IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 9, Issue.5, May 2021 E-ISSN: 2347-2693

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

Allwell Ononiwu Akanwa[1*], Virginia. E. Ejiofor[2]

[1,2]Department of Computer Science, Nnamdi Azikiwe University, Awka Anambra State, Nigeria

**Corresponding Author: amanzebethran@yahoo.com*

DOI: https://doi.org/10.26438/ijcse/v9i5.2230 | Available online at: www.ijcseonline.org

Received: 14/May/2021, Accepted: 20/May/2021, Published: 31/May/2021

Abstract- With the increasing popularity of the internet as well as the evolving acceptance of cashless policy, information and online transaction processing systems are generally more susceptible to direct attack and abuse than their offline counterparts. Various security techniques have previously been developed to regularly assess the vulnerability of these systems and provide security to users. However, a number of these security techniques have proved to have bottlenecks thereby, putting sensitive financial information, services and products at risk of cyber-attacks. In this work, an enhanced security model that improves the security of the online transaction processing system is designed. This algorithm combines the features of Multilevel Security (MLS) and the Bell-Lapadulla model (BLM) to ensure the secure state of the system. Additionally, Mandatory Access Control (MAC) mechanism was used to enhance the security of the sensitive information/data shared during the online transaction processing. The methodology adopted was Object Oriented Hypermedia and Design Methodology (OOHDM) which is well suited for analyzing and designing objects that make up the new security enhanced system. Microsoft Visual Studio 2010 was used as our development environment. The programming language used was PHP and Java Script, while MySQL Server 2008 was used in the development of the database engine. Enhancing the security requirement(s) of the system was considered. The results showed that the enhanced security model using Mandatory Access Control (MAC) mechanism offered a highly secured system where users and organizations felt protected while carrying out transactions online.

Keyword: MAC, OOHDM, MLS, BLM

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 2020. 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, a security measure that can conveniently be regarded as "smart", a security system that can take autonomous decisions based on environmental factors as this would be the solution to defeat the activities of hackers and malicious insiders who constantly strive to find loop holes to penetrate organizations networks and systems (Chen *et.al*, 2016). While traditional information security has always included practice areas related to the security of information and systems, the cyber world that we live in today has become increasingly connected and increasingly mission critical due to our network-delivered society. The traditional enterprise boundaries that formed the basis for securing the perimeter from the outside world have, by necessity, become increasingly porous to support this new, routinely wireless and ubiquitous "always-on" connectivity (Allan, 2015). Most organization 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). The security of computer systems depends on a number of environmental factors: services, operating system, patch level and perhaps most importantly, configuration. Computing services could range from a simple text editing or internet browsing to a more sophisticated satellite navigation or robotic vision (Brandon *et. al*, 2009). Irrespective of the services provided by a computer system, some level of assurance for security is always required. In a large computing environment with high security requirements, it could be very difficult for system administrators to give the necessary attention needed to provide a reasonable amount of security (Geers, 2011). Security of systems and network resources have always been a top priority in any organization, organizations do not want vital data to be compromised, hence they can go extra mile to secure their systems. System administrators are therefore saddled with the heavy task of configuring the

organizations network and systems to present maximum security which would be very difficult to be compromised by any form of security threats such as hackers, malware and any vulnerable application, a task which is always difficult for administrators especially in large enterprises (Anthony, 2007). 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). Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the Nigeria Computer Society 2016 national conference communiqué on cyber security addresses cybercrime as one major challenge underlines this. The universal challenge is a state in a computing system which:

1. allows an attacker to execute commands as another user;
2. allows an attacker to access data that are contrary to the specified access restrictions for that data;
3. allows an attacker to conduct a denial of service;

The aim of this study is to develop an enhanced security model for information and online transaction processing systems. The specific objectives are to:

1. Reduce the growing cross channel fraud, data theft, and ransom ware on e-commerce platforms.
2. Enhance the security capability of e-commerce platforms;
3. Develop an enhanced security system for information and online transaction processing systems using mandatory access control (MAC) mechanism;
4. Evaluate the performance of the newly developed system compared to the existing system.

