International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 4, Jul-Aug 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Enhanced Security Model for Information and Online Transaction Processing System Using Mandatory Access Control (MAC) Mechanism

Enukpere, Victor Efe; Oweh Victor

Computer Engineering, Delta State Polytechnic Otefe Oghara, Delta, Nigeria

ABSTRACT

This research presents a set of patterns appropriate for securing information in an online transaction processing system. The research also shows how security constraints can be added to the domain model by using mandatory access control (MAC). The system developed created three different access levels which include e-platform administrator, the payment gateway administrator and the customers. Each of the users on the platform has limited access areas and this was achieved by applying mandatory access control technique. Security constraints were added to each of the component patterns to produce a domain model for secure e-commerce. The research utilized a security feature called Role-Based Access Control (RBAC). In the RBAC pattern, users are assigned to the roles according to their tasks or jobs and rights are assigned to the roles. In this way, a need-to-know policy can be applied, where roles get only the rights they need to perform their tasks. The software developed utilized the mandatory access control (MAC) as a security mechanism for the online transaction processing which involves product ordering, payment using credit card, and product information management. The system is very robust and MySQL database was used at the back-end.

KEYWORDS: *Administrator, Cybersecurity, Subsystem, Domain Model*

How to cite this paper: Enukpere, Victor Efe | Oweh Victor "Enhanced Security Model for Information and Online Transaction Processing System Using Mandatory Access Control (MAC) Mechanism" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-4, August 2024, pp.37-46, URL: www.ijtsrd.com/papers/ijtsrd67119.pdf

IJTSRD67119

1. INTRODUCTION

Nigeria is turning to broadband internet connectivity as the next frontier to be conquered. With penetration presently at about six percent, the Nigeria Communications Commission (NCC), has sent out an ambitious broadband master plan to achieve a 30 percent penetration by 2025. This increase of activity in the cyber space of Nigeria has led to a corresponding increase in electronic fraud and cyber-attacks. Likewise, an upsurge in the deployment of e-products by Nigerian banks has also led to a surge in e-fraud. About four billion naira was allegedly lost by Nigerian banks to e-fraud in 2015 (Agbo, 2016).

To keep pace and stay ahead of escalating risks, organizations need to rethink their system security postures in the context of a broader risk management strategy and adopt a more stringent approach to system security (Chen *et.al*, 2016).

While traditional information security has always included practice areas related to the security of information and systems, the cyber world has become increasingly connected and porous to the activities of hackers (Allan, 2015).

Most organizations face the challenge of determining how to embrace disruptive technologies and trends such as “everything connected”, mobile, social, cloud computing while also managing the risks that conducting business on the cyberspace poses (Burden & Palmer, 2014).

This motivates the development of a system which can ensure its own security. This self-defending system could be configured to provide and maintain adequate security by itself without any intervention from the system administrator. When an attack is detected or any security breach is suspected, the system should be able to adjust its configuration to defend against such an attack by increasing its logging and shutting down services until the threat has passed (McLean, 2010).

A true self-defending system should be able to protect itself against both internal and external threats which are feature that many operating systems lack due to the fact that they do not possess the mechanism needed to completely monitor and control all aspect of their operations. However, with Security Enhanced Windows and other operating systems that employ the Mandatory Access Control (MAC), it is possible to design systems that are more configurable from a security standpoint. These security conscious systems, coupled with an agent program capable of making informed security decisions, provide a solid foundation for self-defending systems (Rosenquist, 2015).

In this research, an enhanced security model for information and online transaction processing system is being develop using mandatory access control (MAC) mechanism and the model is user-friendly.

2. Literature Review

Over the last few years, researchers have carried out researches to identify the best approach to providing adequate security of information systems, some of these researchers includes:

Li, *et.al* (2016) studied the cybersecurity vulnerabilities of traffic light systems as well as the corresponding defensive measures against the existing and potential cyberattacks. The study provided a general bi-level optimization-based framework for assessing the cybersecurity risks of traffic light systems in terms of the physical implications on traffic networks. The study further developed a minimax-regret-based approach to prioritising defensive measures for mitigating cybersecurity risks in traffic light systems; the approach ensures desired traffic management performance under various network conditions. The pitfall in this study is that it failed to take cognizance of the cyber security needs of networked computer systems as a hybrid framework of interaction between humans and computers, where security and privacy policies play a crucial role.

Oltramari, *et.al* (2016) examined the theory and practice of cyber security, and evaluated whether there are underlying fundamental principles that would make it possible to adopting a more scientific approach. They concluded that the most important requirement would be the construction of a common language and a set of basic concepts about which the security community can develop a shared understanding. "A common language and agreed-upon experimental protocols will facilitate the testing of hypotheses and validation of concepts".

The need for controlled vocabularies and ontologies to make progress toward a science of cyber security was recognized as well. In this domain, ontologies would include the classification of cyber attacks, cyber incidents, and malicious and impacted software programs. From our point of view, where the human component of cyber security is also essential, the analysis needs to be expanded to the different roles that attackers, users, defenders and policies play in the context of cyber security, the different tasks that the members of a team are assigned to by the team leader, and the knowledge, skills and abilities needed to fulfill them.

