Development of an E-Transaction and Information Processing System

[1]Mbagwu Amarachi Austina., [2]Amanze Bethran Chibuike., [3]Agbasonu Valerian Chinedum.,[4]Agbakwuru.A. Onyekachi
[1]Department of Computer science, College of Physical and Applied Sciences, Michael okpara University of Agriculture, Umudike,Umuahia, Abia State, Nigeria.
[2,3,4]Department of Computer Science,
Faculty of Physical sciences, Imo State University, Owerri, Imo State, Nigeria.
amanzebethran@yahoo.com

DOI: 10.56201/ijcsmt.v9.no2.2023.pg1.13

ABSTRACT
The paper utilized the mandatory access control (MAC) as a security mechanism for the E-transaction processing which involves product ordering, payment using credit card, and product information management. The paper 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 system is very robust and My-SQL database was used at the back-end.

Keywords*: Customers, e-platform administrator, payment gateway administrator*

1. INTRODUCTION

The Internet is one of the fastest-growing areas of technical infrastructure development. Today, information and communication technologies (ICTs) are adopted in many sectors and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings. Electricity supply, transportation infrastructure, military services and logistics-virtually all modern services depend on the use of ICTs [1]. Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries can also benefit from new technologies. With the availability of long-distance wireless communication technologies such as WIMAX and computer systems that are now available for less than USD 200, many more people in developing countries should have easier access to the Internet and related products and services [2]. The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services. E-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone

services are growing faster than landline communications [3]. The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for a developing country like Nigeria. ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements. In turn, ICT applications may release technical and human capacity and enable greater access to basic services. In this regard, online identity theft and the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes is now one of the main threats to further deployment of e-government and e-business services [4]. 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 cybercrime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cybercrimes 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 cybercrime 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 cybercrimes also will increase along with the technological advances [5]. 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 [6]. 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 [7]. 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 [8]. 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 [9].

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 [10]. 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 [11]. 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 [12] 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 [13]. 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 [14]. Many operating systems in use today presents some level of security to protect users, processes resources etc from various forms of attacks. Although some of this operating system may not be able to defend completely against both internal and external threat as many of them are not well equipped with the necessary tools to monitor and control all aspect of their operations. Linux employs the Discretionary Access Control (DAC) Mechanism to control access to the system. The DAC mechanism is referred to as discretionary because the control of access is based on the owner's discretion. The owner of the object specifies which subjects can access the object [15].

2. REVIEW OF RELATED WORKS

[16] 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. [17] 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.

Over the last few years, researchers have carried out researches to identify the best approach to providing adequate security of information systems; this follows the increase in the number of attempted cyber-attacks. These attacks when successful have caused serious damages to organizational reputations, huge financial loss and breach of public trust. Many obstacles face

organizations, agencies, government or even individuals when attempting to achieve maximum security of information systems; among them are the existence of dependence of security systems management on human intervention, which is a continuous process that increases the level of difficulty. Another example of obstacles is that attacks on computer/information systems are becoming increasingly sophisticated and there are several deficiencies in current security systems. Thus, the problem of security management is becoming more complex and it is therefore pertinent to use resources offered by policy-based computing. 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.

3. ANALYSIS OF THE SYSTEM

E- transaction processing payment 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 [18].
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 [19]. 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.