Cyber Crime

Cyber Crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber-crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber-crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become a major problem to people and nations. Usually in common man's language cyber-crime may be defined as crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing a major role in a person's life the cyber-crimes also will increase along with the technological advances (Reddy & Reddy, 2014).

Cyber Security

Privacy and security of data will always be top securing concerns to any organization. We are presently living in a world where all the information is maintained in a digital or a cyber-form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures (Geers, 2010). As crime is increasing even the security measures are also increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber-attacks are a serious threat to both their data and their business continuity (Calhoun & Nichols, 2015). There will be new attacks on android operating system based devices, but it will not be on massive scale. The fact that tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms (Boardman & Sauser, 2016). The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security (Bayuk *et.al*, 2012).

2. REVIEW OF RELATED WORKS

Assessing and Mitigating Cyber security Risks

Li, *et.al* (2016) studied the cyber security vulnerabilities of traffic light systems as well as the corresponding defensive measures against the existing and potential cyber-attacks. The study provided a general bi-level optimization-based framework for assessing the cyber security risks of traffic light systems in terms of the physical implications on traffic networks. The study further developed a minimax-regret-based approach to prioritizing defensive measures for mitigating cyber security 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.

Building an Ontology of Cyber Security

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.

Security of Virtual Working on Cloud Computing Platforms

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.

Checkmating Cybercrime with Framework

In a bid to check growing cyber-crime in banks, the CBN in 2017 released a policy/framework that will use biometric verification Number (BVN) as a major tool to fight fraudsters. The release indicated that the BVN would be used to investigate and identify individuals who defraud banks and other customers of banks. It continued that once the investigation proves that they are fraudsters, legal action would be taken against them. From the foregoing, it is obvious that this policy/framework limited cybercrime to financial services institutions rather than tackle this menace as they affect organizations, government, entities and individuals. Again, this solution does not fully translate to adequate protection from cyber-attacks; it focused more on identifying the individuals behind the attacks rather than building a more secure and resilient cyber ecosystem as the world has gone digital (CBN, 2017).

Implementation of ATM Security by Using Fingerprint Recognition and GSM

Amurthy & Redddy (2012) developed an embedded fingerprint system, which was used for ATM security applications. In their system, bankers collect customers' finger prints and mobile numbers while opening accounts, then customer only access ATM Machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access. From our point of view, though the system developed is an aspect of cyber security system but it is limited to ATM machines and does not provide a technique or process that protects a system's information assets from threats to confidentiality, integrity, or availability.

ATM Security Using Fingerprint Biometric Identifier

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.

3. METHODOLOGY AND ANALYSIS

The methodology adopted is the object oriented hypermedia and design methodology (OOHDM). In OOHDM, a hypermedia application is built in four step process, supporting an incremental or prototype process model. Each step focuses on a particular design concern, and an Object-Oriented model is built. Classification, aggregation and generation/specification are used throughout the process to enhance abstraction power and reuse opportunities. These phases are summarized below.

1. Requirement Gathering:

In this phase the UML provide some abstraction mechanisms for this purpose, as the Use Case Diagram, but other diagrammatic tools as the Interaction Diagram (Sequence or Collaboration) or the state chart Diagram can also be used to gather requirements even they are usually used only at design time.

2. Domain/Conceptual Analysis:

In this phase a conceptual model of the application domain is built using well-known object-oriented modeling principles augmented with some primitives such as attribute perspective. Conceptual classes may be built using aggregation and generalization/specialization hierarchies.

3. Navigational Design:

Here we describe the navigational structure of a hypermedia application in terms of navigational contexts, which are induce from navigational classes such as nodes, links, indices, and guided tours. Navigational contexts and classes take into account the type of intended users and their access level.

