A Web Application Security And Web Mash-up Development Using AOP

Indranil Choudhury
Department of Computer Engineering
Indira College of Engineering and
Management, Pune, India
Email: indranil82@gmail.com

Prof. Manjusha Tatiya
Department of Computer Engineering
Indira College of Engineering and
Management, Pune, India
Email:
manjusha.tatiya@indiraicem.ac.in

Abstract: Web application security has come to be of vital significance over the years. In the event that specific estimates aren't taken, a specific arrangement or execution may present vulnerabilities which may furthermore affect the privacy/classification, reliability and availability of the application and measurements/stats included. Safety shortcomings in web programs are regularly simple to misuse. Hacking programmers are for the most part watchful for security shortcomings. Programming programs as web Mashup advancements experience the ill effects of various issues like reduction in modularity. Deficiency of adaptable security plans repress engineers from effectively and safely downloading and joining source codes from different sites over the world. Accordingly, modularity/particularity is a significant viewpoint for different segments of a mashup framework. Measured quality is the consenting viewpoint for enormous scale web and S/W programs for reusability of code. On the off chance that there's adequately one designer or programmer, there may not be a requirement for seclusion. The seclusion ends up critical when various programmers are working without coordination with each other. Without precisely expressed interfaces, creating alteration might be evident to everybody. The lack of real seclusion is a primary insufficiency that slows down web programming and blend improvement in an essentially social manner among various programmers. This seclusion is a basic quality of Aspect Oriented Programming, which is the base of this paper, with regards to the area of web-mashup, and the relating ease with which web-security can be actualized utilizing AOP.

Keywords: Well-defined interfaces, Integrity, Modularity, Confidentiality, Accessibility, Web-mashup, Web Mining, Security, Aspect oriented programming.

Introduction

The web application security and web mashup development for providing the security to web applications using new proposed methods. In this research work, the main focus is given on the Aspect-Oriented programming (AOP) that supplied the power to modularize cross-cutting issues and security in a software gadget [9]. The system provided right here, provides the benefits of AOP i.e. Simultaneous parallel decay of orthogonal concerns that is termed as application transparency and another gain is that the software program programmers and designers can consciousness on their respective situation. One of the maximum common issues is modularity and protection of web software and web mashup which turn out to be one of the most up to date buzzwords in the net applications area, and multiple of agencies and organization are dashing to offer mashup answers The goal attempted in this research work is to use AOP as one of the major tool to design a unique security framework that even if the developer had not considered security as a one of the component of web application in the beginning, at a later stage it should be free (safe) from major vulnerabilities and attacks. The Separation of worries is a recognized technique for the department of a software program mission's problem domain into numerous different factors known as modules. Latest programming languages like OOP make it hard, and occasionally not possible [2], to isolate certain worries into conceptual modules for next translation into pc code. Protection is one challenge that cannot be distributed by traditional methods as it has a tendency to get tangled with the alternative code in a software program device. Aspect -orientated programming (AOP) makes it viable to isolate this and different worries that have been previously inseparable into modules. It is crucial to realize the number of the history and motivation behind the usage of thing-oriented programming (AOP) to individual a protection concern from the enterprise good judgment in an organization environment. And also the aims and objectives of the proposed research work in constructing an AOP based software system to develop concrete methodology a way to separate the security aspect from the main logic of the system [5,6].

Literature Survey

According to Heba A. Kurdi [1], showing the Aspect-oriented programming (AOP) this is explains a promising programming approach for the necessary for non-functional elements attribute, thus as logging, error handling and fault-tolerance. This is used to the alternate concerns and shows the big difficulty that conventional programming model could not modularize really major to an intricate code. In this innovation paper represents the AOP techniques, these are required that led to it, how it provides the better outputs in code quality and S/W developments efficiency, followed by stating difficulty that developers and researchers face when dealing with this techniques.

According to Jose M. Felix [2], depicted the division of concerns plan guideline enhances programming reutilization, comprehend capacity, extensibility and viability. By utilizing the protest situated worldview, it isn't generally conceivable to isolate into free modules the diverse worries of an application. The result is that source code of intersects focus are scattered and tangled across the whole application. The AOP provide a huge amount of measured quality, giving an answer for the code disturbance and scatter problem. To show how to aspects managed programming can be used as a moderate model to improve the determine quantity of question situated applications, this divulgate article introduces the usage of atypical outline design following both the protest and perspective situated ideal models.

