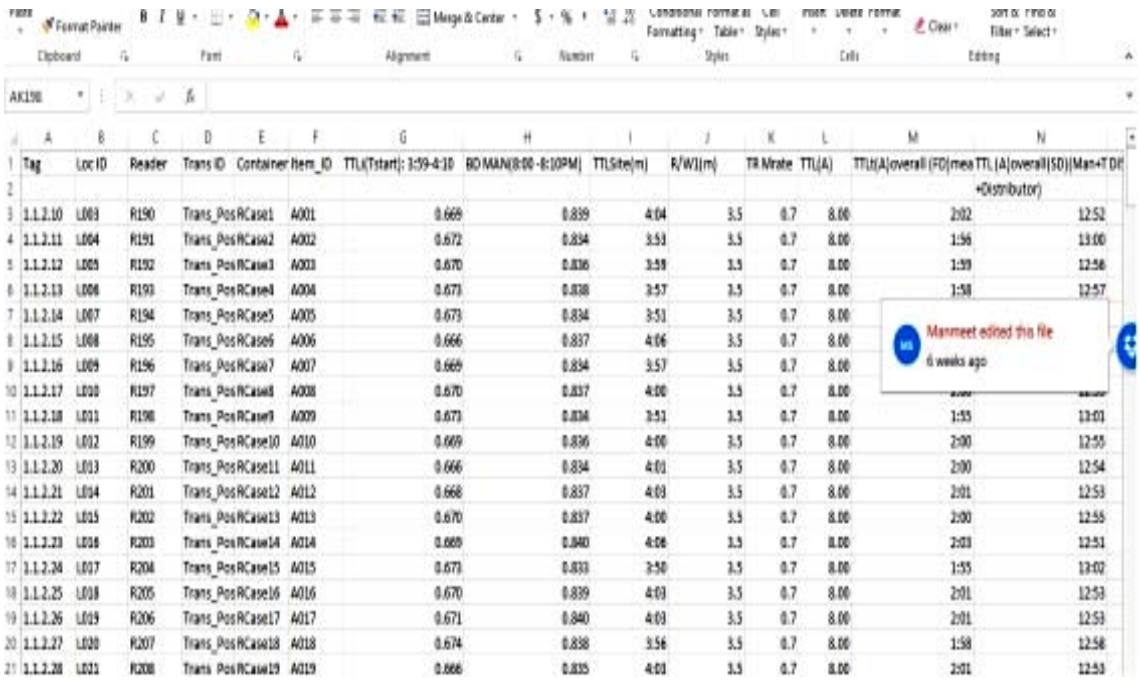
Proposed security model for anti-counterfeiting in SCM: Access Control Policy Testing (ACPT) tool: ACPT is a tool developed by the computer security division of National Institute of Standards and Technology (NIST) and North Carolina State University. This tool makes sure the modeling and verification of access control policy based on access control mechanism in the correct manner. ACPT consists four components that are policy modeling, static verification, dynamic verification and policy implementation. The policy code generation in ACPT enables the access control policies to be converted into a declarative and enforceable policy language known as the eXtensible Access Control Markup Language (XACML).

Policy modeling: ACPT allows researchers to create policies based on access control model example RBAC and Multi-level security. This tool has some features which author policy able to edit, add and delete policies and attributes.

Static verification: These components provide static verification whether it able satisfies its properties.

Dynamic verification: Testing process to ensure policies implementation with test input its request service.

Policy implementation: ACPT will be implemented using JAVA and it able to provide Windows GUI-based tools features. Figure 5 shows that in ACPT, there is several access control model templates which can be used with combine policies such as multi-level, workflow and ABAC. This ACPT tool contains four important functions that subject, object, action, resources.



