Advances in Intelligent Systems and Computing 409

Suresh Chandra Satapathy
Amit Joshi
Nilesh Modi
Nisarg Pathak *Editors*

Proceedings of International Conference on ICT for Sustainable Development

ICT4SD 2015 Volume 2

Springer

Advances in Intelligent Systems and Computing

Volume 409

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

About this Series

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing.

The publications within "Advances in Intelligent Systems and Computing" are primarily textbooks and proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

Advisory Board

More information about this series at http://www.springer.com/series/11156

Suresh Chandra Satapathy · Amit Joshi
Nilesh Modi · Nisarg Pathak
Editors

Proceedings of International Conference on ICT for Sustainable Development

ICT4SD 2015 Volume 2

Springer

Editors
Suresh Chandra Satapathy
Department of Computer Science and Engineering
Anil Neerukonda Institute of Technology and Sciences
Visakhapatnam, Andhra Pradesh
India

Amit Joshi
Sabar Institute of Technology
Sabarkantha, Gujarat
India

Nilesh Modi
Narsinhbhai Institute of Computer Studies and Management
Kadi, Gujarat
India

Nisarg Pathak
Narsinhbhai Institute of Computer Studies and Management
Kadi, Gujarat
India

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-981-10-0133-8 ISBN 978-981-10-0135-2 (eBook)
DOI 10.1007/978-981-10-0135-2

Library of Congress Control Number: 2015955863

Printed on acid-free paper

This Springer imprint is published by SpringerNature
The registered company is Springer Science+Business Media Singapore Pte Ltd.

Preface

These AISC volumes contain the papers presented at the ICT4SD 2015: International Conference on Information and Communication Technology for Sustainable Development. The conference was held during July 3–4, 2015 at Hotel Pride Ahmedabad, India, and communally organized by ASSOCHAM Gujarat Chapter, ACM Professional Chapter, GESIA and Sabar Institute of Technology, Gujarat and Computer Society of India, as Knowledge Partner. The objective of this international conference was to provide an opportunity for researchers, academicians, industry persons, and students to interact and exchange ideas, experience, and expertise in the current trend and strategies for Information and Communication Technologies. Besides this, participants were also enlightened about the vast avenues, current and emerging technological developments in the field of ICT in this era, and its applications. The conference attracted a large number of high-quality submissions and stimulated cutting-edge research discussions among many academic pioneering researchers, scientists, industrial engineers, and students from all over the world and provided a forum for researchers. Research submissions in various advanced technology areas were received and after a rigorous peer-review process with the help of program committee members and external reviewers, 154 (Vol-I: 77, Vol-II: 77) papers were accepted with an acceptance ratio of 0.43. The conference featured many distinguished personalities such as Mr. Job Glas, Head of Mission, NBSO, Netherlands, Mr. Volkmar Blech, Zera Gmbh, Germany, Dr. Mukesh Kumar, TITS, Bhiwani, Dr. Vipin Tyagi, Jaypee University, Guna, Prof. Pravesh Bhadviya, Director, Sabar Education, Mr. Bipin V. Mehta, President CSI, Mr. Hemal Patel, MD, Cyberoam, Ms. Bhagyesh Soneji, Chairperson, ASSOCHAM, and Mr. Jay Ruparel, President, GESIA. Separate invited talks were organized on industrial and academia tracks on both days. The conference also hosted a few tutorials and workshops for the benefit of participants. We are indebted to ASSOCHAM Gujarat Chapter, Sabar Institute of Technology and Computer Society of India, ACM Professional Chapter for their immense support to make this conference possible on such a grand scale. A total of 18 sessions were organized as a part of ICT4SD including 15 technical, 2 plenary, and 1 inaugural

session. The Session Chairs for the technical sessions included Dr. Chirag Thaker, GEC, Bhavnagar, India, Dr. Vipin Tyagi, Jaypee University, MP, India, Dr. Munesh Trivedi, ABES Engineering College, Ghaziabad, India, Dr. Ramesh Thakur, DAVV, Indore, India, Dr. Dilip Kumar Sharma, GLA University, Mathura, India, Dr. Bhushan Trivedi, GLS University, Ahmedabad, India, Dr. S.M. Shah, KSV University, India, Dr. Nikita Vats Doohan, Indore, MP, India, Dr. Harshal Arolkar, GlS University, Ahmedabad, India, Dr. Priyanka Sharma, Raksha Shakti University, Ahmedabad, India, Dr. Nilesh Modi, KSV, Ahmedabad, India, Dr. Satyen Parikh, Ganpat University, India, Dr. Sakshi Kaushal, UIET, Punjab University, India, Dr. S.C. Satapathy, Visakhapatnam, India, and Dr. Nisarg Pathak, KSV, Ahmedabad, India.

We express our sincere thanks to the members of the technical review committee for their valuable support in doing critical reviews to enhance the quality of all accepted papers. Our heartfelt thanks are due to the National and International Advisory Committee and CSI Execomm Members for their support in making this a grand success. Our authors deserve big thanks since it is due to them that the conference was such a huge success.

Our sincere thanks to all the sponsors, press, print, and electronic media for their excellent coverage of this convention.