According to Cinzia Cappiello [3] concentrate on Modern Web 2.0applications are portrayed by high client association: clients get bolster for making substance and comments and additionally" creating" applications utilizing substance and capacities from outsiders. This last wonder is known as Web Concoction and is picking up ubiquity even with clients who have few programming aptitudes, raising an arrangement of impossible to miss data quality issues. Surveying a blend’s quality, particularly the data it gives, requires seeing how the concoction has been produced, how its segments resemble the other alike, and how quality spreads from essential segments to the last concoction application.

According to Brent Ashley [4] presenting the current web browsers security issues. The current browsers are not designed for security to get content by the many sources for the web applications pages. They describe the use of available tools by the developers to complete the assigned task and the results of the web applications for the applications security and scalability. To learn about the many current browser improvements for proposed remedy to multiple situation. To become the part of the communication in development beyond to this hurdle to the interoperability.

According to Jinyu [5] introducing the web mashups development. The web applications are developed using the contents and the service. It is available on internet. Despite of increasing interest in mashups developments, comprehensive development tools, frameworks and it is used in large cases for mashing up recent applications to imply the important manual programming difficulty. This research paper represents that reviews of recent tools, approach and the techniques implements to help for mashup developments. The researcher is using a set of attributes dimensions to highlight the strengths and weaknesses of several representative models.

According to Gerald Bader [6], describing the Evolution of internet 2.0 applications has modified the review of commercial enterprise approach and institution. Industry required considering their advertising, conversation and sale channels and how to their client and employees communicates with externally or internally. The recent scheme, in contributed they desire to undertake their IT infrastructure and rising their on-line presence and offerings as a way to live aggressive of their organizations. Via this methodological conversion to internet 2.0 paradigm current securities and privacy issue increasing which ought to be deliberates to protection the fully RIA (rich internet application).

According to Jonas Magazinius [7] supplying the internet mashup is an internet software that combine content from different providers to make a recent service, no longer supplied through the content vendors. As mashups increase in demanding, the disturbance of secure facts drift among mashup additional turns in growing critically. In this innovation paper provide protection lattice-based whole techniques to mashup safety, in which the origins of the distinctive elements of the mashup are utilized as tiers Distinctive and include the security lattice. Declassification enable handled facts launch among the elements. The author define a approach of combined define launch scheme and provides for realistic (static as well as runtime) implementation of mashup statistics-glide safety rules in an internet browser.

According to Kotrappa Sirbi [8], defined an application security has two primary dreams: first, it is meant to save you unauthorized personnel from having access to data at better category than their authorization. Second, its miles supposed to prevent employees from declassifying data. Using an object oriented technique to implementing application security consequences no longer most effective with the issues of code scattering and code tangling, but also outcomes in weaker enforcement of safety. This weaker enforcement of security might be due to the inherent layout of the gadget or because of programming errors. Aspect orientated Programming (AOP) complements Object Oriented Programming (OOP) by using supplying another manner of considering program shape. The important thing key unit of modularity in OOP is the magnificence, while in AOP the unit of modularity is the component. The goal of the paper is to present that aspect orientated Programming Aspect J integrated with Spring AOP presents very powerful mechanisms for stronger enforcement of safety.

According to RohitSethi [9], implementing the Aspect -orientated programming (AOP) is a scheme is fast growing grip within the increase international. At least partly prompt with the support of the popularity of the Java Spring framework [1], human are conception to detection the significant advantages that AOP to implementation. At the same time as some others have firm AOP security, the author suggest that, the main objectives of this innovation to detecting among data safety colleagues that AOP could have a substantially useful impact on application safety. The author suggest that, developer are implemented the better application to make the secure programs and perhaps, more significantly add safety in to existing self-consciences applications.

According to Nicolai Kuntze [10], expressed the identity control is becoming an increasing number of essential in enterprise systems as they're opened for third events consisting of trading companions, purchasers and providers. This paper affords an approach securing a device with none understanding of the gadget source code. The security module provides to the existing device authentication and authorization primarily based on element oriented programming and the liberty alliance framework, an upcoming industries fashionable imparting single sign on. In a preliminary education segment the module is adapted to the utility that's to be secured. Furthermore the use of hardware tokens and proactive computing is demonstrated. The excessive modularization is achieved thru use of Aspect a programming language extension of Java.