Tag	Loc ID	Reader	Trans ID	Container	Item_ID	TTL(Tstart): 3:59-4:10	BD MAN(8:00 -8:10PM)	TTLSite(m)	R/W1(m)	TR Mrate	TTL(A)	TTLt(A)overall (FD(mea	TTL (A)overall(SD)(Man+T Dif
												+Distributor)	
1.1.2.10	L003	R190	Trans_PosRCase1		A001	0.669	0.839	4:04	3.5	0.7	8.00	2:02	12:52
1.1.2.11	L004	R191	Trans_PosRCase2		A002	0.672	0.834	3:53	3.5	0.7	8.00	1:56	13:00
1.1.2.12	L005	R192	Trans_PosRCase3		A003	0.670	0.836	3:59	3.5	0.7	8.00	1:59	12:56
1.1.2.13	L006	R193	Trans_PosRCase4		A004	0.673	0.838	3:57	3.5	0.7	8.00	1:58	12:57
1.1.2.14	L007	R194	Trans_PosRCase5		A005	0.673	0.834	3:51	3.5	0.7	8.00		
1.1.2.15	L008	R195	Trans_PosRCase6		A006	0.666	0.837	4:06	3.5	0.7	8.00		
1.1.2.16	L009	R196	Trans_PosRCase7		A007	0.669	0.834	3:57	3.5	0.7	8.00		
1.1.2.17	L010	R197	Trans_PosRCase8		A008	0.670	0.837	4:00	3.5	0.7	8.00		
1.1.2.18	L011	R198	Trans_PosRCase9		A009	0.673	0.834	3:51	3.5	0.7	8.00	1:55	13:01
1.1.2.19	L012	R199	Trans_PosRCase10		A010	0.669	0.836	4:00	3.5	0.7	8.00	2:00	12:55
1.1.2.20	L013	R200	Trans_PosRCase11		A011	0.666	0.834	4:01	3.5	0.7	8.00	2:00	12:54
1.1.2.21	L014	R201	Trans_PosRCase12		A012	0.668	0.837	4:03	3.5	0.7	8.00	2:01	12:53
1.1.2.22	L015	R202	Trans_PosRCase13		A013	0.670	0.837	4:00	3.5	0.7	8.00	2:00	12:55
1.1.2.23	L016	R203	Trans_PosRCase14		A014	0.669	0.840	4:08	3.5	0.7	8.00	2:03	12:51
1.1.2.24	L017	R204	Trans_PosRCase15		A015	0.673	0.833	3:50	3.5	0.7	8.00	1:55	13:02
1.1.2.25	L018	R205	Trans_PosRCase16		A016	0.670	0.839	4:03	3.5	0.7	8.00	2:01	12:53
1.1.2.26	L019	R206	Trans_PosRCase17		A017	0.671	0.840	4:03	3.5	0.7	8.00	2:01	12:53
1.1.2.27	L020	R207	Trans_PosRCase18		A018	0.674	0.838	3:56	3.5	0.7	8.00	1:58	12:58
1.1.2.28	L021	R208	Trans_PosRCase19		A019	0.666	0.835	4:03	3.5	0.7	8.00	2:01	12:53

Manmeet edited this file
6 weeks ago

Fig. 4: Sample of RFID dataset

Fig. 5: ACPT tool framework

RFID SCM dataset and its architecture: There are three methods that can be used to simulate RFID dataset in SCM either manually, using some techniques such as SYSRFID or Monte Carlo method. Manually generate low data cost but its long time to generate a huge volume of datasets. SYSRFID is a tool that can generate a large number of datasets but in the term to process all data it is very expensive. As mention Fig. 5, the Monte Carlo are used for this research as it is able to generate data with random value. It also can be generated by using add-in for Microsoft Excel to generate a real-time dataset. Monte Carlo algorithm calculates the reader ID, timestamp, EPC tag. It consumes less time to generate the RFID dataset and low cost.

This existing architecture (RFID SCM) based on client-server architecture that done by Lim Mei Tin. Client side (administrator, employees from partners) that requests data information via web browsers (Internet

Explorer, Mozilla Firefox). The partners are referred manufacturer, retailer or distributor. While at server side the Apache tomcat and oracle Database (DB) servers. The Oracle database servers act as local Electronic Products Code Information Service (EPC IS) that stores the information. For example, if client's requests for information that stored in Oracle database, the Apache tomcat will process and require from the database. Oracle database will return information to the Apache tomcat server. Last Apache tomcat server will send back the request information to the client. The network plays as a medium for client and server. All data or information that stored in EPC IS will also save to into global EPC IS Discovery Service. The Systems Components for RFID enable SCM. The RFID-enabled supply chain simulator runs either single link or multilink paths.