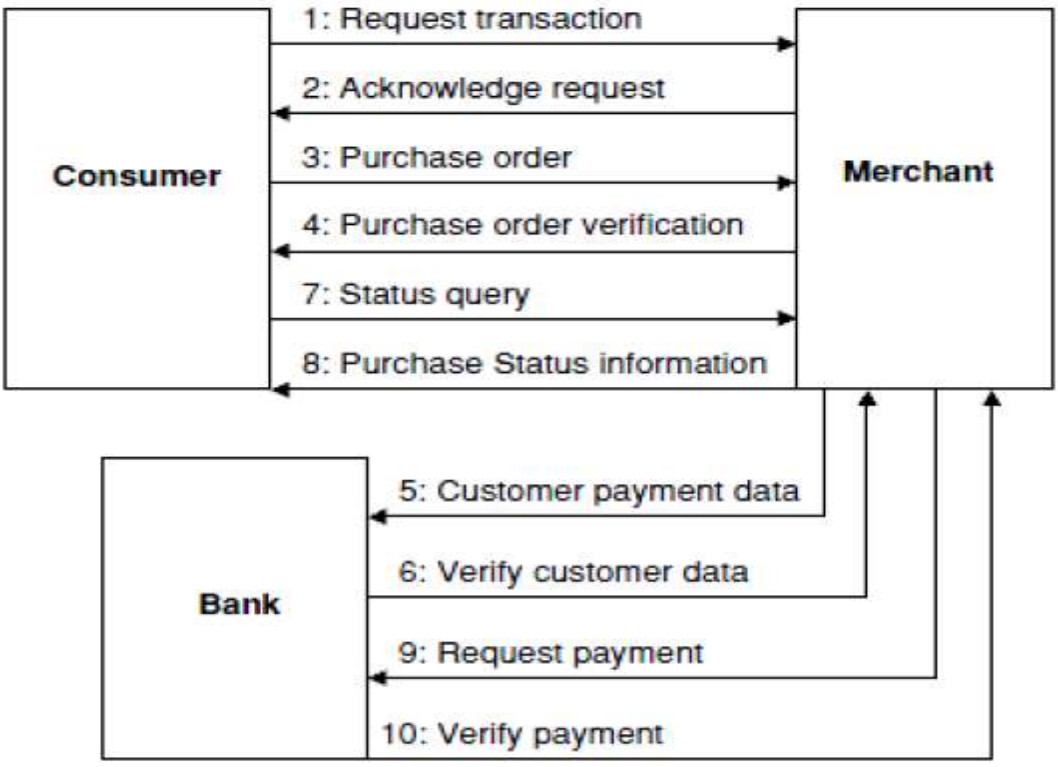

Figure 1: E-transaction processing steps

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.

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.