July 2015

Suresh Chandra Satapathy
Amit Joshi
Nilesh Modi
Nisarg Pathak

Contents

Committee

Advisory Committee

Mr. H.R. Mohan, Past President, CSI
Prof. Bipin Mehta, President, CSI
Mr. P.N. Jain, Add. Sec., R&D, Government of Gujarat, India
Dr. Srinivas Padmanabhuni, President ACM India
Dr. Anirban Basu, Vice President, CSI
Prof. R.P. Soni, RVP, Region III, CSI
Dr. Malay Nayak, Director-IT, London
Mr. Chandrashekhar Sahasrabudhe, ACM India
Dr. Pawan Lingras, Saint Mary's University, Canada
Prof. (Dr.) P. Thrimurthy, Past President, CSI
Dr. Shayam Akashe, ITM, Gwalior, MP, India
Dr. S.C. Sathapathy, Visakhapatnam, India
Dr. Dharm Singh, Windhoek, Namibia
Prof. S.K. Sharma, Pacific University, Udaipur, India
Prof. H.R. Vishwakarma, VIT, Vellore, India
Prof. Pravesh Bhadviya, Director, Sabar Education, India
Mr. Mignesh Parekh, Ahmedabad, India
Dr. Muneesh Trivedi, ABES, Gaziabad, India
Dr. Chandana Unnithan, Victoria University, Australia
Prof. Deva Ram Godara, Bikaner, India
Dr. Y.C. Bhatt, Chairman, CSI Udaipur Chapter
Dr. B.R. Ranwah, Past Chairman, CSI Udaipur Chapter
Dr. Arpan Kumar Kar, IIT Delhi, India

Organizing Committee

General Chairs
Ms. Bhagyesh Soneji, Chairperson, ASSOCHAM Gujarat
Mr. Jay Ruparel, President, GESIA
Mr. Bharat Patel, COO, Yudiz Solutions

Organizing Chairs
Dr. Durgesh Kumar Mishra, Chairman, Division IV, CSI
Dr. Rajveer Shekhawat, Chairman, ACM Udaipur Chapter

Organizing Co-chair
Dr. Harshal Arolkar, Associate Professor, GLS Ahmedabad

Members
Dr. Vimal Pandya, Ahmedabad, India
Dr. G.N. Jani, Ahmedabad, India
Mr. Nilesh Vaghela, Electromech, Ahmedabad, India
Mr. Vinod Thummar, SITG, Gujarat, India
Dr. Chirag Thaker, GEC, Bhavnagar, Gujarat, India
Mr. Maulik Patel, SITG, Gujarat, India
Mr. Nilesh Vaghela, Electromech Corp., Ahmedabad, India
Dr. Savita Gandhi, GU, Ahmedabad, India
Mr. Nayan Patel, SITG, Gujarat, India
Dr. Jyoti Parikh, Associate Professor, CE, GU, Ahmedabad, India
Dr. Vipin Tyagi, Jaypee University, Guna, India
Prof. Sanjay Shah, GEC, Gandhinagar, India
Dr. Chirag Thaker, GEC, Bhavnagar, Gujarat, India
Mr. Mihir Chauhan, VICT, Gujarat, India
Mr. Chetan Patel, Gandhinagar, India

Program Committee

Program Chair
Dr. Nilesh Modi, Professor and Head, NICSM, Kadi

Program Co-chair
Dr. Nisarg Pathak, SSC, CSI, Gujarat

Members
Dr. Mukesh Sharma, SFSU, Jaipur
Dr. Manuj Joshi, SGI, Udaipur, India
Dr. Bharat Singh Deora, JRNRV University, Udaipur
Prof. D.A. Parikh, Head, CE, LDCE, Ahmedabad, India
Prof. L.C. Bishnoi, GPC, Kota, India

Mr. Alpesh Patel, SITG, Gujarat
Dr. Nisheeth Joshi, Banasthali University, Rajasthan, India
Dr. Vishal Gaur, Bikaner, India
Dr. Aditya patel, Ahmedabad University, Gujarat, India
Mr. Ajay Choudhary, IIT Roorkee, India
Dr. Dinesh Goyal, Gyan Vihar, Jaipur, India
Mr. Nirav Patel, SITG, Gujarat
Dr. Muneesh Trivedi, ABES, Gaziabad, India
Mr. Ajit Pujara, SITG, Gujarat, India
Dr. Dilip Kumar Sharma, Mathura, India
Prof. R.K. Banyal, RTU, Kota, India
Mr. Jeril Kuriakose, Manipal University, Jaipur, India
Dr. M. Sundaresan, Chairman, CSI Coimbatore Chapter
Prof. Jayshree Upadhyay, HOD-CE, VCIT, Gujarat
Dr. Sandeep Vasant, Ahmedabad University, Gujarat, India

About the Editors

Dr. Suresh Chandra Satapathy is currently working as Professor and Head, at the Department of CSE at Anil Neerukonda Institute of Technology and Sciences (ANITS), Andhra Pradesh, India. He obtained his Ph.D. in Computer Science and Engineering from JNTU Hyderabad and his M.Tech. in CSE from NIT, Rourkela, Odisha, India. He has 26 years of teaching experience. His research interests include data mining, machine intelligence, and swarm intelligence. He has acted as program chair of many international conferences and edited six volumes of proceedings from Springer LNCS and AISC series. He is currently guiding eight scholars for Ph.Ds. Dr. Satapathy is also a senior member of IEEE.