4. Abstract Interface Design:

The abstract interface model is built by defining perceptible objects (e.g., a picture, a city map, and so forth) in terms of

interface classes. Interface classes are defined as aggregations of primitive classes (such as text fields and buttons) and recursively of interface classes. Interface objects map to navigational objects, providing a perceptible appearance. Interface behavior is declared by specifying how to handle external and user-generated events and how communication takes place between interface and navigational objects.

5. Implementation:

Implementation maps interface objects to implementation objects and may involve elaborated architecture (e.g., client-server), in which applications are clients to a shared database server containing the conceptual objects.

The OOHDM approach is motivated by the kind of system we desire to develop. We desire to build a usable and evolvable hypermedia application. Good web applications should be good hypermedia applications. The very nature of the proposed system, in which navigation is combined with the inherent difficulties of dealing with multimedia data, needs an OOHDM approach. Traditional methodologies do not contain useful abstractions to deal with the hypertext metaphor. They do not provide the notion of linking. The interface of Web apps is more complex than in traditional software systems, navigation and functionality should be seamlessly integrated and the navigational structure should be decoupled from the domain model of the app, therefore OOHDM was chosen for its functionalities, in that it allows object oriented abstractions for analysis and design of information-intensive web applications. Besides the modeling abstractions, it also provides a methodology which guides a developer through different activities in the web application development.

Analysis of the Existing System

Online transaction processing payment transaction model has the interactions of four roles:

Payer – The payer is an authorizer of a payment means supported by an issuer. Ordering a payment may be done using a card, a token, or a certificate. The payer is the customer or buyer in an electronic commerce scenario.

Payee – The payee is a merchant providing goods, services, and/or information and receiving electronically the payment for something purchased by the payer. Usually, the payee is simply referred to as the vendor, merchant, or seller in an electronic commerce scenario.

Issuer – The financial instrument that supports issuing payment cards (or means) by using cryptographic technologies which guarantees the association with ―real money. Its role is to provide the payer and the payee with instances of monetary value which are used in payment protocols to transfer ―real money‖ from the payer to the payee.

Acquirer – This is a financial institution (a bank, for example) which transforms the cryptographic objects involved in the payment into ―real money‖ on behalf of the payee.

The security requirements vary from one role to another. However, it appears that acquirer and issuer have very close requirements. In the following we examine individually the requirements of each role. Client Transaction confidentiality, especially the information occurring in the payment card, is a major security need for a client. The nature of the transaction may require confidentiality. Various security protocols have been developed for e-commerce. The major protocols include:

1. The Secure Socket Layer (SSL) protocol: SSL was developed in 1994 by Netscape to provide secure communication between Web browsers and Web servers. SSL provides server authentication, data integrity, and client authentication.
2. The Transport Layer Security (TLS) protocol: This was introduced by the Internet Engineering Task Force in 1995 (Dierks and Allen, 1999).
3. The Secure Electronic Transaction (SET) protocol: SET was developed by Visa, MasterCard, and other companies to facilitate secure electronic commerce transactions and provide confidentiality of payment card information, data integrity, authentication of both merchant and cardholder, and authorization of transactions.
4. The 3-D Secure Protocol This has been developed by Visa recently (Visa, 2002). It provides cardholder authentication for merchants using access control servers and the Visa Directory Server.

Once registration is done, cardholder and merchant can start performing their transactions, which involve five basic steps in this protocol:

1. The customer browses the website and selects the goods to purchase. Then the customer sends the order and payment information, which includes two parts in one message: the purchase order (say part a) and the card information (say part b). While the former information part is for the merchant, the latter is for the merchant‘s bank only.
2. The merchant forwards part b to its bank to check with the issuer for payment authorization.
3. On receipt of the authorization from the issuer, the merchant‘s bank sends it to the merchant.
4. The merchant completes the order, sends confirmation to the customer and captures the transaction from his/her bank.
5. The issuer finally prints a credit card bill (or an invoice) to the customer. SET relies on cryptography and digital certificate to ensure message confidentiality and security. Message data is encrypted using a randomly generated key that is further encrypted using the recipient‘s public key.