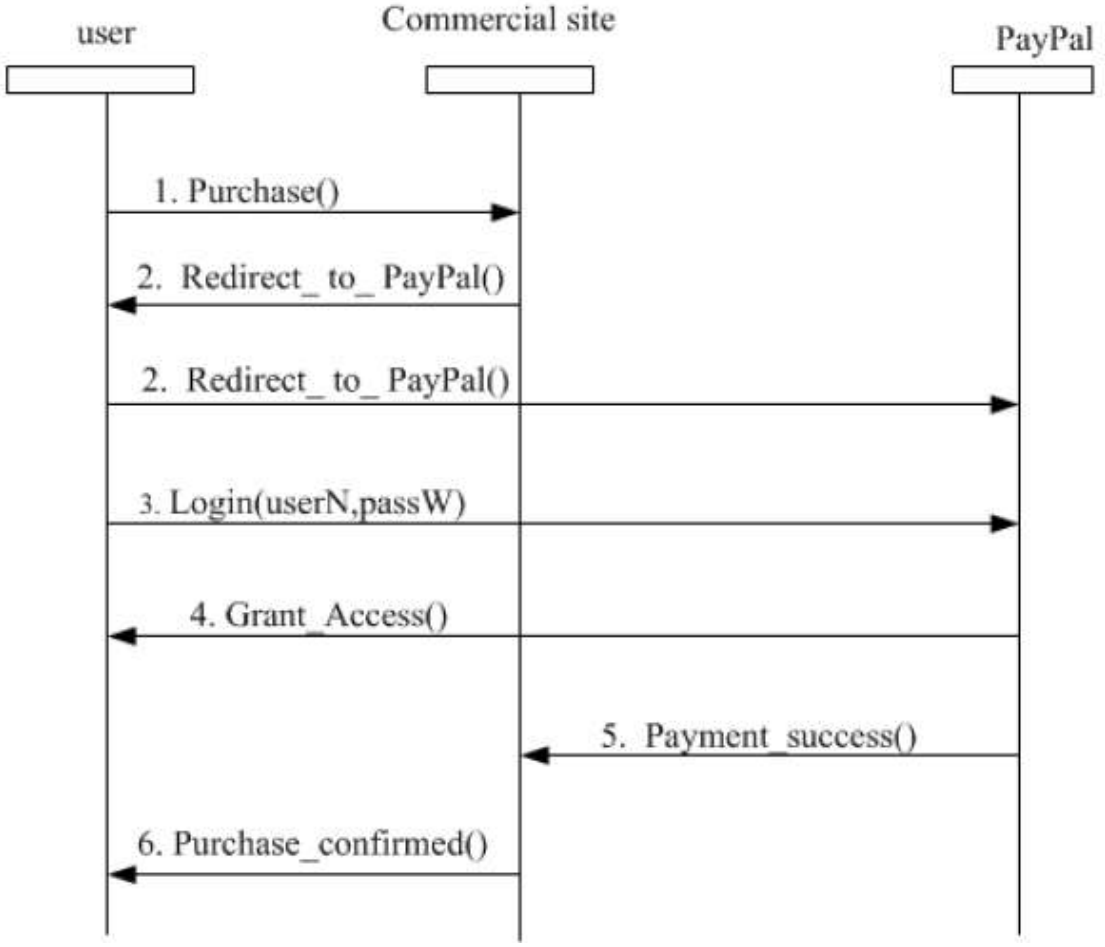

Figure 2: PayPal authentication process flow

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.

