Secure Access Design Pattern for Cloud Based IR Systems

Ayesha Javed, Nausheen Javaid
Lahore Garrison University, Lahore, Pakistan

***Abstract* - Cloud computing is an approach where virtualized resources become a source for providing services to user at internet. Despite positive aspect of this computing, it exhibits some security challenges that result in data leakage. Due to increase in technology, there is a rapid growth of network digital information on the internet. Characteristic of cloud computing is to retrieve the information and discover the knowledge from centralized database. Sensitive information is being places on the cloud database. To provide data security and privacy is a challenging task. Some design patterns are also proposed for the security purposes. In this paper we first time propose some secure design patterns and solve the problem of cloud base Information Retrieval system.**

Keyword: Cloud computing, secure design pattern Security challenges, Information retrieval, Design pattern.

1. INTRODUCTION

Cloud computing is one of the most alluring technology in today’s world due to cost efficiency and flexibility [1]. Cloud computing is centralized remote service which is used to preserve data and all software application. Sensitive information is being placed in cloud database. To preserve the data is challenging task [2].Few years ago, everyone was using desktop computer and preserve the data on their personal computer that was not accessed by other. However through cloud computing technology no one need to save data on their personal computer there is a centralized database exist in cloud computing. Through web browsers user can easily access the application and without installation. With increase in technology on internet cloud computing gain a lot of attention and is recently most research topic.[3]. There’s variety of definition related to cloud computing [4]. Still there is a lot of changing in the definition of cloud computing but the latest one is “These resources can be dynamically reconfigured to adjust to a variable load, allowing also for an optimum resource utilization” [5]. In the center of cloud platform the accessive data benefits cloud provider as well as the consumer and is recovering or regaining or else seeking information among business, medical information and cooperative information retrieval platform. Information retrieval and knowledge extraction in the cloud platform become important issue [6]. Many major issues exist in cloud computing information retrieval system, which need a lot of attention. Many research papers mention many problem and key challenges in cloud computing IR system. Another major issue in cloud computing is security that how to secure data in cloud that the person who is retrieving the information is authenticate and no unauthorized person get access to the database to secure the cloud computing data many techniques has been introduced. One of the solutions to secure the data is to develop a design pattern, which are reusable solution. This work analyze and personal many problems in cloud computing IR system.

2. RELATED WORK DONE ON SECURITY DESIGN PATTERN

Year	Author	Patterns	Details
1997	Joseph and Jeffrey [7]	Architectural Patterns for Enabling Application Security	Seven security patterns are given to make the system secure
1998	Rubira et all [8]	A pattern language for cryptographic software	Group of nine patterns are given related to the cryptography
1999	DiVietri et all [9]	The Authenticator Pattern	Perform authentication before providing access
2001	Eduardo et all [10]	A pattern language for security models	3 design patterns are discussed in this paper which is used for file authorization purpose
2002	Darrell et all [11]	Security Patterns for Web Application Development	This paper define 29 group of design patterns which are classify as structural and procedural patterns
2004	Shabalin et all [12]	Tools for Secure Systems Development with UML	Define the design pattern to transfer the data securely
2004	Heath et all [13]	Security Design Patterns	This define architectural and design level that is focus on availability and protection of resources
2004	B. Fernandez et all [14]	A pattern system for access control	This paper explain the authorization pattern
2005	M Hafiz [15]	A Pattern for Performance and Security	This paper define the security an privacy of those process which are in source pool and attacker can easily attack those process
2006	Morrison et all [16]	The Credential Pattern	Define the authentication and authorization of information which is in distributed system
2006	Lorrie Faith Cranor [17]	Privacy Patterns for Online Interactions	Three privacy and security patterns are define in this paper, which deal with online transactions
2007	J.C. Pelae et all [18]	Security pattern for voice over ip network.	Guarantee the integrity of calls.
2009	B. Fernandez et all [19]	A pattern system for access Control	This define the role of user to the information

Table 1: Related Works on Security Patterns

3. KEY CHALLENGES

Many major issues exist in cloud computing information retrieval system, which needs a lot of attention. Many research papers mention in many problem and key challenges in cloud computing IR system.

3.1 *Data Integrity And User privacy*

Cloud computing data center hold a large amount of data, which raise the issues, related to protection of user privacy and data integrity.

3.2 *System Elasticity*

Resource pooling needs more security and privacy. If the resource are in resource pool and stay there for long time, than malicious attackers can used that process and can utilize other process for the wrong purpose.

3.3 *Privacy from untrust worthy host*

A client data must be save on the trusted host to prevent the data from malicious host. If data reach an unintended destination, they self-destroy by apoptosis or evaporation to prevent falling into wrong hands.