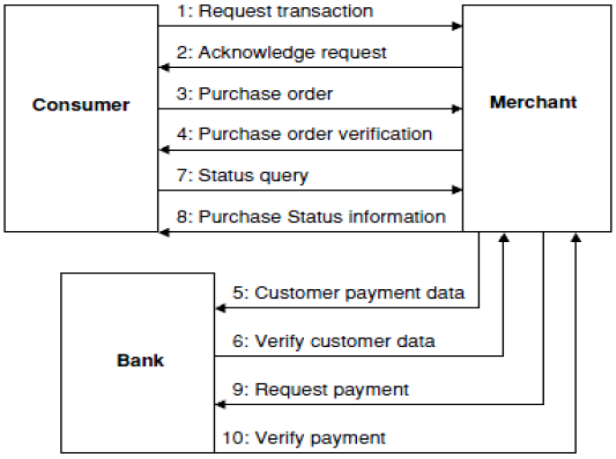

Figure 1: Online transaction processing steps

1. The customer opens an account: The customer obtains a credit card account, such as MasterCard or Visa, with a bank that supports electronic payment and SET.
2. The customer receives a certificate: After a suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank. The certificate verifies the customer‘s RSA public key and its expiration date. It also establishes a relationship, guaranteed by the bank, between the customer‘s key pair and his/her credit card. A merchant who accepts a certain variety of cards must be in possession of two certificates for two public keys: one for signing messages and one for key exchange. The merchant also needs a copy of the payment gateway‘s public-key certificate.
3. The customer places an order: This is a process that may involve the customer first browsing through the merchant‘s Web site to select items and determine their prices. The customer then sends the list of the items to be purchased from the merchant, who returns an order form containing the list of items, their individual prices, a total price, and an order number.
4. The merchant is verified: In addition to the order form, the merchant sends a copy of his certificate, so that the customer can verify that he/she is dealing with a valid store.
5. The order and payment are sent: The customer sends both an order and payment information to the merchant, along with the customer‘s certificate. The order confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer‘s certificate enables the merchant to verify the customer.
6. The merchant requests payment authorization: The merchant sends the payment information to the payment gateway, requesting authorization that the customer‘s available credit is sufficient for this purchase.
7. The merchant confirms the order: The merchant sends confirmation of the order to the customer.
8. The merchant provides the goods or service The merchant ships the goods or provides the service to the customer.
9. The merchant requests payment: This request is sent to the payment gateway, which handles all of the payment processing.

This project was able to identify various methods of carrying out authentication and secure payments, and most of these methods are currently used in existing commercial systems/products today. Thus, this section documents our analysis of these existing systems with the aim of finding out the most secure and realistic way to authenticate and perform payments online.
During the explorative process, four different kinds of systems were identified in the market that claims to offer a secure authentication process.

PayPal password login
This is a system which makes use of a one-factor authentication. The strength of this system lies in the underlying fact that users are mandated to choose strong passwords (e.g. combination of different data types, restriction on short passwords etc.). Although a strong password can be chosen, such one-factor systems have been shown to be vulnerable to attacks such as password cracking and is not considered secure enough.

PayPal ensures that users register their personal details (e.g. password) which are then used for verification during the login process. A PayPal user intending to purchase goods from an e-commerce store is redirected to PayPal where he is asked to supply his User ID and Password. PayPal verifies the authenticity of the credentials entered by the user. It allows the user to proceed and finalize the payment.