Liang, *et.al* (2017) investigated the security of virtual working on cloud computing platforms. The target of this investigation was to propose a novel solution as a security service on cloud computing platform to protect virtual working with on-demand virtual private network (VPN) as well as transparent encryption. Based on transparent encryption for all user data, the solution uses authentication cloud, relay cloud and storage cloud to set up security architecture for the virtual working. FSFD based technology was used to perform the transparent encryption and the combination of authentication cloud and relay cloud was used to set up VPN tunnel for the virtual working solution. However, the shortcoming in this study is the development of systems with several different technologies which can actually cause an increase in complexity.

Onyesolu, *et.al* (2012) developed a fingerprint mechanism as a biometric measure to enhance e-banking security in Nigeria. The prototype of the developed application was found promising on the account of its sensitivity to the recognition of the customers' fingerprint as contained in the database. The researchers concluded that when the system is fully deployed only the registered owner of a card can access the bank account thereby reducing the rate of fraudulent activities on the ATM machines. The drawback of this system is that it did not incorporate other platforms of e-banking such as individuals using a networked computer to transfer money from one account to the other.

From the forgoing, it is obvious that none of the authors considered developing a system that would resist suspicious activities by making autonomic decision(s) based on in-built policies thereby enhancing the security of the system as well as make the user feel protected. Basically, policy-based systems were designed to support run-time reconfiguration ability of systems decision-making logic. Policy-based computing describes a methodology for embedding dynamic behavior into software components and this makes them more reliable. Thus, an enhanced security model that

implements MAC mechanism was proposed, where customers on e-commerce platforms are granted access/privilege based on pre-defined policies before they can make successful transaction(s) on the platform.

3. Analysis of the New System

In the new system only certified sellers and buyers can participate, this will ensure the security because only legitimate users will be able to take part in the online electronic transactions. Sellers and buyers will be certified by the certifying authority. Certifying authority will certify the user while the user may be seller or buyer that wants to get certified, and hence participate in the transactions. The username or passwords which the buyer enters may be credit card number or online banking username and password and this should be secure and no one else should be able to read the sensitive information hence a multiple encryption scheme will be used for the security of information. The hacking or attacks on the e-commerce application and the sensitive information sent over the network through the modules of the proposed system was also checked. There are four modules in the proposed system and they are stated as follows:

A. Certification of Entities Participating in online Electronic Transaction;
B. Encryption of Sensitive Information Using Multiple Encryption Scheme;
C. Checking for the hacking or attacking on application and sensitive information sent over insecure channel and;
D. Defense Mechanism used for the attack on web application.

At the conceptual level, a database that contains data labeled over a set of sensitivity levels has relations that may contain data labeled over this same set of sensitivity levels. These multilevel relations are decomposed into single -level or system-high fragments. The multilevel secure DBMS stores the fragments within physically separate single -level objects. Then, the MLS DBMS can enforce mandatory access control on requests to access these separate single -level or system-high objects. MAC assigns security levels to different subjects (users) and objects (relations attribute). There are 4 security levels mentioned according to their priorities:

A. Top Secret (Ts)
B. Secret (S)
C. Confidential (C)
D. Unclassified (U)

A level which can be accessed by anyone has to be introduced in the online transaction processing system. This can be done by combining java access specifiers with MAC security levels. Thus, the following security levels as shown in Figure 1.0

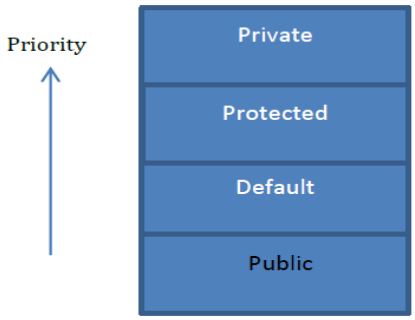

Figure 1.0: Proposed MAC

Private is at highest level while public is at lowest level. These levels can be assigned to both subject (user) as well as to object (relations). Private is assigned to subjects and objects which are at highest priority and are principal part of an organization which cannot be shared to anyone inside or outside the organization. Protected is assigned to those subjects and objects which are at very high priority and cannot be accessed by those which are at lower level of organization or common people outside the organization. Default is assigned to those which are at lower level of an organization that are a part of organization and information which cannot be shared outside the organization. Public level is assigned to everyone inside or outside this organization. It contains information which can be used to attract new customers or letting know people about your business or organization. Public is most handy level for strategy planners and analysts to advertise your business or organization. Unauthorized person cannot receive any confidential information from accessing public level data or information

4. Use Case Diagram(Using the mandatory access control (MAC) mechanism)

There are four actors in the online transaction processing system:

A. the credit card issuer assigned private role
B. The merchant assigned protected role
C. The customers get the default role
D. Site visitors gets public role