Problem Description

Design a unique and concert security framework to address a security and modularity problem encountered specially in web Mashup application in that even if the developer had not considered security and modularity as a one of the component of web application in the beginning, at a later stage it should be free (safe) from major vulnerabilities and attacks with the help of new programming paradigm i.e. Aspect oriented programming (AOP).

Scope of System

Multiuser mashups: The mashups analyzed in the previous chapter were like conventional Web applications, that is, instantiated independently for each individual user of the mashup.

Mobile mashups: In line with the general trend in software/Web engineering and the growing demand coming from a user basis that is increasingly accessing the Web via mobile devices, mobile mashups aim at bringing mashups to mobile devices, such as mobile phones or tablets

Telco mashups: Bringing together the power of both multiuser and mobile mashups, telco mashups are mashups that aim to provide people with novel, integrated communication capabilities and features. Both real-time (synchronous) and non-real-time (asynchronous) communications are possible.

Enterprise mashups: Finally, enterprise mashups are mashups that usually run inside enterprise boundaries. While all the above-mentioned mashups and the mashups introduced in the previous chapter focus on the satisfaction of functional requirements, if mashups are to be executed in an enterprise environment some nonfunctional requirements also become important.

Proposed System

In this research, we propose a complete platform to extract the web data from various platforms on a single portal. The system is designed so as to be able to eliminate different network attacks like SQL Injection, DOS, and man in the middle (MiM) etc. The system illustrates in entire architecture how the system communicates with various web domains and extracts the data in data stream. A number of middleware attacks chould be possible during the data transmission, thus the proposed work also takes care of data security.

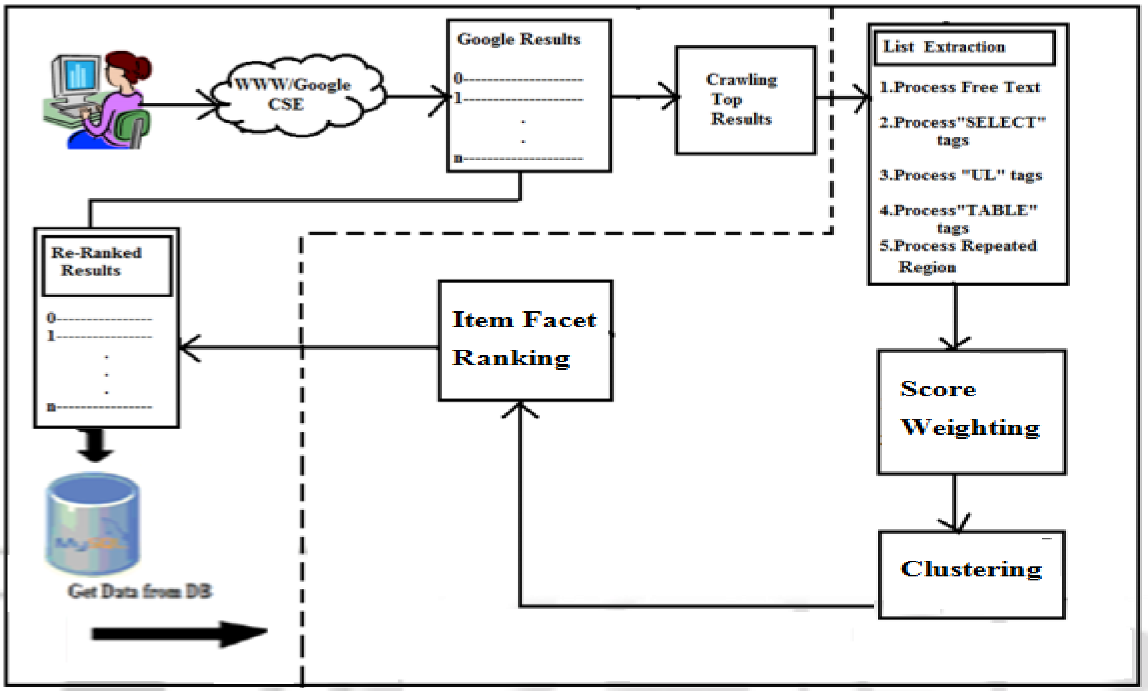

Figure 1 : Web page extraction

We develop a pattern matching based algorithm to check the runtime queries and prevent then automatically in case it contains malicious parameters. Below figure 1 illustrates the overall system architecture with current execution.