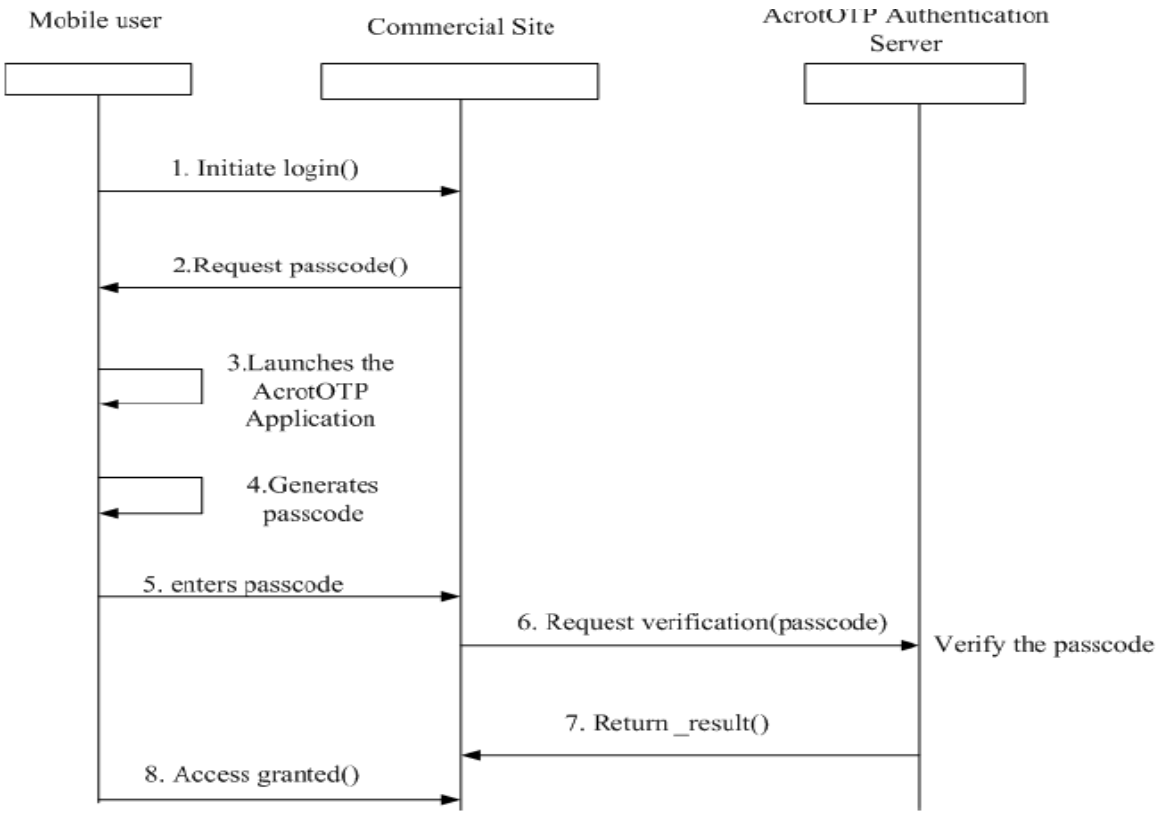

Figure 3: AcrotOTP authentication process flow

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 subsequently 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.