5. Class Diagram

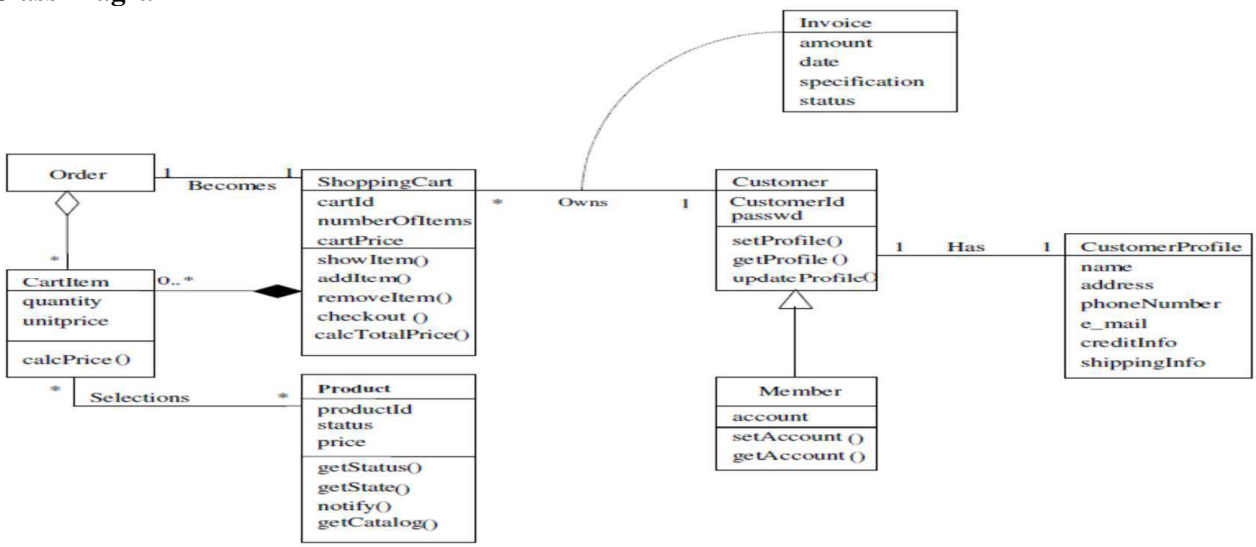

Figure 2.0: Class diagram for Shopping Cart

Class diagrams are one of the most useful types of diagrams in UML as they clearly map out the structure of a particular system by modeling its classes, attributes, operations, and relationships between objects.

Customers can select and purchase different products for a web shop. The shopping process must have well defined steps. This is necessary because the customer need to know where he is in the process. Figure 2.0 shows the class diagram for the Shopping Cart pattern. The Shopping Cart class collects information about all the products a customer has selected. The Cart Item object indicates the quantity and the product selected by a customer. A customer can query the products in his cart and remove products from the cart. The Customer class indicates the customer responsible for a shopping cart. When the shopping cart is checked out, an order and an invoice will be generated (the Order and Invoice classes). There are many systems that need to combine the functions of creating and preparing an invoice, and paying that invoice, including the corresponding validations. The system is affected by the following processes:

A. The creation, preparation, and validation of an invoice require specific actors, actions in specific sequences, and must follow specific rules.

B. Preparation and validation should be done by different people (separation of duty).

C. There should be flexibility about who is responsible for a payment and how the payments will be made.

D. The system and the client need a convenient way of keeping track of the payments made.

E. Validation of every prepared invoice and every received payment has to be made to ensure that the client's information is correct and in accordance to the requirements and regulations of each system.

F. The track of who created an invoice, who validated it, and who validated a payment need to be kept.

Figure 3.0 shows the class diagram for the Invoice pattern. Class Invoice Creator defines an interface for creating an invoice.