Er. Amit Joshi has experience of around 6 years in academic and industry in prestigious organizations in Rajasthan and Gujarat. Currently, he is working as Assistant Professor in the Department of Information Technology at Sabar Institute in Gujarat. He is an active member of ACM, CSI, AMIE, IEEE, IACSIT-Singapore, IDES, ACEEE, NPA, and many other professional societies. Currently, he is Honorary Secretary of CSI Udaipur Chapter and Honorary Secretary for ACM Udaipur Chapter. He has presented and published more than 40 papers in national and international journals/conferences of IEEE, Springer and ACM. He has also edited three books on diversified subjects including Advances in Open Source Mobile Technologies, ICT for Integrated Rural Development, and ICT for Competitive Strategies. He has also organized more than 25 national and international conferences and workshops including International Conference ETNCC 2011 at Udaipur through IEEE, international conference ICTCS—2014 at Udaipur through ACM, international conference ICT4SD 2015—by Springer recently. He has also served on Organizing and Program Committees of more than 50 conferences/seminars/workshops throughout the world and presented six invited talks at various conferences. For his contribution towards society he has been awarded by The Institution of Engineers (India), ULC, the Appreciation Award on the celebration of Engineers, 2014 and by SIG-WNs Computer Society of India on ACCE, 2012.

Dr. Nilesh Modi has rich experience of around 13 years in academics and in the IT industry. He holds a doctorate in e-Security (Computer Science and Application). Continuing his research on cybersecurity, presently he is pursuing postdoctoral research on Wireless Communication and Security and certification as Ethical Hacking. He has a good number of research papers in his name and has presented more than 75 research papers in international and national journals and conferences. He has delivered a number of expert talks on e-Security and hacking in national and international conferences. Dr. Modi, a person with vibrancy, is an active life member of CSI, ACM IEEE, IACSIT, IACSI, and IAEng apart from his academic and industrial careers. As a consultant, he contributes to different system development projects with the IT industry and has carried out different government projects.

Dr. Nisarg Pathak is an astute and result-oriented professional with 10 years of experience in teaching and carving state, national, and international events like workshops, seminars, and conferences. Being a mathematics scholar and a computer science professional, he is actively involved in the research of data mining and big data analytics. He has a strong list of national and international publications to his name. Dr. Pathak is currently Associate Professor of Computer Science and Application at Narsinhbhai Institute of Computer Studies and Management affiliated to Kadi Sarva Vishvavidyalaya. He received his Ph.D. from Hemchandracharya North Gujarat University in Computer Science and his Master's in Mathematics from the same university. His other tenures include research fellow at Indian Statistical Institute, Kolkata, and Indian Institute of Science, Bengaluru.

Implementing the Logical Security Framework for E-Commerce Based on Service-Oriented Architecture

Ashish Kr. Luhach, Sanjay K. Dwivedi and Chandra K. Jha

Abstract Logical security of the modern E-commerce system is one of the major issues, effecting the growth of sophisticated E-commerce systems. Due to poor designing and configuration of the modern E-commerce's system, they lacked in quality attributes such as logical security. In the last decade, the number of highly equipped and trained intruders is increased significantly, due to increase in availability of computer systems and internet. These highly equipped and trained intruders are serious threat for the growing E-commerce industry. One of the leading Indian newspapers in 2013 reported about bugs on some of the most famous E-commerce websites such as Western Union and Facebook. This paper proposed a logical security framework for the small- and medium-sized E-commerce systems. The proposed logical security framework is inherited the benefits of service-oriented architecture and presents an analysis of the eminent security attacks which can be prevented. The proposed logical security framework is implemented and validated on osCommerce, an open source E-commerce.

Keywords Service-oriented architectures · Web services · Encrypted database · Security attacks · Legacy systems

1 Introduction

With the rapid development in information and communication technology (ICT), computers became the most valuable assets to the governing body. This rapid development in ICT transforms the physical existence of the markets and E-markets

A.Kr. Luhach (✉)
Dronacharya College of Engineering, Gurgaon, Haryana, India
e-mail: ashishluhach@gmail.com

S.K. Dwivedi
BBA University, Lucknow, U.P., India

C.K. Jha
Banasthali University, Jaipur, Rajasthan, India

S.C. Satapathy et al. (eds.), *Proceedings of International Conference on ICT for Sustainable Development*, Advances in Intelligent Systems and Computing 409, DOI 10.1007/978-981-10-0135-2_1

introduced. Organizations start moving toward fast and dependable systems to cope up with the changing customer's demands from legacy organizations. These legacy systems have established very important tactical elements to the arrangements. The maintenance of legacy systems increased, and outweighs the benefit they generate to the organizations [1]. Legacy systems can prevent enterprises from transforming toward E-commerce, but customers are quick to take over. For instance, an organization implemented a home-grown E-commerce platform 10 years ago, which has already updated its legacy systems numerous times in the final ten. Updating the existing system means patching up new functionality and operability on top of already built legacy systems, now the organization ends up with a scheme which is not upgradable or even difficult to put back. These systems were tightly coupled with their legacy systems, and it is almost impossible to shift from these legacy systems to fast and reliable systems without involving the business [2]. These legacy systems are not compatible with modern days E-commerce systems, as today's E-commerce systems have demands of dynamic commercial enterprise applications, which are developed on the concepts of loose coupling and flexibility.