3.2.1 Data Flow of the Old System

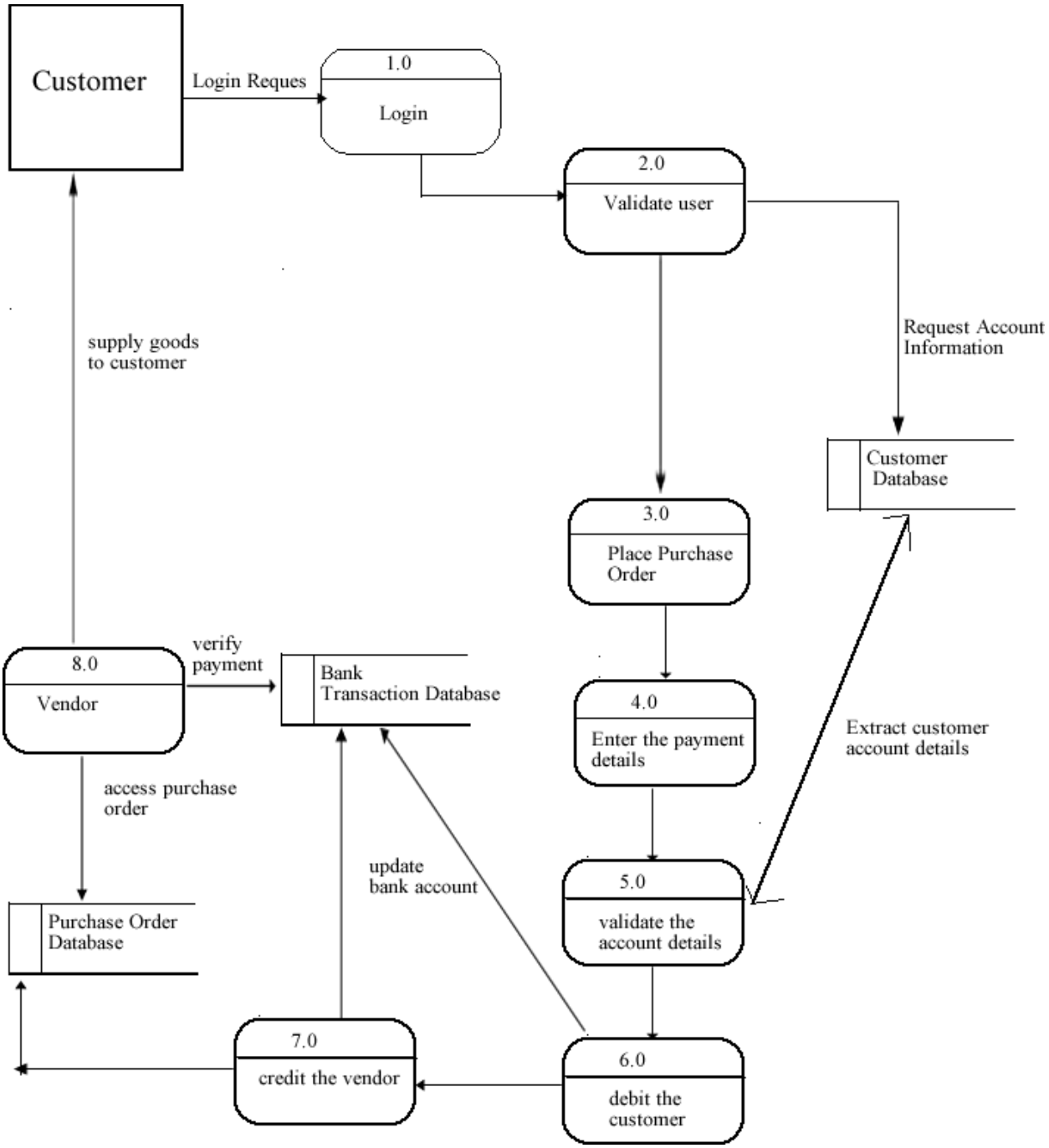

Figure 4: Data Flow Diagram of the E-transaction processing

In the system (figure 4), it 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.

4. ARCHITECTURE OF THE PROPOSED SOLUTION

The architectural model, as illustrated in Figure 5, is described as follows: threats target electronic transaction processing systems (assets). The threat actor(s) gain access to the assets via attack vectors and vulnerabilities present in the technology components that house or provide direct access to the targeted assets. Security controls are applied to the technology components with the intent to counter or mitigate the vulnerabilities and/or attack vectors used by the threat actors, thereby protecting the assets.