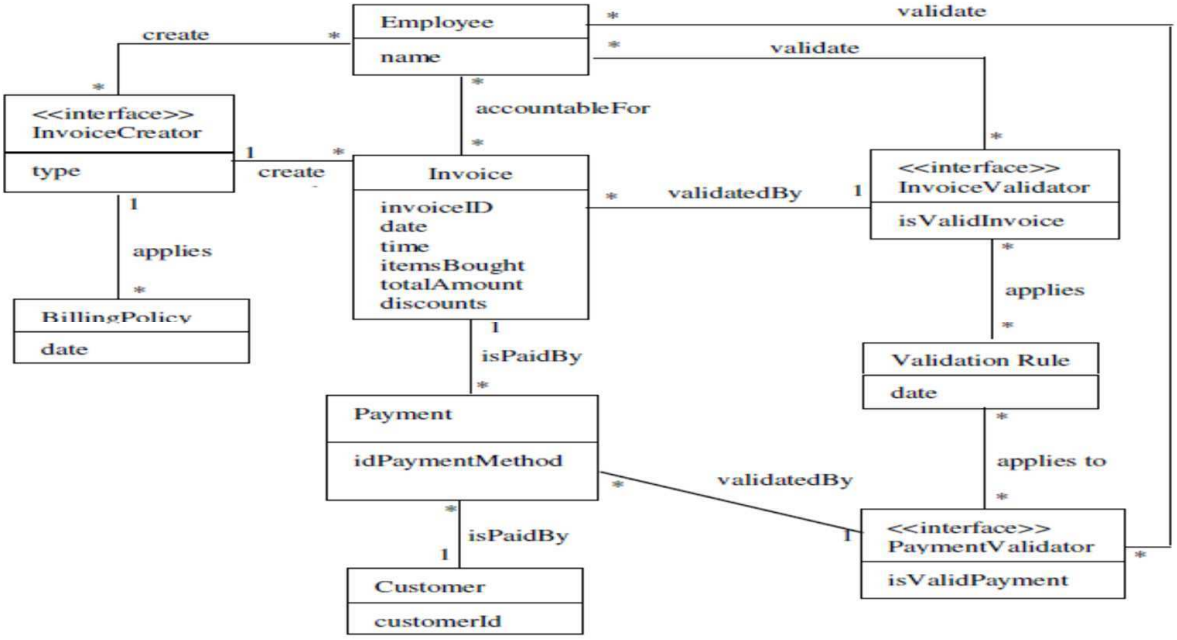

Figure 3.0: Class diagram for Invoice

Sequence Diagram

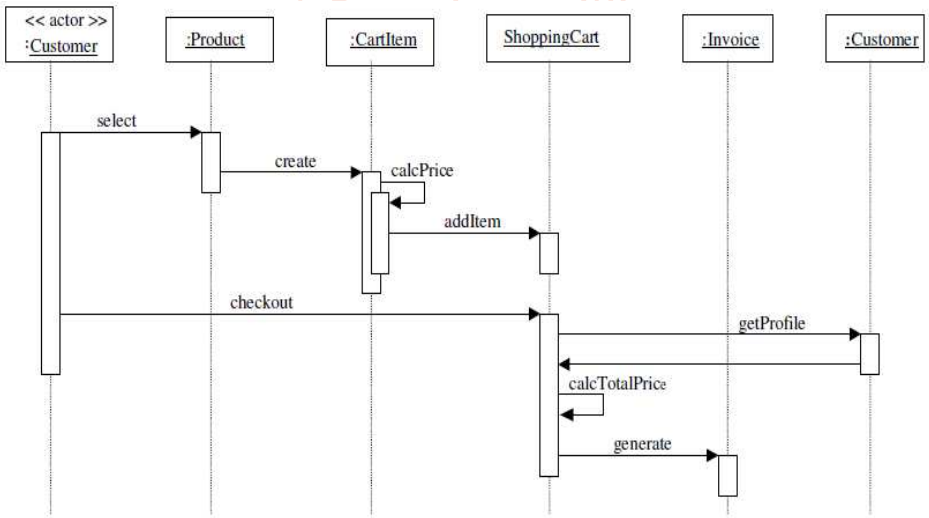

Figure 4.0: Sequence diagram for ordering of product

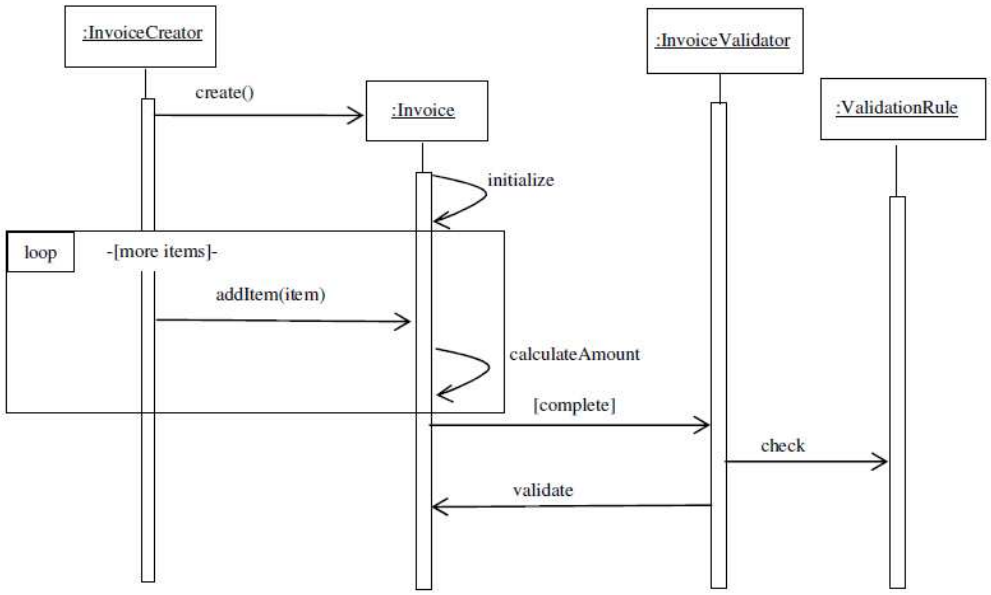

Figure 5.0: Sequence diagram for creating, preparing and validating an invoice

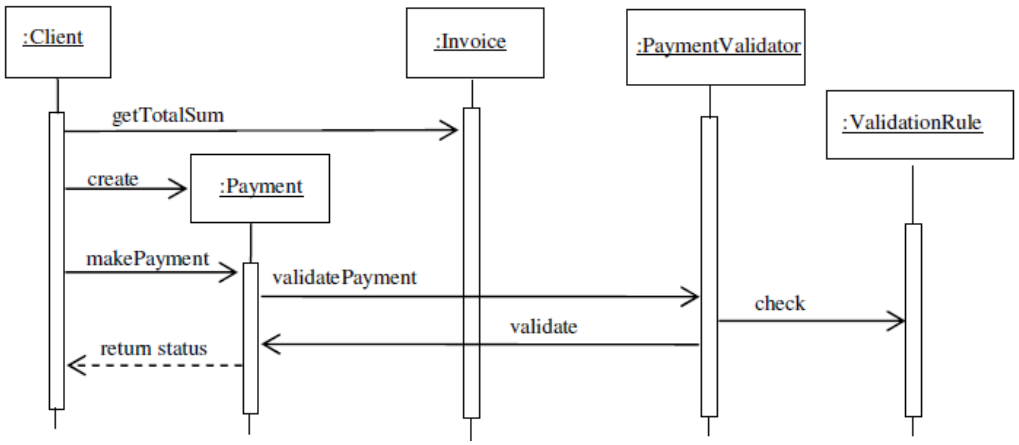

Figure 6.0: Sequence diagram for invoice payment

Activity Diagram for User Side

The activity diagram for user side describes all the operations users can perform on the e-commerce platform.