Service-oriented architecture (SOA) is an information technology advancement in which the already existing applications of an organization employed with the various services available in a network, for example, World Wide Web. These types of services which can be easily integrated with the existing one can be developed using SOA. The main problems for developing sophisticated E-commerce systems are integration and transmission of information but SOA can ease the above-mentioned problem as SOA has the feature of loose coupling. SOA has the feature of open standard protocols and excellent encapsulation; this makes SOA the apt pick to employ E-commerce system [3].

2 SOA and Traditional Software Architecture

At present, lot of research is going on and various conferences being conducted on E-commerce to bring all the academician and researcher together to provide help and support to the organizations, so these organizations can migrate toward modern days E-commerce. The general idea behind developing SOA is to incorporate software into services. SOA applications are embedded into network services using XML. Web services attract organizations and various businesses to get the benefits of connectivity through the networks [4]. Table 1 shows the evaluation of various parameters between SOA and component-oriented software architecture (COSA) [5].

Table 1 Evaluation between SOA and COSA

Service-oriented architecture (SOA)	Component-oriented software architecture (COSA)
Flexible and loose coupling	Tight coupling
Harmonious services	Blocked applications
Information-oriented	Object-oriented
Independent of the implementation details	Deep understanding of the implementation details required
Development of interaction and reusability	Long development cycle
Flow-oriented	Function-oriented
Isomeric technologies	Isomorphic technologies

3 Security Analysis of SOA-Based E-Commerce

For accessing the E-commerce system, the users have to authenticate himself as a transaction or enterprise user. If an attacker bypasses this security mechanism of E-commerce system he will be able to gain access to the core database and product search area of E-commerce system. Figure 1 shows the generic system prototype of E-commerce system [2]. Figure 1 shows that the transaction users get access to the E-commerce platform that consists of various business service components, for example, customer information service, etc. through a web server but the enterprise user can access the business service components by directly communicating with simple object access protocol (SOAP). E-commerce system is not only used for online transactions but also can be practiced as a sequential publication of services such as banking services. Most of the E-commerce systems consist of various business services, for example, a famous E-commerce, Policybazar.com provides various services to their customer such as motor and health insurance. These different business services can be managed by diverse vendor or by different departments within the same organization such as Policybazar.com has different departments for the motor and health insurance which manage their own business services. The different services managed by the different departments make an E-commerce a service-oriented heterogeneous system [6, 7]. On the basis of literature review conducted for this research, it is concluded that this heterogeneous E-commerce system will have design and security issues which are as follows.

3.1 Certificate Duplicity

To gain access to E-commerce system components, user must have a valid certificate of authentication. The authentication certificate is issued by identity management service (IMS) upon the subsequent submission of authorized login credentials by the

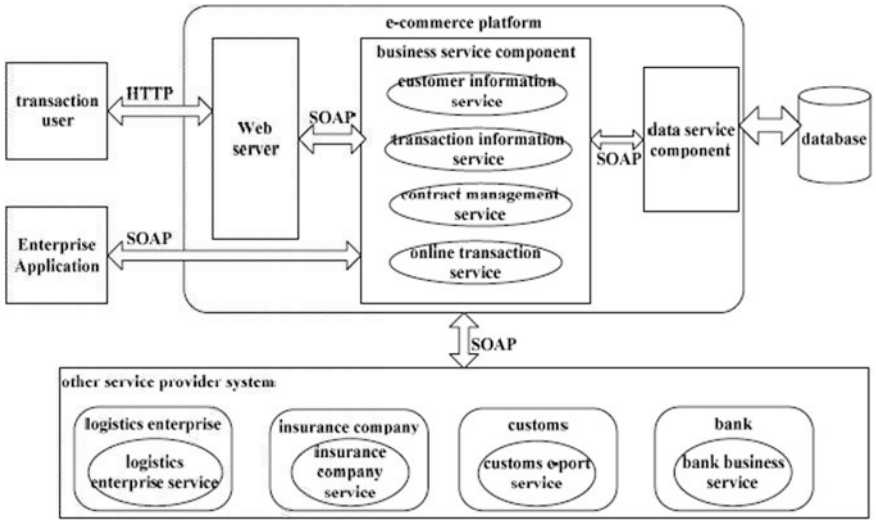

Fig. 1 System architecture of E-commerce platform

user. An intruder or attacker can generate the authorization certificate by gaining some kind of information from the user or through IMS.

3.2 Unsecure Protocols

All kind of communication between the user and E-commerce system is based on the protocols. The most common protocol used for this type of communication is hypertext transfer protocol (HTTP). In contrast, E-commerce requires a more sophisticated protocol for communication, when it comes to handle man-in-middle attacks by the attacker to access the important information from the communication. Man-in-middle attacks can be defined as the form of attacks in which intruder or attacker establishes a network connection with source and destination and relay messages between them giving sender and receiver an illusion that they are communicating directly [8].