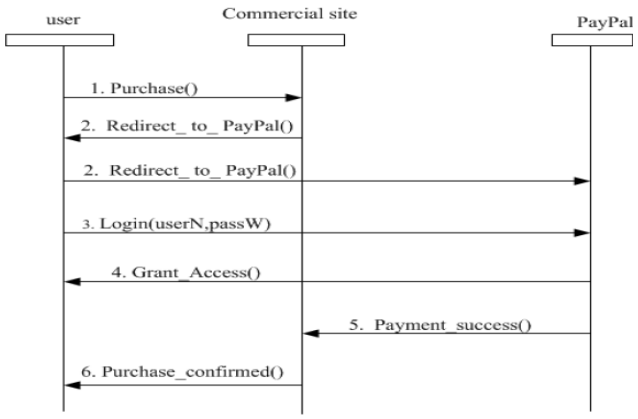

Figure 2: PayPal authentication process flow

AcrotOTP Mobile
This authentication system employs two-factor authentication by using a mobile device as the hardware token. The mobile device possesses an OTP generator module that generates random one-time passwords. The AcrotOTP system is made up of a container which holds the Acrot keys used for generating Random OTP. The Acrot keys are protected by cryptographically strong encryption. The system is made up of an authentication server which is used to verify that the OTP entered by the user is indeed a valid token.

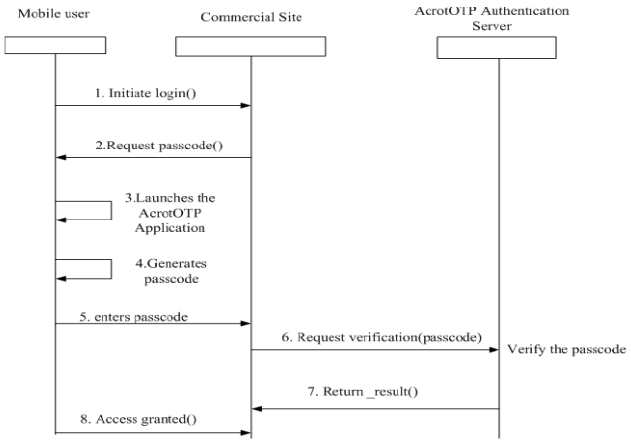

Figure 3: AcrotOTP authentication process flow

User initiates login process with a commercial site. The site prompts user to enter a passcode. User launches AcrotOTP application on his mobile phone and subsequent-ly generates a passcode with the application by entering his pin code. User enters the generated passcode into the commercial site and the entered passcode is verified with the AcrotOTP authentication server. The user is either granted or denied access based on the results returned from the authentication server.

Data Flow of the Old System

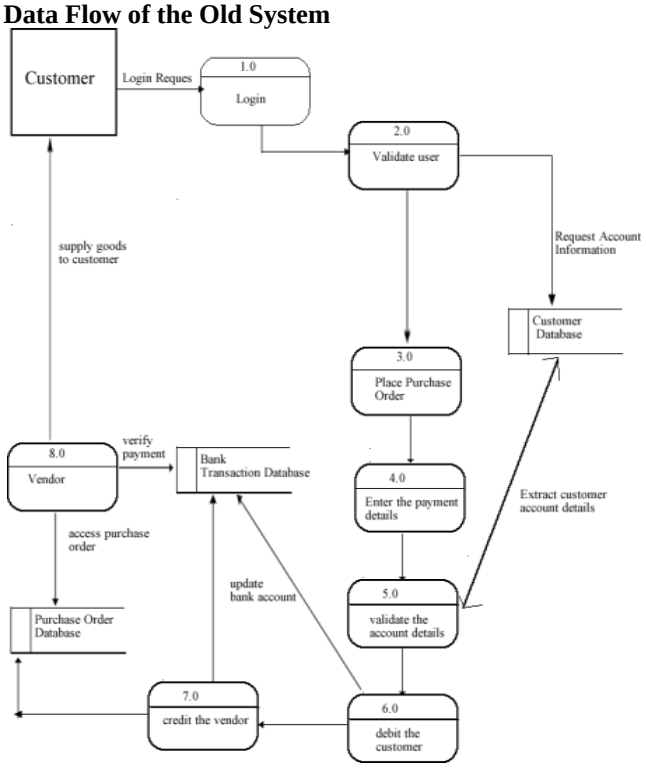

Figure 4: Data Flow Diagram of the existing online transaction processing

In the present system is a series of processes that the client logs into the vendor's website through the web-browser installed on the PC and carries out various online transactions by using a private username and password. The customer has to make payment through the use of credit card. The system verifies the credit card details before forwarding the purchase order to the vendor who in turns verify the payment before delivering the ordered product to the customer.