Performance evaluation: Access policies (AC) policies are high-level requirements that specify how access is managed and who, under what circumstances, may access what information. An example where the subject can access action within the context of an organization that applied on the application, policies, etc. The properties to be evaluated based on National Institute of Standard and Technology Assessment and ACPT tool itself. These are divided into four categories according to an organization's operational needs:

- Administration: properties that in general impact the cost and efficiency of AC system
- Performance: properties that impact performance by adding the rules in addition to the enforcement of the AC system's processes
- Support: properties that are not necessary but that can increase the usability and portability of an AC system

RESULTS AND DISCUSSION

Modelling policies: Several security policies are identified and proposed after thorough literature review and study which are then developed using access control policy specification within ACPT. These policies models are Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) and Mandatory Access Control (MAC). In this study, the process of modeling policies for access control defined.

This study also of explain the concepts of access control connected to ACPT. Figure 6 shows that ACPT uses environment concept that contains a subject, resources and action. Then, it selects specific environment related to model for testing. For example, roles are subject and attribute values; student, doctor, employee. Resources is the information that wants to access example; file, employee record. Action type of access depends on the restriction on system example read and write.

Table 2: Properties and attributes of access control model ABAC policy

Subjects	Attributes	Values attributes
Subject	Emp position organizations	Employee; supervisor; system admin; manufacturer; distributer; retailer
Object	Files	EPC Files; transaction files; process files
Action	Action	View; create; edit; delete
Environment	Is within workings hours Is within working places Is other orgedit Is other org create	True; false

The environment is in the set condition or situation the access will be granted example: working an hour and working place. To set the rules with condition property link selected by add-in dialog box. Verification and test are to check the correctness of policy. ACPT is converted the rule and merged the rules in XACML. Table 2 shows the access control properties and attributes of ABAC.

There two type of subject's attributes that have been used for this research that organizations and Employee Position. Organizations can be categories into three attributes values that are manufacturer, distributor and retailer. Employee position attributes consist employee, supervisor and system admin. The action that been used a view, create, modify and delete. The environment that been used is within working hours. Withinworking place, is other org edit and is other org create

With in working hours: This environment will set that time of working hours of organizations. If the access information happens within hours, then attributes show true and access granted

With in woking place: This environment is organizations places or working places. The access of granting or denied depend on organization depend on limit of employee position

Is othe rorg edit: This environment is about the access that granted or denied if access requested by different organizations. There is a limitation in order the access what of resources.

Is other org view: The environment is about how other organizations creates files to the otherOrganisation resources. There is three type object that used in this SCM environment that EPC, Process and Transaction files.

If subjects want to access an object within working hours in an organization, then environment attributes show true. Subjects from different organizations want to access objects it needs to verify so that environment attributes is other org edit and is other org view permit

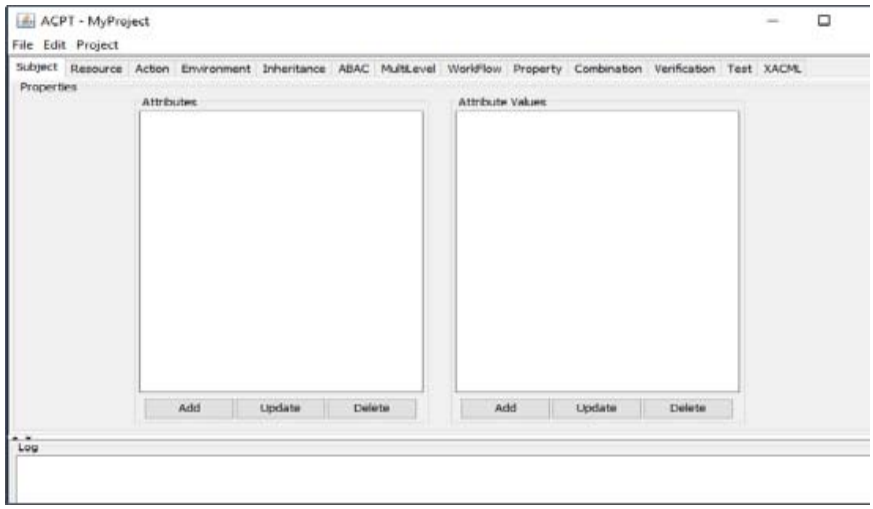


Fig. 6: Framework ACPT tool

operation allowed. Within same organization, both employee and supervisor are allowed view and edit if it is same file management. MAC only can performance two actions that are read and write operations. There is three type of environment that iswith in working hours is With in working place and is trusted source.