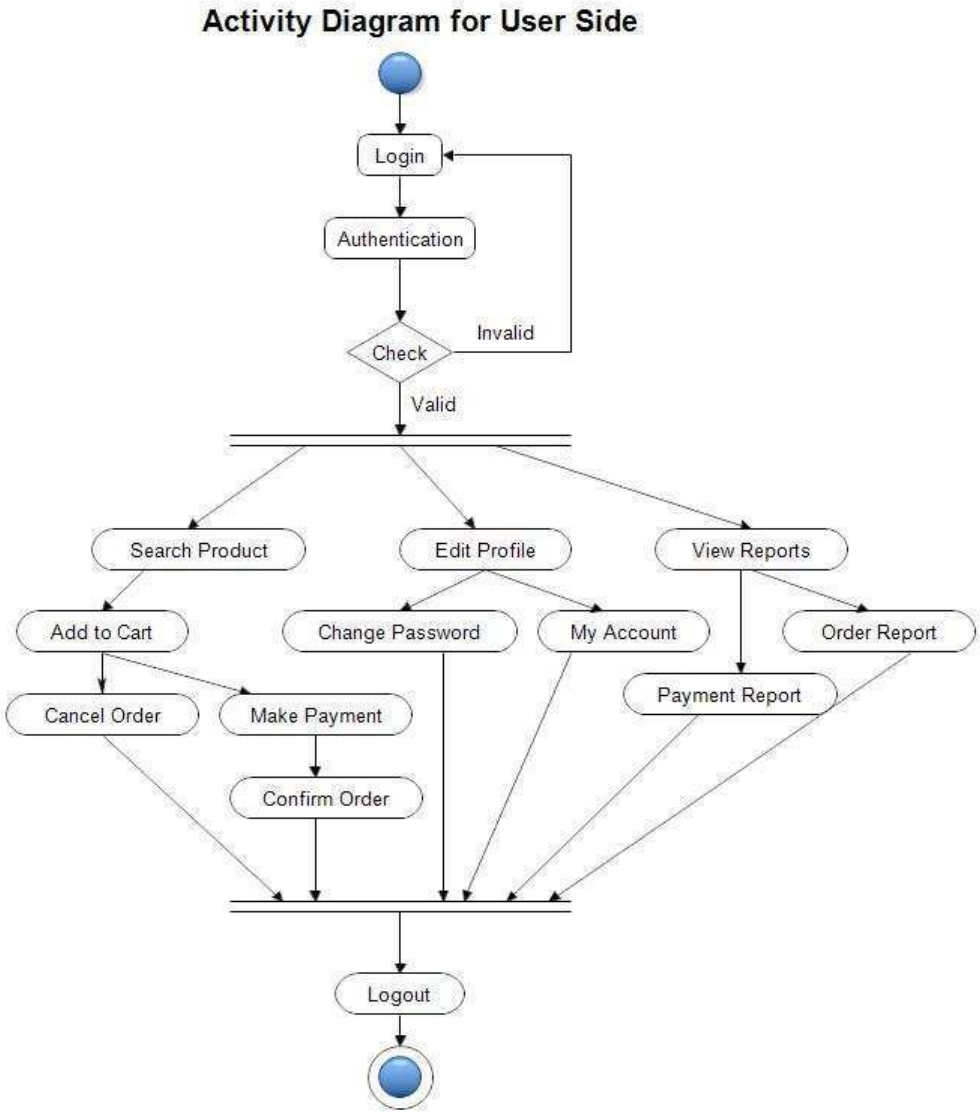

Figure 7.0: Activity diagram for user side

6. Secure Online Transaction Processing Collaboration Diagram

Security constraints can be added to each of the component patterns to produce a domain model for secure e-commerce. It is demonstrated here how to add security constraints by instantiating a security pattern, that is, Role-Based Access Control (RBAC) pattern. In the RBAC pattern, users are assigned to the roles according to their tasks or jobs and rights are assigned to the roles.

In this way, a need-to-know policy can be applied, where roles get only the rights they need to perform their tasks. Figure 8.0 shows how to add security constraints to the Shopping Cart pattern by applying instances of the RBAC pattern.