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 we use multiple encryption scheme for the security of information. We also check for the hacking or attacks on the e-commerce application and the sensitive information sent over the network through the modules of the proposed system. There are four modules in the proposed system and they are stated as follows:

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

Everyone normally pay for goods purchased over the Internet by giving the merchant their credit card details. To prevent this information from unwanted people from stealing the card number, the message undergoes a session of the secure sockets layer (SSL) protocol. In this arrangement the cardholder and merchant should trust each other. That requirement is undesirable even in face-to-face transactions, but over the internet it has risks. The cardholder is protected from eavesdroppers but not from the merchant itself. Some merchants are dishonest. They do not protect the sensitive information. The merchant also needs to be protected and should have some protection against dishonest cardholders who supply an invalid credit card number.

Mandatory Access Controls (MAC) systems are appropriate for many multilevel secure applications (MLS). Multilevel security is the implementation of MAC idea application. And we introduced it as the traditional MAC application. The methodology we propose allows a database administrator to define labels and to set up a database table such that access to a row in that table is based upon the label associated with that row and the label associated with the user accessing that row. More specifically, the methodology allows the database administrator to:

1. Define label types
2. Define label access rules and exceptions to them
3. Assign labels and exceptions to database users

4. Attach a label type and a set of label access rules to a database table

Multilevel database systems is attempting to develop database systems that protect classified information from unauthorized users based on the classification of the data and the clearances of the users. The data stored in a local database system are classified into several levels. Access rights are grouped by level, and the use of resources is restricted to individuals authorized to assume the associated level.

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:

1. Top Secret (Ts)
2. Secret (S)
3. Confidential (C)
4. Unclassified (U)

A level which can be accessed by anyone has to be introduced in the online transaction processing system. We can do this by combining java access specifiers with MAC security levels. Thus we get following security levels:

1. Private
2. Protected
3. Default
4. Public

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.

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. We demonstrate 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 3.17 shows how to add security constraints to the Shopping Cart pattern by applying instances of the RBAC pattern.