Is with in working hours: The subjects are denied access the objects if it does not happen within the working hours that set by the organization. This environment attribute returns true if the access within the range of working hours.

Is with in working place: This environment attribute returns true if within access happen in same organizations. The subjects access to the objects are denied if it happens different organizations with employee position.

Is trusted source and: This environment attribute returns true if the object is from a trusted origin source. Access to the object will be denied if the environment attributes are false depend on user classification and clearances level.

Implementation RBAC and ECA in RFID SCM Simulator: In this section, will use previous research done in (Derakhshan *et al*., 2007), there are four types of attack could happen in RFID SCM that are eavesdropping, skimming, man in the middle and physical attacks.

Counterfeiting: RFID counterfeiting attack can be categorized into two which are clone and fraud. Fraud attack happens when the new duplication tags and contain have electronic product code that not listed on database. For cloning attacks, when there is an empty tag which has same EPC identification number.

Eavesdropping: If tag A and B similar to each other but R/W and TTL are different from the same sites, then eavesdropping attacks occur during process tagging, packaging or shelving.

Man in the middle attack: Man in the middle attack happens when two points communicated each other. Example when an unauthorized person acts as a real reader and communicate to the tags to steal information.

Physical attack: The physical attack occurs when tag information read by the reader, recorded can't be read because of security measurement example encryption. EPC tag A and EPC tag B will have same content within sites SCM because the information hashed.

Figure 7 show the prototype that used in this project, based on this web page there two type of SCM that is single-link and multilink. This simulator generates RFID dataset by using monte carlo method. The users can track the location, process and attacks status of EPC-tagged with items. The active mechanism of the active database is implemented by the definition of active rules and corresponding execution mechanism. The active rule is also called ECA (Event-Condition-Action) rule. A rule with three components that are:

- E-Event-internal or external events can update database operations

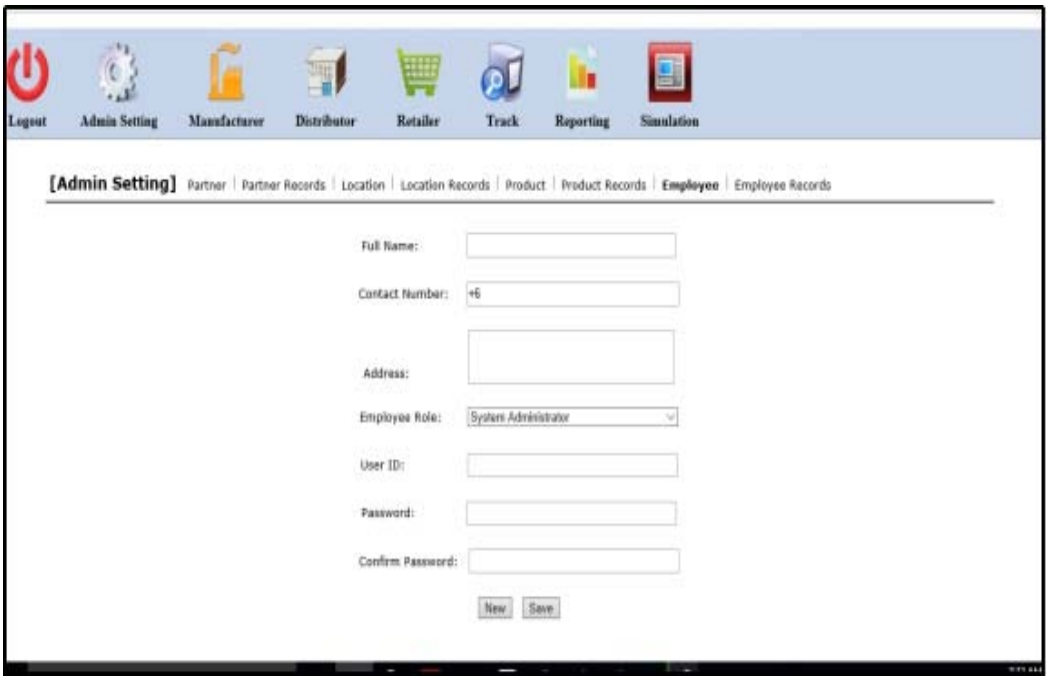


Fig. 7: RFID SCM simulator interface

- C-Condition-rule of action that will declare the situation
- Action- SQL statement that will automatically execute