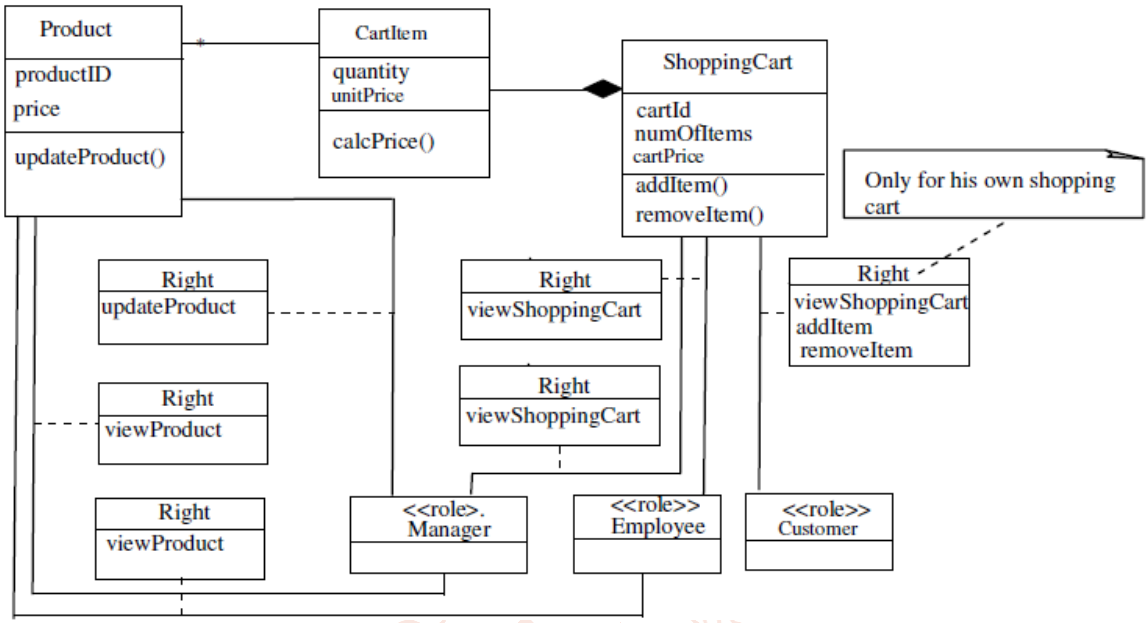

Figure 8.0: Adding security constraint to Shopping Cart

7. SYSTEM DESIGN AND IMPLEMENTATION

Overall Object Diagram of New System

The five component patterns can be combined to develop a domain model for online transaction processing applications. Each component pattern can correspond to a subsystem. Figure 4.14 is the object diagram which shows how the component patterns are combined into the domain model. Classes that are in several component patterns such as Customer, Invoice are only included in one subsystem. Subsystems dependencies are also shown in the diagram.

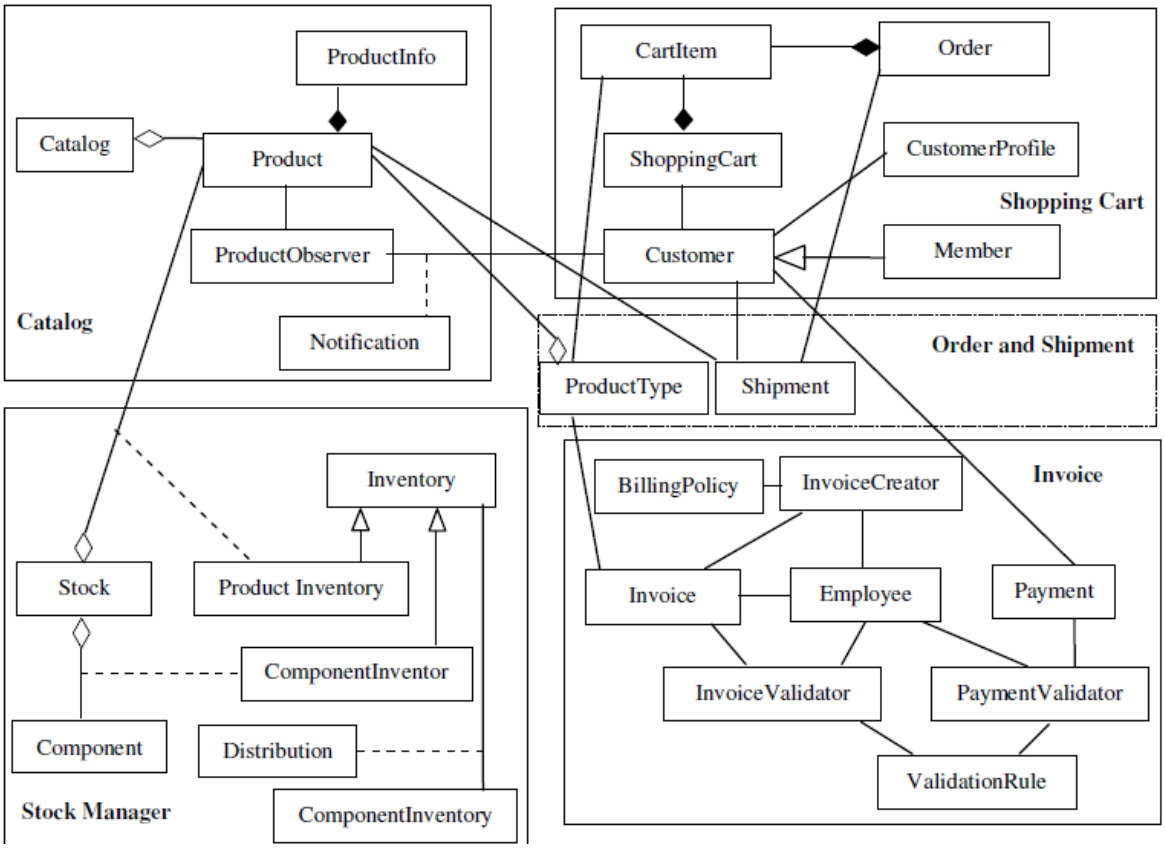

Figure 9.0: Overall Object Diagram of New System

8. Algorithm

This algorithm below combines the features of Multilevel Security (MLS) and the Bell-Lapadulla model to ensure the secure state of the system.