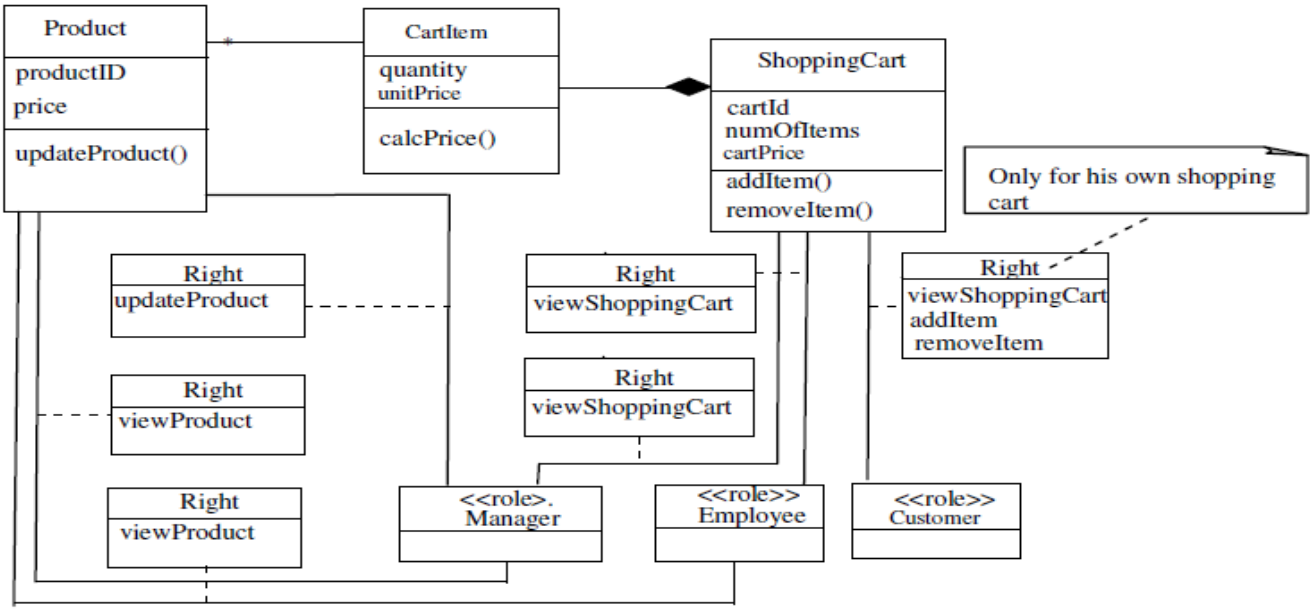

Figure 3.16: Adding security constraint to Shopping Cart

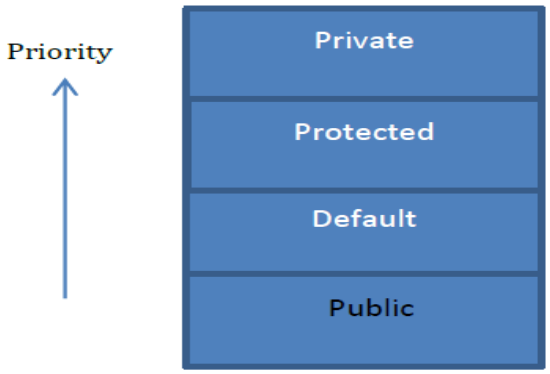

Figure 5: Proposed MAC

Only read down is allowed. A subject can read an object only if its security level is greater than or equal to that of object. Other objects are not provided and cannot be read by that subject.

A subject can perform write or modify operation only in that view provided and that also at level which is not less than level of object to prevent flow of information from higher level to lower level. In other words, a subject can only perform write operation if security level of subject is equal to that of object.