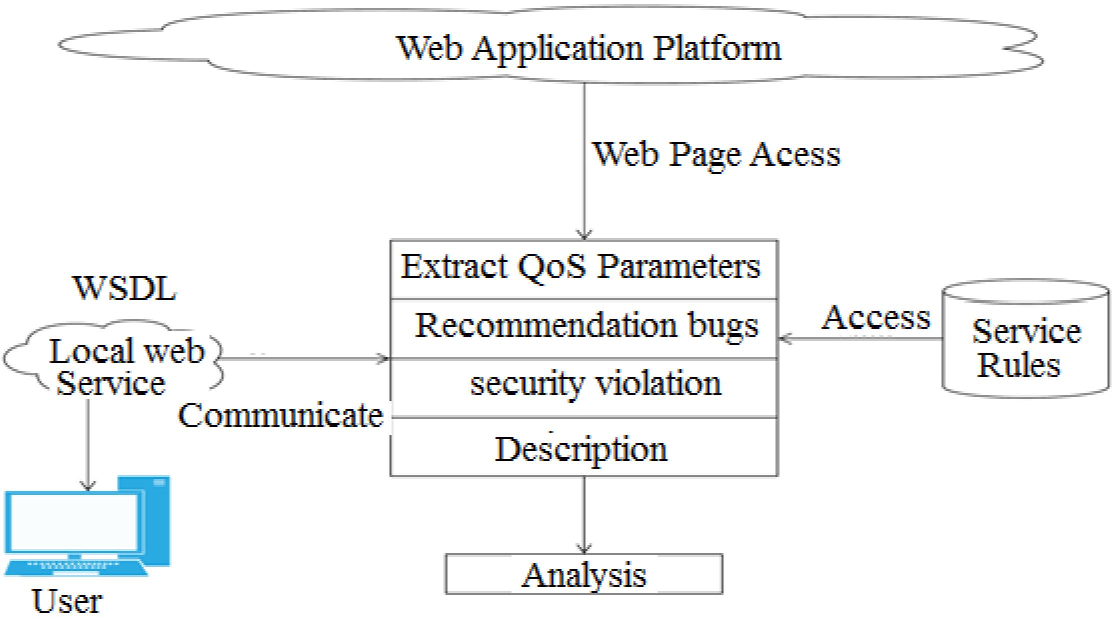

Figure 2 : Proposed system architecture

If a person wishes to change the invocation of the code associated to crosscutting concerns, he needs to alternate every distinction that includes such an invocation. Doing so breaks the Open/close precept-opens for extension, however closed for changes. The overall outcome is a higher price for presenting features and fixing bugs. Now these problems can be solved by a new programming paradigm like aspect-oriented programming (AOP).

Algorithms Design

Document webpage retrieval Algorithm

Input: Users query as Q , Network Connection N;

Output: result from relevancy calculation top k pages base on Q.

```
Step 1: User provide the Q to system.
Step 2: if (N!=Null)
        Process
        Read each attribute A from ith Row in D
        Res[i]=Calcsim(Q,A)
Else No connection
Step 3: For each(k to Res)
Step 4:  Arraylist Objarray to bind Q to Res[i] or k
Step 5: Return to users Objarray
Step 6: Display Objarray
```

Weight Calculation Algorithm

Input: Query generated from user Q, each retrieved list L from webpage.

Output: Each list with weight.

Here system have to find similarity of two lists: $\vec{a} = (a_1, a_2, a_3, \ldots)$ and $\vec{b} = (b_1, b_2, b_3, \ldots)$, where a_n and b_n are the components of the vector (features of the document, or values for each word of the comment) and the n is the dimension of the vectors:

```
Step 1: Read each row R from Data List L
Step 2:  for each (Column c from R)
Step 3:  Apply formula (1) on c and Q
Step 4: Score=Calc(c,Q)
Step 5: calculate relevancy score for attribute list.
Step 6: assign each Row to current weight
Step 7: Categorize all instances
Step 8: end for end procedure
```

Mathematical Model

AOP mathematical model for QoS based Aspect Selection &

Petri Net Algebra:

The selection of net services is controlled by means of the option module with the level of QoS necessary as the input. This methods of service selection, entire service which content the measuring QoS level are been selected.

Let N = {WS1, WS2, WS3…WSn} be the set of internet service recorded in the record.