Algorithm 1: ECA rules syntax example:

CREATE TIGGER <tigger name>
(BEFORE | AFTER)
(INSERT | DELETE | UPDATE [OF <col names>] <on subject table>
[REFRENCING {OLD old-name | NEW new name}]
([FOR EACH (ROW | STATEMENT)}
[WHEN <condition>]
<actions>

Figure 8 output show that decision for this manufacturer rules is pending which show there is an error in term model and properties. Modeling of rules according to properties not establish in the correct manner.

Figure 8 and 9 show the result of three access control models, based on the result the ABAC, RBAC and MAC policy decision deny. All decision show that it deny the access. This is because subject from manufacturer employee does not have permission to access different organization files. The employee does not have permission to read transaction files even though within the same organization. Based on the rule that set for ABAC employee have permission to write or read to process files. RBAC verification of properties shows true which show the correctness of policy for that access control.

Table 3: Metric evaluation for access control security policy

Quality metrics	MAC	RBAC	ABAC
Size of organization	Large	Large	Large
Cost	High	High	High
Complexity	Not complex	Moderate	Complex
Support of separation duty	Least	Most	Significant
Safety	High	High	Low
Flexibility of configuration of existing systems	Low	Most	Most
Degree of privileges support	Least	More	More

Evaluation between MAC vs. RBAC vs. ABAC: In this study, the evaluation done by comparing three type of access control policy with a different metric. Performance metric national institute of standards and technology can be classified into four metrics; administration, performance, support and enforcement (Hu and Kent, 2012). Only two rules of action are used for this section that permits or deny. The correctness of policy is important so that unauthorized agents do not access the resources. The security policy depends on the requirement of subject privileges. Table 3 shows the metrics evaluation for access control security policy.

The policy, not been declared correct policy which related to the model or property. Access to the resources depends on the context where there are selected environment such within working hours and within working place. Both ABAC and RBAC are flexible and scalable. Only different ABAC more advanced or new compared RBAC. RBAC and ABAC can both be used by viewing roles as user attributes. The access control RBAC