3.4 *Efficient Authentication Demand*

Due to increase in technology, it allows the large number of clients on the client side to use the cloud application instead of purchasing a license. So the user should be authenticated so that no untrustworthy clients use cloud applications.

3.5 *Mash-up authorization*.

There allot of services who are performing mash-ups of data which increased the security problem related to data leaks and in terms of the number of sources of data a user may have to pull data from. Facebook is one of the example of mash-up of data, user upload both private and public data. Facebook use this data to present to other user, and this information was use by the third party applications that are run by platform. Hence, many malicious applications can steal this information.

4. PROPOSED SOLUTION

We aim to provide secure design patterns to resolve the problems of authentication, privacy, integrity and availability of data retrieval that exist in cloud computing information Retrieval system

4.1 *Data Integrity And User privacy*

This design pattern check the data integrity and user privacy. When user send the request to the information *user privacy patterns* check the user privacy who is accessing the data and if the user is authenticated then check the data integrity that weather that user who is demanding for the information has the right to get that information. If the user have rite to access the information the information will be provided to the user.

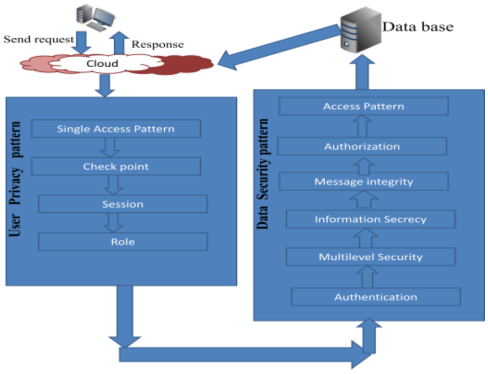

Figure 1: User Privacy And Data Integrity Pattern

4.2 *System Elasticity*

When user send the request for any resource then *checker pattern* check the authentication of the user. If the user is authenticated then assign the role and session will be created. After checking the authentication *checker signature pattern* check the user if the user belongs to administrator provide the source and if the user is not in administrator check source pool if the source is free assign that source to the user but if resource is not free then check whether it is read only. In case of read only resource the copy of that resource will be created and assign to the user but in other case keep that user in waiting list to wait for the resource until it get free.

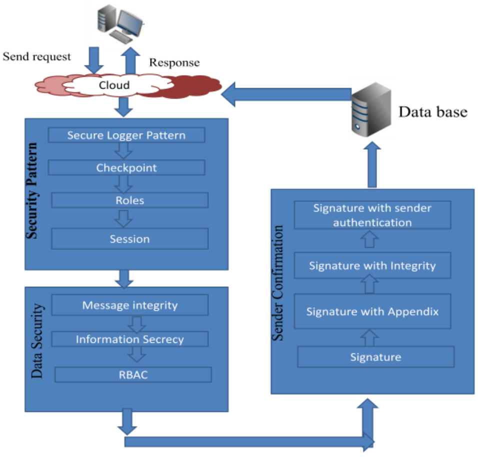

Figure 2: System Elasticity Pattern

4.3 *Privacy from untrust worthy host*

When user send request to save the data *Host Authentication pattern* check that weather the host is authenticated or not. After the host authentication check the *user authentication* and if the user is valid then allow user to save the data in database.

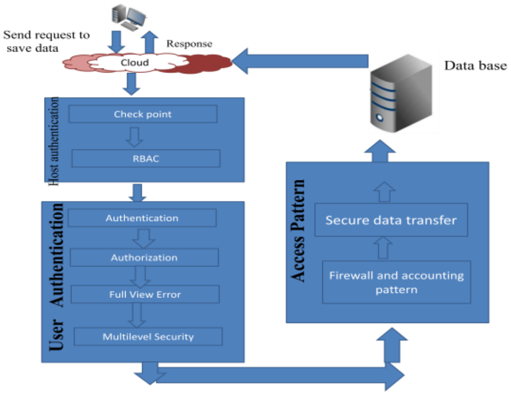

Figure 3: security pattern

4.4 *Efficient Authentication Demand*

To increase the authentication when the user send request for getting the information *secure logger pattern* check the user login and then authenticate the user and provide the information to user.