Determined QoS = (Service Req, Expected Res)

WSSelect = select (WS_Non_functional_params, DeterminedQoS)

An attribute is provided in 3 tuple elements thus are provider, role and description. The Role identify whether or not it has to be carried out earlier than, after or around.

Petri Net Algebra

A Petri internet offers modeling technique for specifying formal metrics. Its miles observe as a instruments for recognize the efficiency of the implemented formal semantics The set of rules (AoWSC) is designed to element – orientated web service Composition.

Algorithm: AoWSC.

```
Step 1: Initialize.
Step 2: Service Req =
Step 3: Determined QOS = f (Service Req, Expected Res).
Step 4: For eachi in Service Req
Step 5: Search (Serviceregistry, Concept (i))
Step 6: Add To Temp Candidate WS List ().
Step 7: For each j in Temp Candidate WSL ist
        If (chk Qos (WS (j) > Determined Qos)
        Add To Candidate Ws List ()
Step 8: End For
Step 9: End For
```

Results and Discussions

Table 2: Comparative analysis of system

Comparative Factor	Proposed System (AOP using VCS)	Facet Search Using TF-IDF	Semantic based RDF search	Hierarchy based spatial clustering	Object Search
Reliability	High	Medium	Low	Medium	Medium
Security	Medium	Low	Medium	Low	Medium
Performance	High	High	Low	Medium	Low
Portability	Yes	No	Yes	Yes	Yes
Configuration	Medium	Low	Medium	Low	Medium
Compatibility	Highly Compatible New operating environments	Medium	Low	Low	High

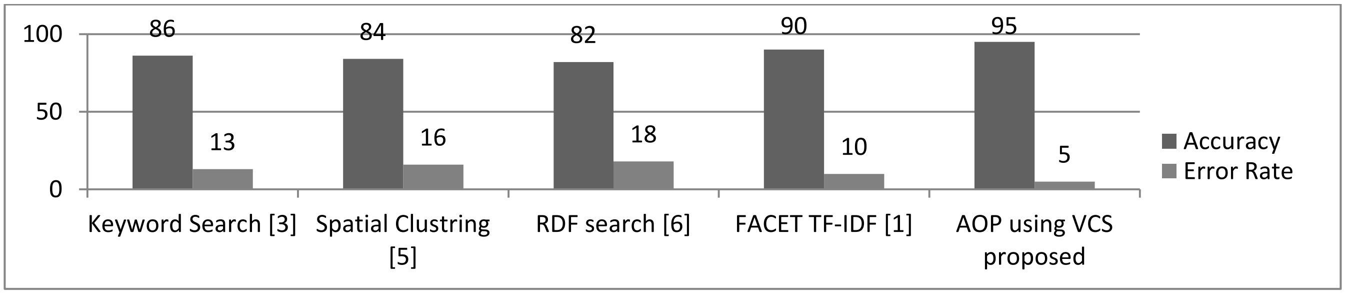

Figure 2: Accuracy between proposed vs Existing systems

According to above figure 2, we examine proposed system performance analysis with some existing systems. We measure the accuracy parameter for different kinds of search queries and measure the performance based on different confusion Matrix parameters. The proposed system provides around 95% accuracy, and 5% average error rate to entire execution. The keyword search [1], RDF [6], spatial clustering [5] and facet based keyword search [1] are the existing systems used to evaluate our proposed system. It increases around 5-6% accuracy compared to other existing systems, while it reduces the error rate around 8-10%.