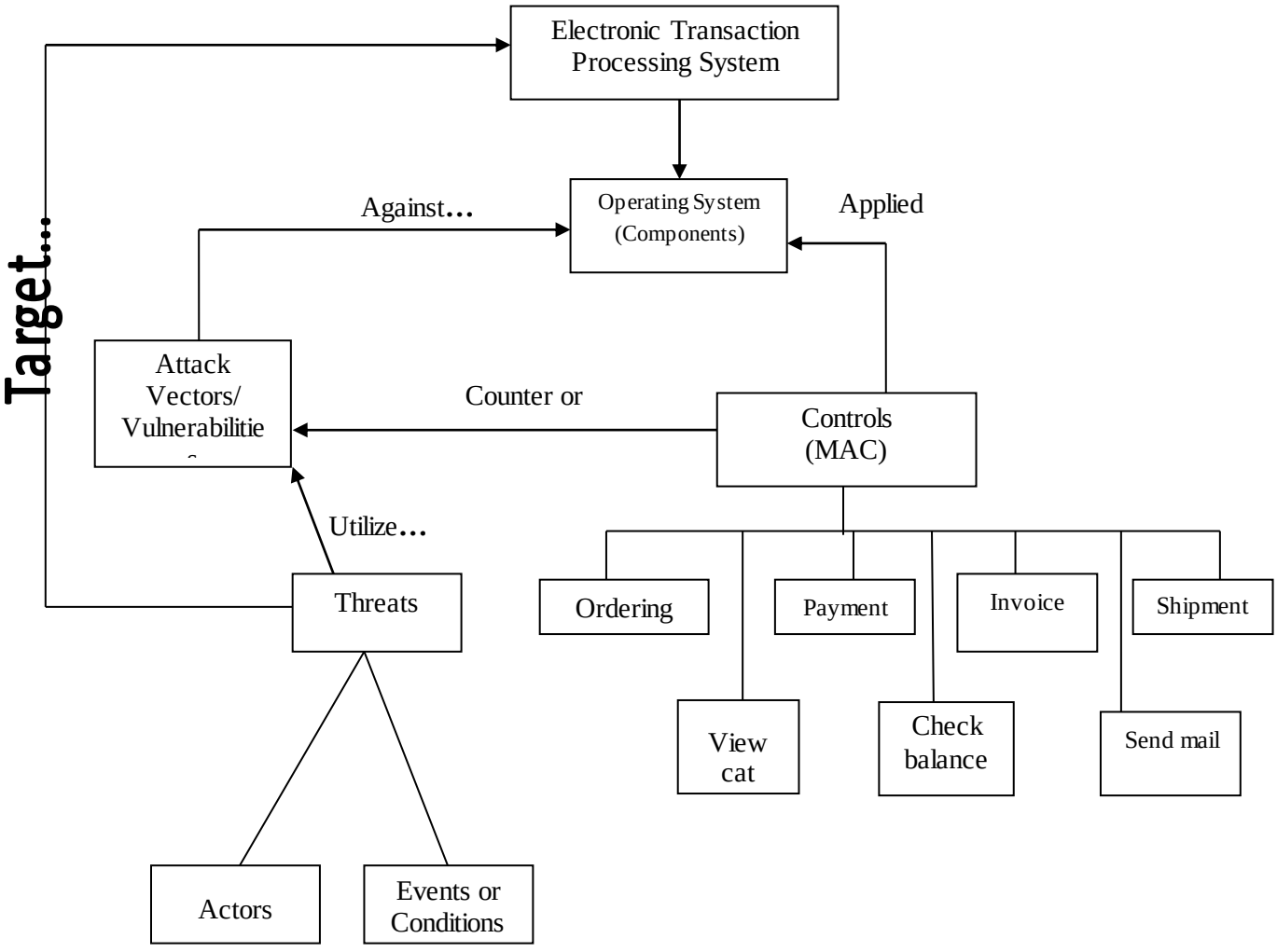

Figure 5: Architecture of the Proposed Solution

5. RESULT AND DISCUSSION

To identify the bottleneck and performance related issues we have tested the online transaction processing system using different methods and analyze the query and their execution path. We have taken records in every table of our database for simulation. We have executed some query by putting it into stored procedure using front end and query analyzer. We have taken random transaction ID several times. We have got the results with Hardware configuration: Intel® Duel Core 2.8GHz 2GB RAM as shown in table 1.

Table1: 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:
1. On Front –end is 0.0483 seconds
2. On Query Analyzer is 0.0577 seconds

Table 2: 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**

We have executed same query 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:

1. On query analyzer using Hash indexing technique is 0.0312 seconds.
2. On front end using Hash indexing technique is 0.0143 seconds.

6. CONCLUSION

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 paper 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.

REFERENCES

[1]. Schutzer, D. (2014). Cyber Security Trends. BITS/Financial Services Roundtable, 3(5), 247-255.

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

[3]. Olayemi, O. J. (2014). A Socio-Technological Analysis of Cyber Crime and Cyber Security in Nigeria. International Journal of Sociology and Anthropology, 6 (3), 116-125.

[4]. Jacobson, D. (2011). Security Literacy: tackling modern threats requires educating the general public about cyber security. Information Security Magazine, 13 (9), 23-24.

[5]. 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.

[6]. Geers, K. (2010). Live Fire Exercise: Preparing for Cyber War. Journal of Homeland Security and Emergency Management, 7 (1), 1-16.

[7]. 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.

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

[9]. 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.

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

[11]. 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.

[12]. Gercke, V. (2012). Cybercrime & Cybercriminals: An Overview. Estonia: CCDCOE Publication, 254-258.

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

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

[15]. Franco, L.; Sahama, T. & Croll, P. (2008). Security Enhanced Linux to Enforce Mandatory Access Control in Health Information Systems. Proceeding of 2nd Australasian Workshop on Health Data and Knowledge Management (HDKM 2008), Wollongong, Australia, 144-250.

[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.

[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.

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

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