3.3 No Filters Mentioned on the Application Level

Code or request filters may be used to block the security threats at the initial entry point of the communication with the E-commerce system. The absence of these kinds of filters at the application level can promote the attackers attempt, which may lead to a security attack. This type of attack which an attacker can perform in

the absence of the code or request filters is cross-site scripting and remote file inclusion [9].

3.4 Database Security

Database is the backbone of any E-commerce system and lot of emphasis put on the database security. Attacker can penetrate into E-commerce database without breaking an extra shell of the security which was not there. Infected database may lead to leakage of the sensitive information of the customers and organization [10].

4 The Proposed Security Framework and Implementation for SOA-Based E-Commerce

The proposed logical security framework has the benefits of SOA designing approach. The proposed logical security framework is designed to secure the E-commerce system from known computing threats or attacks. Figure 2 shows the proposed logical security framework. In the proposed logical security framework both the transaction and enterprise users can communicate with the E-commerce system through SOAP instead of earlier or traditional frameworks in which only the enterprise users can directly communicate with E-commerce system through SOAP. The proposed logical security framework consists of a special code or request filtering security layer known as input sanitization and all transaction/enterprise users requesting to access the business service components of the E-commerce system are conceded through this additional security layer. Rule-based plug-in is defined in the proposed logical security framework which implements an additional security layer. For efficient monitoring of the incoming and outgoing packets, intrusion detection system (IDS) and intrusion protection system (IPS) are employed in the proposed logical security framework. With the help of IDS and IPS, each and every packet is monitored and infected packets can be blocked or traced easily. Figure 2 clearly shows that the database of the E-commerce is maintained on a completely different web server named as Server 2 in the proposed logical security framework. All the business service components are maintained on a different web server named as Server 1. The communication between Server 1 and Server 2 is closely monitored by the IDS and IPS, which actually create additional layer of defense from attacker attempt. By placing both business service components and database on different servers, it is very easy to disconnect the database from the E-commerce to ensure the minimal loss of the sensitive information either related to customers or organization.

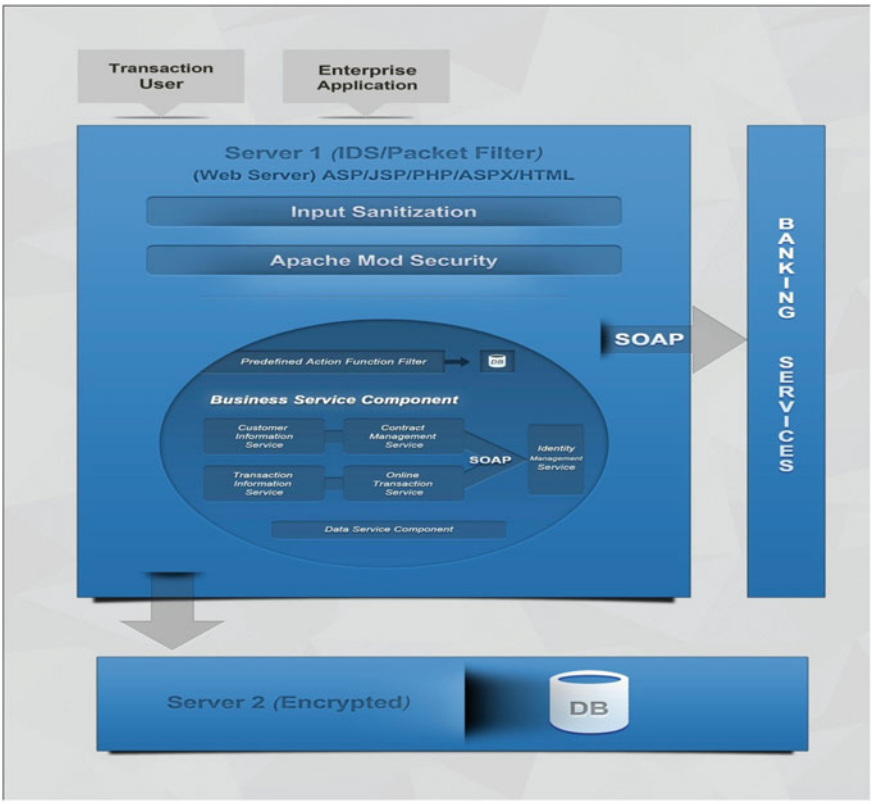

Fig. 2 Proposed logical security framework

5 Usage Scenario

In this part, we look at the usage scenario of the suggested framework. Figure 3 depicts the flow of events in this scenario and the interaction directions between different elements.

- The end user would like to access the E-commerce, for example, a user attempting to buy DVDs from an E-commerce site. He accesses the information related to DVDs under the movies section using his login credentials.
- The web application running on the E-commerce websites uses SOAP messaging and HTTPs for communication.
- The authentication assurance services, which are based on username and password pairs, permit the users to access the DVDs detailed information. The authentication assurance is managed by IMS. To access the business service component uses must be successfully through IMS.