Client Server

1. Establish a Secure Channel and send Request for a page →

2. Generate cookie key (k)
   - Generate a cookie
   - Encrypt and send the cookie
   - Store key ID with K

3. ← Key ID, e_k(Cookie), k, Requested page

4. – Store encrypted cookie with Key ID, and the key ID with K

The next time the client requests a page from the web site:

5.- Generate a time stamp T.
- Concatenate it with the encrypted cookie
- Compute a MAC on the result

6. Request for a page, key ID,

T, e_k(Cookie), MAC_k (e_k(Cookie) || T) →

7. - Verify the Mac
- Check if the time stamp T is within the acceptance window. If so, send requested page; otherwise, decline the request

8. ← Requested page, e_k (Cookie)

9. System Flowchart

Figure 4.15 shows how to add security constraints to the Shopping Cart pattern by applying six instances of the MAC pattern.

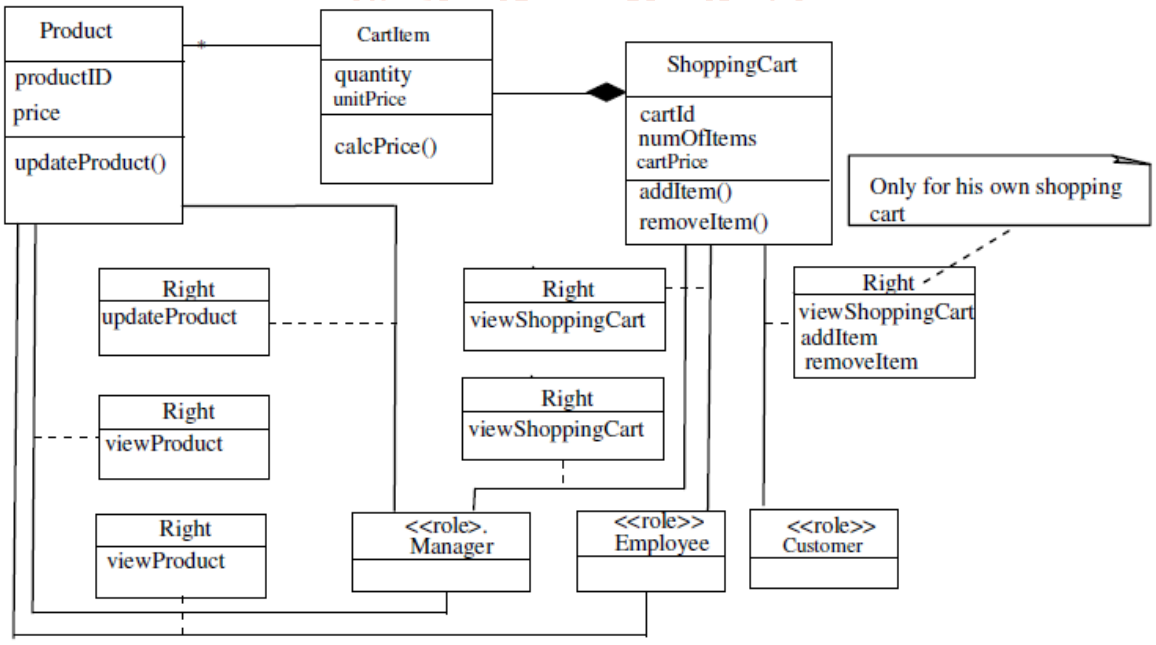

Figure 10: System flowchart for adding security constraint to Shopping Cart pattern

Security constraints can be added to each of the component patterns to produce a domain model for secure online transaction processing system. It is demonstrated here how to add security constraints by instantiating a security pattern, that is, Mandatory Access Control (MAC) pattern. In the MAC pattern, users are assigned to the

roles according to their tasks or jobs and rights are assigned to the roles. In this way, a need-to-know policy can be applied, where roles get only the rights they need to perform their tasks.

10. New System Requirements

The hardware and software are required for the implementation of the secured online transaction processing system using mandatory access control:

A. 2.4 GHZ of processor speed and above
B. 2GB RAM and above
C. 500 GB Hard disk
D. Internet Modem
E. Coloured Monitor
F. Printer
G. Windows XP, window 7, Window 8 or windows 10
H. Microsoft Dream Weaver 8
I. Wamp Server
J. JQuery
K. Fireworks
L. PHP-MySQL

11. Results and Discussion

To identify the bottleneck and performance related issues, there is need to test the online transaction processing system using different methods and analyze the query and their execution path. Records in every table of the database are taken for simulation. Some queries were executed by putting it into stored procedure using front end and query analyzer. Random transaction ID was taken several times. The results were gotten with Hardware configuration: Intel® Duel Core 2.8GHz 2GB RAM. Tables 4.9 and 4.10 shows the retrieval time with traditional MySQL database without using the mandatory access control (MAC) mechanism and the retrieval time from optimized MySQL database using mandatory access control (MAC) mechanism respectively.