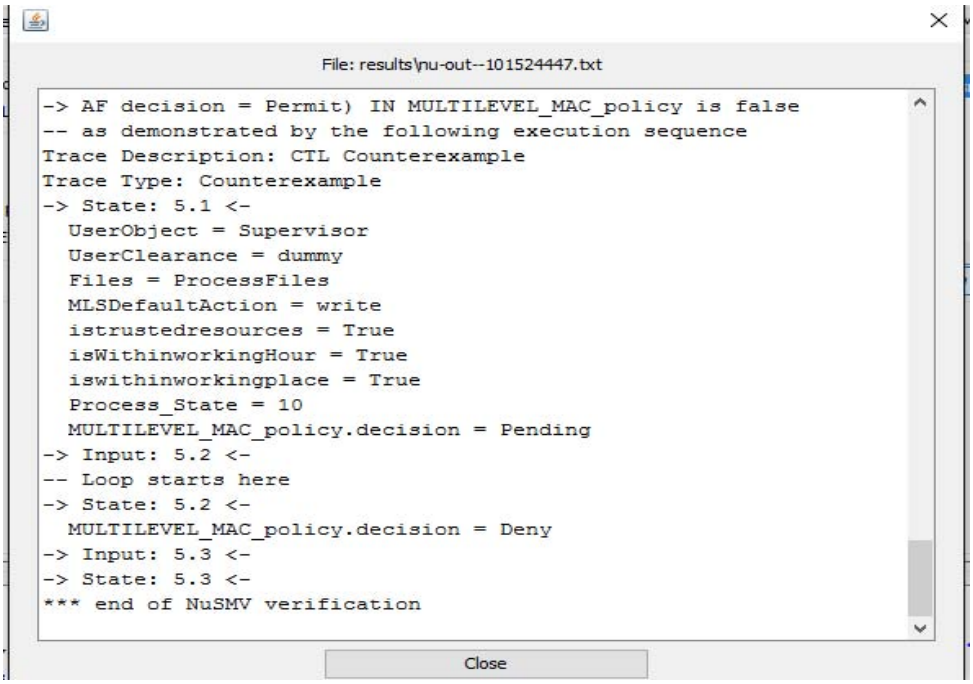


Fig. 8: Result of MAC policy

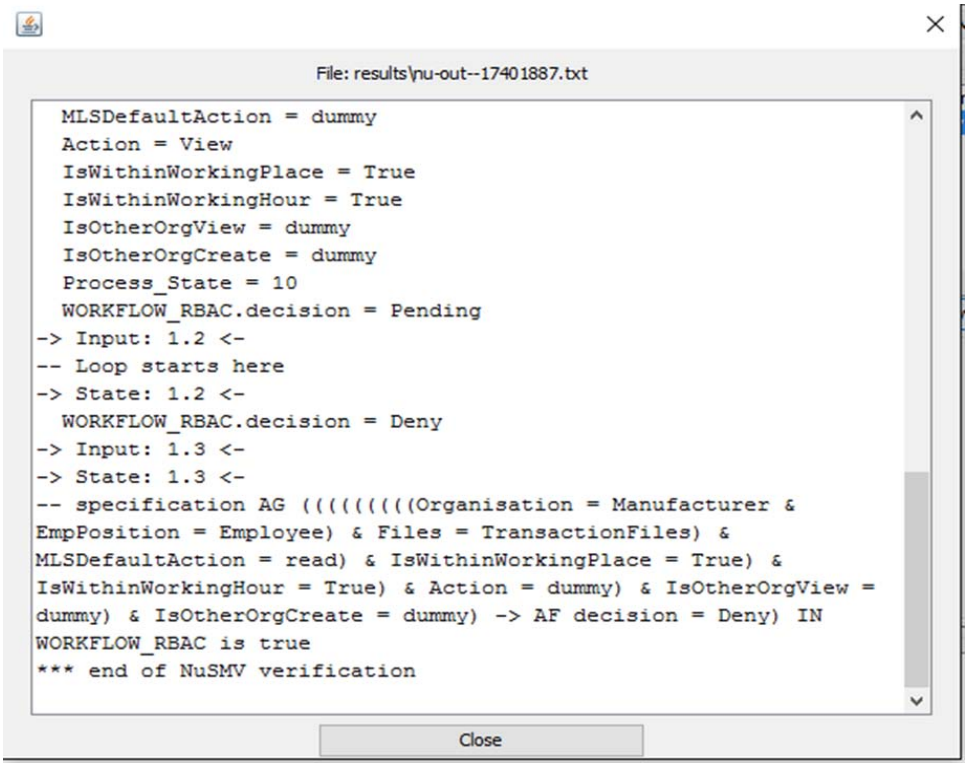


Fig. 9: Result of RBAC policy

Table 4: Proposed security policies model tackling anti-counterfeiting in SCM

Policy model	Context	Description	Who is involve
Intra working limit	Time/User ID	The access the resources within working hour with subject access level	Subject; EmpPosition
Intra working place	Location/User ID	The access within organization with subject access level	Subject: EmpPosition; organisation
Intrapersonal	Location/User ID	The access for the resources iffered organization with subject access level	Subject: EmpPosition; organisation
Interpersonal	Location/User ID	The access based on view and subject level	Subject: EmpPosition; organisation
Intresources	User ID/location	The access to the resources within organization	Subject: EmpPosition; organisation

shows that access for each different organization will deny if it the employee, supervisor and admin system is trying to get permission to access the file in a different organization. To ensure the correctness the policy, the author policy need evaluate the request before deciding the request that needs to add. Role-Based Access Control (RBAC) method can classified users by given roles and privileges in they can access. ABAC does not use roles with permission but role more to attributes. The main aims of ABAC by defining right access to properties of the user in the framework. Lack of flexibility and hard to implement make MAC not implemented by many application. Mostly implemented in military and government that required safety of the document. MAC is immune to Trojan horses attack. Disadvantages of MAC cannot modify the underlying policies and it is difficult for an application to business and financial. ABAC and RBAC almost show a similar result but in term of specifying or adding a new role, RBAC is more suitable. There no need to add or modify policy in order to give permission to perform an action. The test shows that RBAC is best security model that can be implemented in RFID SCM Simulator. Based on ACPT tool we have created a standard policy model for tackling counterfeiting in any Supply Chain Management. This is demonstrated in Table 3.