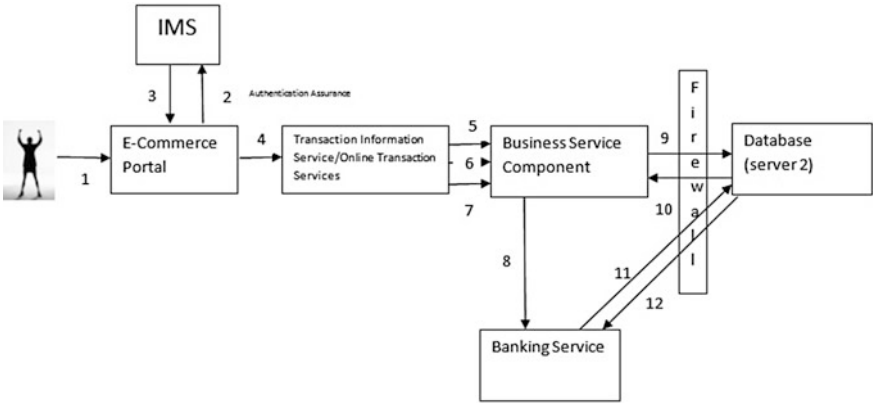

Fig. 3 Usage scenario of the proposed framework

- The user's service requests are first sanitized and then monitored by IDS/IPS before being forwarded to the database.
- The database is maintained on different servers and connected to business service components via firewall.
- Banking services can be accessed through business service components and connected to the database via firewall.

The presented scenario outlines how the proposed framework fulfills the security essential for today's E-commerce system. First, input sanitization solves the risk of certificate duplicity. Predefined actions, filters mentioned in proposed framework, are responsible for separating out the actions specified on web pages. The database is maintained onto a totally different server, which is monitored by IDS/IPS. The presentation of IDS/IPS will avoid the denial of service attempts.

6 Results and Discussion

The proposed logical security framework is validated on an open source E-commerce system, osCommerce. osCommerce provides free of cost online E-commerce solutions for various organizations. osCommerce allows organizations to arrange up their online stores without software costs or license fees. Till now, the osCommerce community provided more than 5,000 add-ons that are absolutely free of cost. osCommerce also provides customized solutions for individual clients equally well. osCommerce implemented with PHP as web scripting language and uses MySQL as database for their server data. The combination of PHP and MySQL allows osCommerce Online Merchant to run on whatever network server environment that supports PHP and MySQL, for example, Linux, Solaris, BSD, Mac OS X, and Microsoft Windows environments. osCommerce was started in

March 2000 and has since matured to a solution that is powering many thousands of online shops around the globe. The implementation benefits which are already implemented so far for the proposed logical security framework are discussed below.

6.1 Input Sanitization

It provides an extra layer of security for the proposed logical security framework as it verifies all the incoming packets submitted by the attacker or user. If the user request consists of any special characters to bypass the security layer such as '#@123*,' this extra layer of security will clean the user submitted input as '123' and forwarded to the next layer for further operation. This extra layer will resolve the issue of certificate duplicity. The highlighted text shown in Fig. 4 is a sample of infected input submitted by the attacker to bypass the security mechanism of an E-commerce system. The input sanitization layer of the proposed logical security framework will clean the infected input submitted by the user as shown in Fig. 5.