Table 1.0: Retrieval time with traditional MySQL database without using the Mandatory Access Control (MAC) mechanism

Iteration	On Php Search Page (Front-End)	On Query Analyzer
1	.0491	.0543
2	.0473	.0537
3	.0489	.0631
4	.0491	.0571
5	.0478	.0544
6	.0483	.0597
7	.0462	.0549
8	.0497	.0572
Mean value (seconds)	**0.0483**	**0.0568**

After running the query with traditional MySQL database, retrieval time in stored procedure using front end is less than query analyzer.

Retrieval time of transaction-ID with traditional MySQL database in stored procedure:

A. On Front –end is 0.0483 seconds
B. On Query Analyzer is 0.0577 seconds

Table 2.0: Retrieval time from optimized MySQL database using the Mandatory Access Control (MAC) mechanism

Iteration	On Php Search Page (Front-End)	On Query Analyzer
1	.0131	.0289
2	.0159	.0246
3	.0142	.0290
4	.0148	.0394
5	.0136	.0379
6	.0142	.0290
7	.0162	.0287
8	.0130	.0325
Mean value (seconds)	**0143**	**.0312**

The same query was executed using new databases and Hash indexing technique by putting it into stored procedure on front end and query analyzer and taking random transaction ID several times on the database of centralized server. Retrieval time to execute the query using hash indexes from optimized MySQL database of centralized server is less than from the traditional database. Retrieval time of transaction-ID using stored procedure on MySQL database of centralized server:

A. On query analyzer using Hash indexing technique is 0.0312 seconds.
B. On front end using Hash indexing technique is 0.0143 seconds.

12. Conclusion

Privacy and Security are the two major factors that affect costumers trust in electronic transaction. Therefore companies or websites or organizations that offer and sell their products or services online should put more efforts in positively influencing their costumer‘s perceptions of privacy and security. Information technology users should be informed and should take responsibility for the security of resources that they are using and building.

This research has introduced a flexible and generic implementation of MAC in Relational Database Management Systems (RDBMS) that can be used to address the requirements from a variety of application domains, as well as to allow an RDBMS to efficiently take part in an end-to-end MAC enterprise solution. The research work suggests an object-oriented analysis and design methodology for secure web

application system. For such purpose, a security emphasized modeling language, UML was used and php/Javascript's role-based access control was used for the implementation. Therefore, the object-oriented analysis and design methodology for secure web application system offers a consistent analysis and design method that was not supported by existing object-oriented analysis and design methodologies. In addition, the correlation with Javascript that was not provided by UML is provided through role-based access control. Thus, the correlations among existing object-oriented analysis and design methodologies, security, and Javascript are presented to enable object-oriented analysis and design for the whole process of system development. It concludes that the effectiveness of the object-oriented analysis and design methodology for secure web application system was proved by successfully applying it to the on-line transaction processing system development.

REFERENCES

[1] Agbo, A. (2016). Cyber Security Made Easy: Cyber Security Threats and Solutions. Business Journal, 16(1), 18-27.

[2] Allan, K. (2015). Cyber Security and the Internet of Things. Indian Journal of Computer Science and Engineering, 3(4), 356-365.

[3] Burden, F. & Palmer, W. (2014). Controlling Threats: Computing & Control Engineering. New York: Momentum Press, 29-35.

[4] Chen, D.; Cong, J.; Gurumani, S.; Hwu, W.; Rupnow, K. & Zhang, Z. (2016). Cyber-Physical Systems: Theory & Applications. Journal of the Institution of Engineering and Technology, 1 (1), 70-77.

[5] Li, Z.; Jin, D.; Hannon, C.; Shahidehpour, M. & Wang, J. (2016). Assessing and Mitigating Cyber Security Risks. Journal of the Institution of Engineering and Technology, 1 (1), 60-69.

[6] Liang, F.; Cole, F. & Mark, H. (2017). Security of Virtual Working on Cloud Computing Platforms. Journal of the Institution of Engineering and Technology, 2(1), 79-87.

[7] McLean, V. A. (2010). Science of Cyber-Security. New York: The MITRE Corporation, 29-49.

[8] Oltramari, A.; Cranor, L. F.; Walls, R. J. & McDaniel, P. (2016). Building an Ontology of Cyber Security. International Symposium on Information, Computer, and Communications Security, 1(1), 54-61.

[9] Onyesolu, M. O. & Ezeani, M. I. (2012). ATM Security Using Fingerprint Biometric Identifier: An Investigative Study. International Journal of Advanced Computer Science and Applications, 3 (5), 67-74.

[10] Rosenquist, M. (2015). Navigating the Digital Age: The Definitive Cyber Security Guide for Directors and Officers. Chicago: Caxton Business & Legal, Inc., 1-19.