Based on Table 3, standard policy is created using Environment attributes with the condition of access. There are five policies IntraWorkingLimit, IntraWorkingPlace, IntraPersonal, InterPersonal and IntResources. Three type of context can include categories that are location, user id and time.

CONCLUSION

As mentioned in the introduction, the main aim of this project is to create security policy and verification based on access control. There are three access control techniques that used for this research; Role-based access control (RBAC), Mandatory Access Control (MAC) and Attributes based access control (ABAC). Checking the correctness of security policy in condition and requirement. Error in policy modeling can cause a problem such as authorized agents denied to get access to the resources. All access control have advantages and disadvantages. RBAC are adopted in an administrative environment. The subject will be assigned will role. The duty of separation metric can be used in access control subject can get more than roles to complete the tasks. For example, employees frequently change roles and jobs within an organization and need different access privileges. RBAC are chosen as the best candidate for access control model based on context RFID SCM. Based on the testing and evaluation RBAC in RFID SCM Simulator. Each employee is assigned a role in prototype example administrator, employee and supervisor. Monte Carlo method is used to generate real-time dataset by simulation process. This simulator able to checks whether tags are cloned or fraud. Event Condition Action (ECA) rule are used in the database to detect events that occur, evaluate the condition and if the condition is true, then execute the action. The information flow can track in any sides of SCM. Based on ECA, we able to classified the counterfeiting attacks and create attacks policy. Thus, the main findings of this research is the generation of five policies model which are IntraWorkingLimit, IntraWorkingPlace, IntraPersonal, InterPersonal and IntResources. In future work, classification of attacks rule can enhance that depend on scenario RFID counterfeiting attacks in SCM. Moreover, hybrid access control model can be enhanced to test and evaluate the policies.

ACKNOWLEDGEMENT

This research is supported by the Fundamental Research Grant Scheme (FRGS) [203/PKOMP/6711424] of Universiti Sains Malaysia.

REFERENCES

Ausanka-Crues, R., 2001. Methods for access control: Advances and limitations. Harvey Mudd College, Claremont, California. https://www.cs.hmc.edu/~mike/public_html/courses/security/s06/projects/ryan.pdf.

Belokosztolszki, A., 2004. Role-based access control policy administration. Ph.D Thesis, University of Cambridge, Cambridge, England.

Derakhshan, R., M.E. Orlowska and X. Li, 2007. RFID data management: Challenges and opportunities. Proceedings of the IEEE International Conference on RFID, March 26-28, 2007, Grapevine, TX., USA., pp: 175-182.

Dey, A.K., G.D. Abowd and A. Wood, 1998. CyberDesk: A framework for providing self-integrating context-awareservices. Knowledge Based Syst., 11: 3-13.

Dey, A.K., G.D. Abowd and D. Salber, 2001. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. Human-Comput. Interact., 16: 97-166.

Hong, J.Y., E.H. Suh and S.J. Kim, 2009. Context-aware systems: A literature review and classification. Expert Syst. Appl., 36: 8509-8522.

Hu, V.C. and K.A. Kent, 2012. Guidelines for access control system evaluation metrics. US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, Maryland. https://pdfs.semanticscholar.org/b01a/85f6fb0d3ca85e49955af9d87cea830b55ff.pdf.

Hwang, J., T. Xie and V.C. Hu, 2009. Detection of multiple-duty-related security leakage in access control policies. Proceedings of the 3rd IEEE International Conference on Secure Software Integration and Reliability Improvement, July 8-10, 2009, IEEE, North Carolina, USA., ISBN: 978-0-7695-3758-0, pp: 65-74.