Overall Object Diagram of the New System

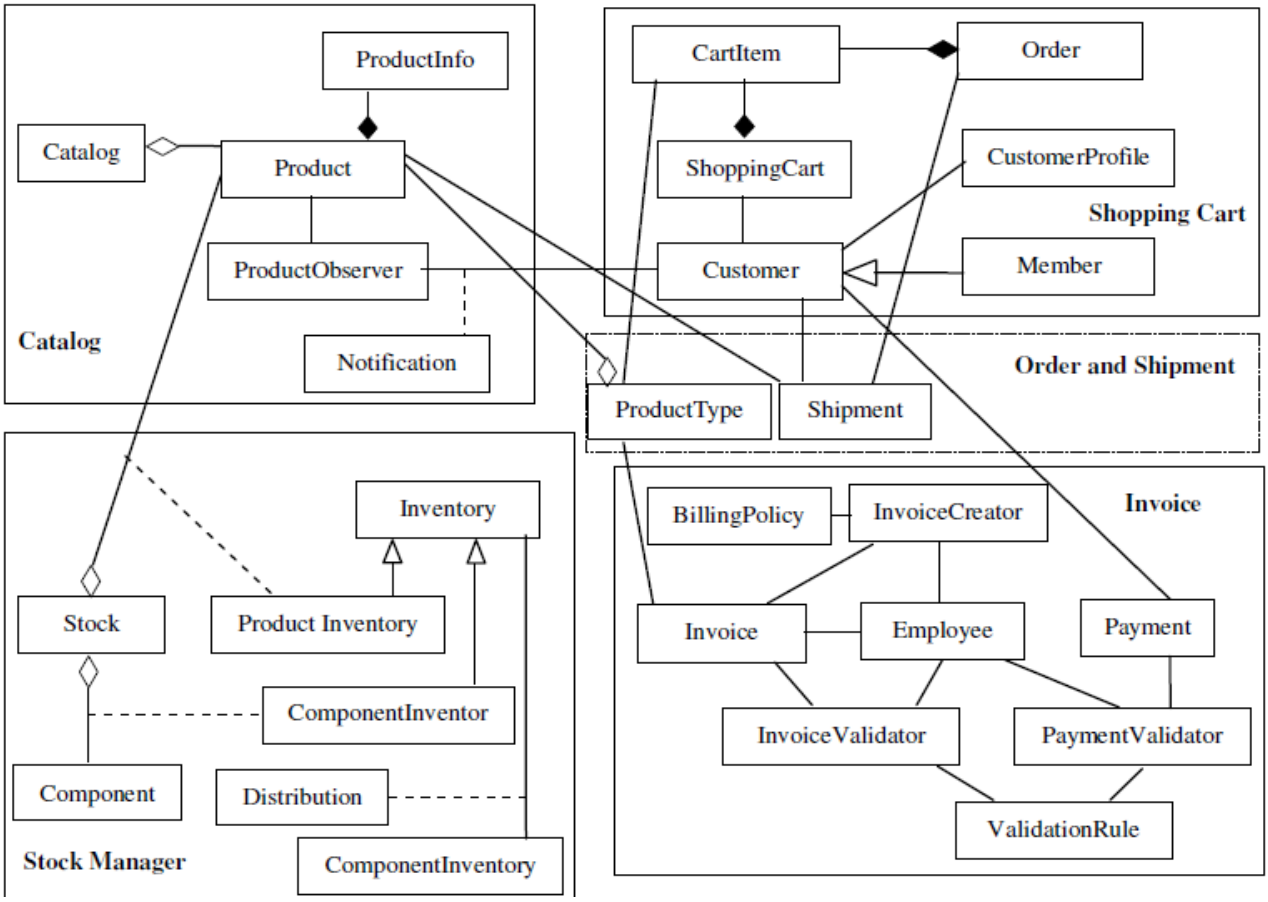

Figure 6: Object Diagram

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 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.

4. 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. Computer system security is a worldwide problem that is affecting private as well as corporate users of information technology. Information technology users should be informed and should take responsibility for the security of resources that they are using and building.

This work 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, 2016.**

[2] 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, 2016.**

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

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

[5] Bottino, J. & Hughes, V. (2015). Understanding and Managing Cybercrime. Boston: Allyn & Bacon, **202-244, 2015.**

[6] Geers, K. (2011). From Cambridge to Lisbon: the quest for strategic cyber defense. Journal of Homeland Security and Emergency Management, **8 (1), 1-16, 2011.**

[7] Anthony, R. J. (2007). Policy-centric Integration and Dynamic Composition of Autonomic Computing Techniques. International Conference on Autonomic Computing (ICAC), IEEE, **103-116, 2007.**

[8] McLean, Reddy, G. N. & Reddy, G. J. U. (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. International Journal of Engineering and Technology, **4 (1), 48-51, 2014.**

[9] Reddy, G. N. & Reddy, G. J. U. (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. International Journal of Engineering and Technology**, 4 (1), 48-51, 2014.**

[10] Calhoun, C. D. & Nichols, J. I. (2015). Developing a Comprehensive Cyber Security Curriculum with a Collaborative Learning Environment. National Cyber Security Institute Journal, **2 (2), 1-56, 2015.**

[11] Boardman, A. & Sauser, M. (2016). Computer Security Issues & Trends. California: Sogeti and IBM, **105-119, 2016.**

[12] Bayuk, J. L.; Healey, J.; Rohmeyer, P.; Sachs, M. H.; Schmidt, J. & Weiss, J. (2012). Cyber Security Policy Guidebook. New Jersey: John Wiley & Sons, Inc., **1056-1088, 2012.**

[13] 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, 2016.**

[14] 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, 2016.**

[15] 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, 2017.**

[16] Amurthy, P. K. & Redddy, M. S. (2012). Implementation of ATM Security by Using Fingerprint Recognition and GSM. International Journal of Electronics Communication and Computer Engineering, **3 (1), 83-86, 2012.**

[17] 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, 2012.**

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