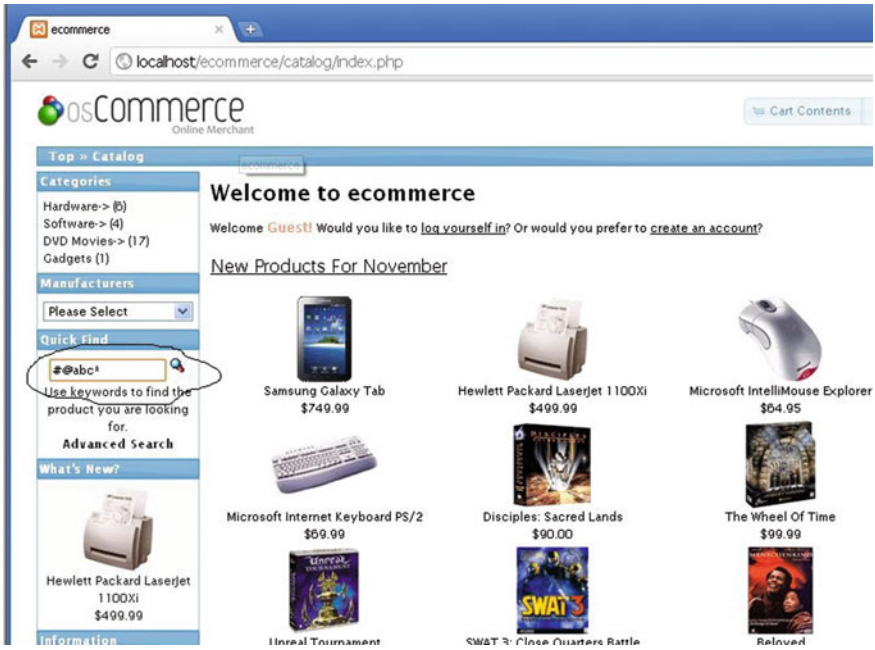

Fig. 4 Sample of infected input

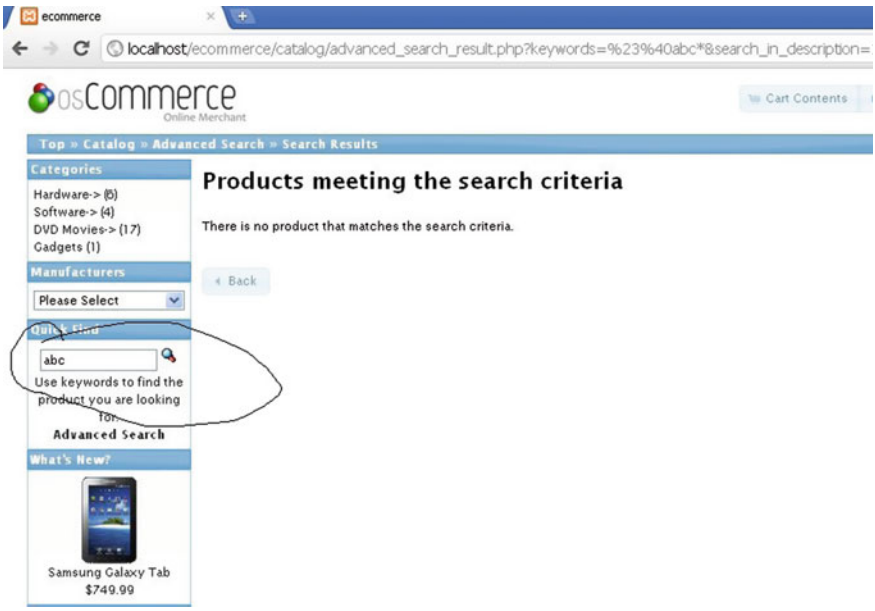

Fig. 5 Sanitizated input by the proposed logical security framework

6.2 *Rule-Based Plug-in for Additional Security*

This security layer provides an extra layer of security for the proposed logical security framework. This layer comes into play when the attacker successfully bypasses the initial layer of filtration which is input sanitization layer. This additional security layer is created by defining the various rules for accessing the business service component of the E-commerce system. These rules are just another filtering and blocking technique for the input submitted by the user. The user request is matched with the created rules and if matched with the created rules, then the user requested is blocked and rejected. Figure 6 shows the sample user attempt for retrieving the important information without proper means of authentication. Figure 7 shows that the users attempt is filtered and blocked by the proposed logical security framework. The user request was denied and web page remains the same as highlighted.

6.3 *Predefined Action Filters*

These types of action filters are used to block the attacker attempt of remote code execution or SQL injection. If somehow attacker bypasses the input sanitization and rule-based plug-in for additional security and able to execute his infected code, then