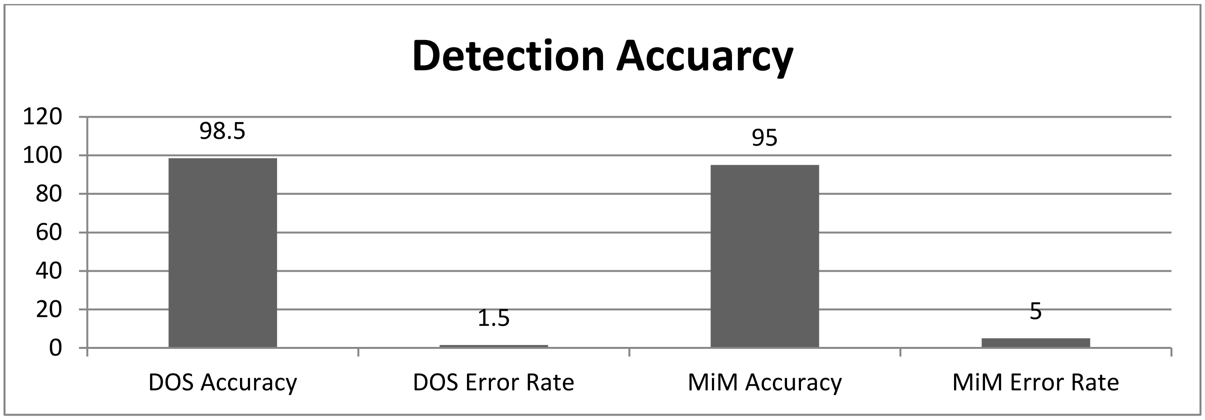

Figure 3 : Time required for data encryption in milliseconds with various attribute set

The figure 3 shows the system performance evaluation that was done with virus experiment analysis. In entire system, we have done different experiments with all models and calculated the average results which are shown in figure 3 and figure 4. Finally, we conclude the proposed system is able to handle role based access control with data security in untrusted network environment as well as it also able to defend various kind of network attack like DOS or MiM etc.

Conclusion

In the proposed system, we provide AOP based application, for better user preference as well as to provide the different web results on a single platform. Initially, system extracts the web data from various streams and combines it into a Mashup platform. The system also illustrates defence mechanism from various network attacks, denial of services (DOS) and man in the middle (MiM) are the attacks which are successfully prevented by the system. Sometimes the system has to face some privacy constraints from different web applications, which prevents the data extraction, in such a scenario it will return a null value for empty results. It is mandatory to allow two accessibility rights of web pages whenever we access the data from different web portals for application. Finally, the system provides good results compared to other classical existing systems which are used for user preference for personalized search engines.

Future Work

The system can be implemented on various cross platforms and can apply the various security parameters which can provide drastic supervision for sensitive data of users as well as applications. To combine various platform's data using AOP with different security mechanisms, using deep learning for machine learning approaches. This will provide the highest security against different network attack. To gain accurate results is the other measurable parameter to focus in future work which provides better user preference to such systems.

References

[1] Heba Kurdi A. Computer Science Department Imam Muhammad Ibn Saud Islamic University

Riyadh, Saudi Arabia. Review on Aspect Oriented Programming" International Journal of Advanced Computer Science and Applications. 2013; 4(9):22.

[2] Jose Felix M. Principality of Asturias, Computer Science Department, Oviedo, Spain Francisco Ortin, University of Oviedo, Computer Science Department, Oviedo, Spain, Aspect-Oriented Programming to Improve Modularity of Object-Oriented Applications. Journal of Software. 2014; 9(9). doi:10.4304/jsw.9.9. Pages 2454-2460

[3] Cinzia Cappiello, Politecnico di Milano, Florian Daniel, Maristella Matera Cesare Pautasso Itely and Switzerland "Information Quality in Mashups Int'l Journal, Internet Computing. 2010; 14(4):14-22.

[4] Website Brent Ashley. Shaping the future of secure Ajax mashups Available at http://www.ibm.com/developerworks/library/x-securemashups/ Pub 3-4-07 accessed on 8 Nov 2010

[5] Jin Yu, Benatallah B, Casati F, Daniel F. Understanding Mashup Development Int. Journal Internet Computing Year. 2008; 12(5):44-52.

[6] Bader G, Anjomshoaa A, Tjoa AM. Privacy Aspects of Mashup Architecture Proc. of Int l Conf ACM Publication Year. 2010; (s):1141-1146.

[7] Jonas Magazinius, Andrei Sabelfeld Chalmers, Aslan Askarov Cornell University: A Lattice-based Approach to Mashup Security. Proc of Int' l conf ACM. 2010, 15-23.

[8] Kotrappa Sirbi, Prakash Jayanth Kulkarni. Stronger Enforcement of Security Using AOP & Spring AOP Int. J of computing. 2010; 2(6):99-105. ISSN 2151-9617

[9] Website Rohit Sethi. Aspect-Oriented Programming and Security "Available at: http://www.symantec.com/connect/articles/aspect-oriented-programming-and-security Pub. 2007, 2010.

[10] Nicolaikuntze, Thomas Rauch, Andreas U. Schmidt: Security for Distributed web-application via Aspect Oriented programming. Proc of Int' conf, 2005.