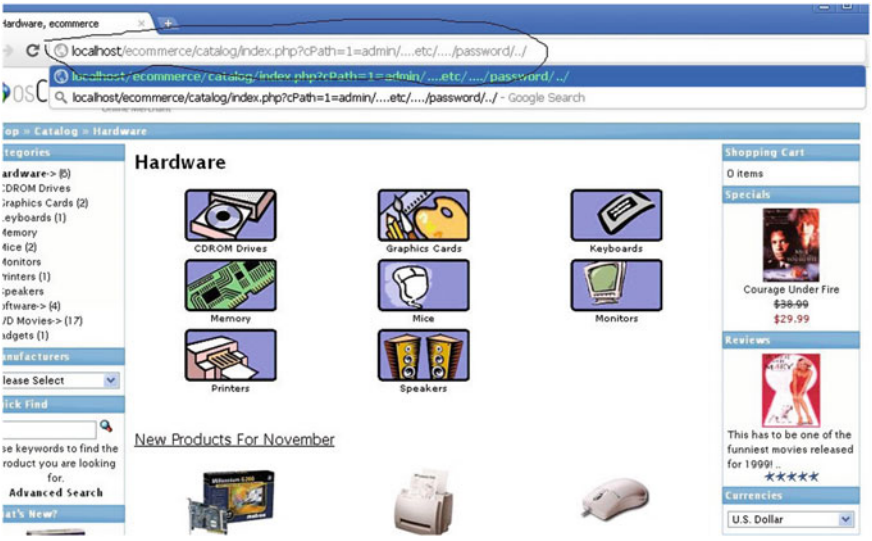

Fig. 6 User attempts to include the local files into their commands

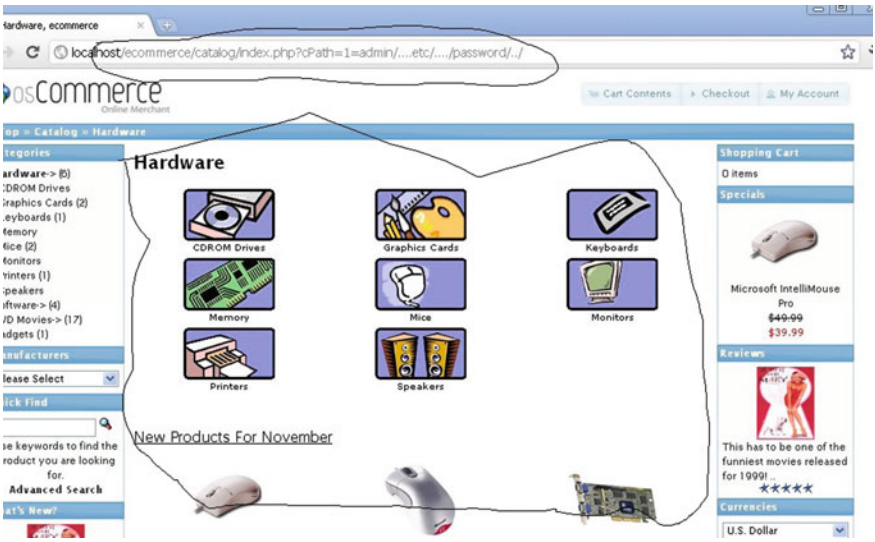

Fig. 7 Local file inclusion is blocked by proposed security design

these predefined action filters block the infected code or program executed by the attacker. Figure 8 shows user attempt of SQL Injection as infected URL and Fig. 9 shows the filtering of the same for the proposed logical security framework and the web page remains the same.

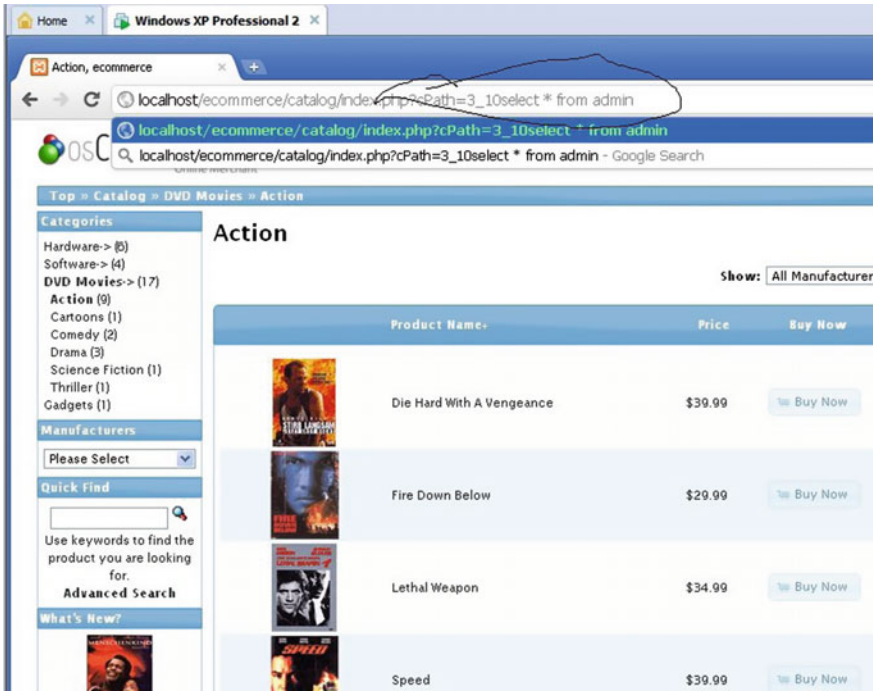

Fig. 8 User attempt of SQL injection

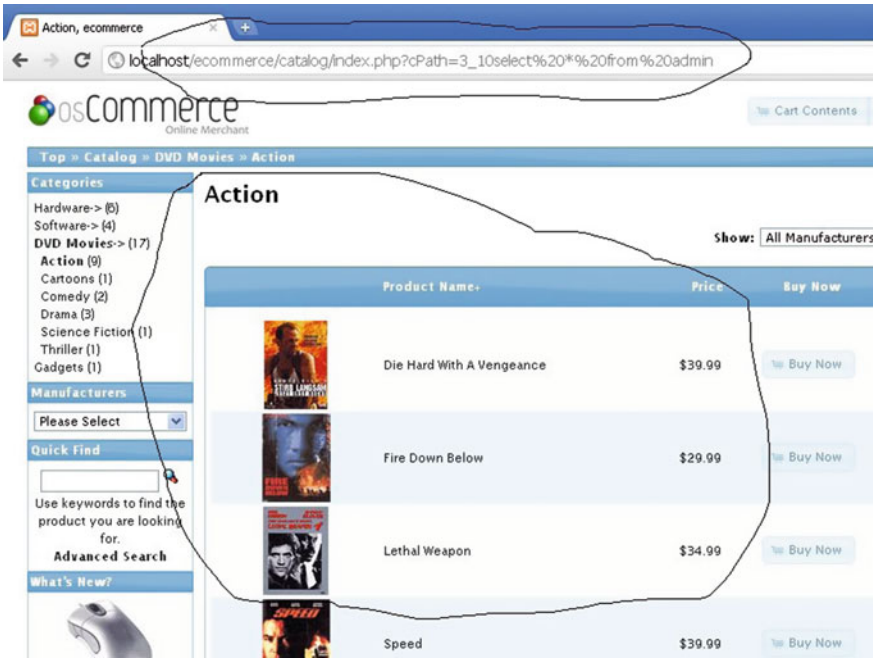

Fig. 9 Action filtering for the proposed security design