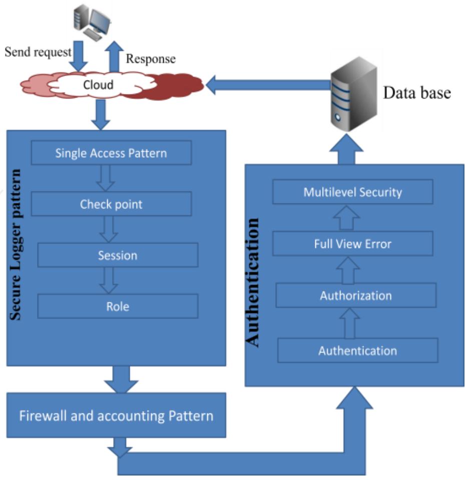

Figure 4: Efficient Authentication pattern

4.5 *Mash-up authorization.*

To increase the authentication when the user send request for getting the information secure logger pattern check the user login and then authenticate the user and provide the information to user.

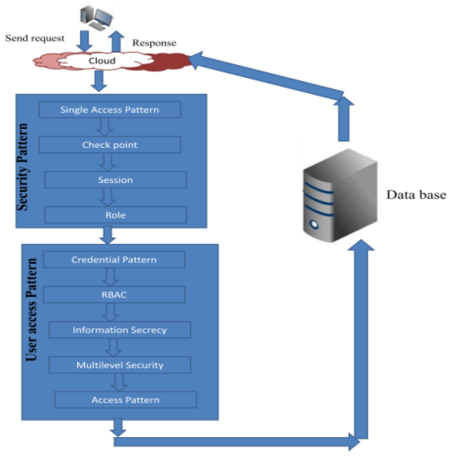

Figure 5: Mash-up Authorization pattern

5. VERIFICATION FOR PROPOSED STRATEGY USING CASE STUDY

WE PROOF OUR WORK BY USING CASE STUDY.

6. TEST CASES

TO FIND THE WAY FOR PRESERVING DATA INTEGRITY AND USER PRIVACY

6.1 *Targeted Problem no 1*

To find the way for preserving data integrity and user privacy

Test Case #: 1 Designed By: Ayesha Javed Executed by : Ayesha Javed	Test Case Name: Preserve data integrity and user privacy. Designed Date: 28/5/2011 Execution Date: 2/6/2011		
Short description: To secure the user privacy and check the data integrity			
Preconditions: User should be authorized			
Step	Action	Expected System Response	Pass / Fail
1	User send request to access his personal data	System check the user authentication	Pass
2	User get the response back	System response back if the user is valid.	Pass

Table 1 data integrity and User privacy

6.2 *Targeted Problem no 2*

To find the way for making system elastic for effective utilization of resources

Test Case #: 2 Designed By: Ayesha Javed Executed by : Ayesha Javed	Test Case Name: system elasticity Designed Date: 28/5/2011 Execution Date: 2/6/2011		
Short description: Resource should be provided on demand.			
Preconditions: user send the request for the process			
Step	Action	Expected System Response	Pass / Fail
1	Process request	If resource is not free and is modifiable then gave the duplicate otherwise place it in waiting list and set the priority.	Pass
2	Request responded	When resource become free then provides the resource to user.	Pass

Table 2 system elasticity Failure scenario

6.3 *Targeted Problem no 3*

To preserve the data from the untrust worthy host

Test Case #: 3 Designed By: Ayesha Javed Executed by : Ayesha Javed	Test Case Name: Preserving data from the untrust worthy host. Designed Date: 28/5/2011 Execution Date: 2/6/2011		
Short description: To check the authentication of host.			
Preconditions: Host should be authorized			
Step	Action	Expected System Response	Pass / Fail
1	User send request to save data	System check the host authentication Then check user authentication	Pass
2	User get the response back	System response back if the host is authenticated and allow user to save the data.	Pass

Table 3 Host authentication.

6.4 *Targeted Problem no 4*

To increase the authentication demand

Test Case #: 4 Designed By: Ayesha Javed Executed by : Ayesha Javed	Test Case Name: Efficient Authentication Designed Date: 28/5/2011 Execution Date: 2/6/2011		
Short description: To increase the authentication demand.			
Preconditions: User should be valid			
Step	Action	Expected System Response	Pass / Fail
1	User send request	Check user status Assign the role	Pass
2	Request responded	Authenticate the user	Pass

Table 4 user authentication Failure scenario

6.5 *Targeted Problem no 5*

Mash up authentication.

Test Case #: 5 Designed By: Ayesha Javed Executed by : Ayesha Javed	Test Case Name: Designed Date: 28/5/2011 Execution Date: 2/6/2011		
Short description: To save the data from malicious applications			
Step	Action	Expected System Response	Pass / Fail
1	User send request	When user try to access the information . Just check the login if the user is from the same login provides the information.	Pass
2	Send Response	Allow to save data	Pass

Table 5 Mash up authentication Failure scenario

7. CONCLUSION

Privacy of data and its one of the major issue in cloud computing Information Retrieval system so there must be several ways of authenticated access, privacy, integrity and availability of data retrieval through cloud computing. In this work, we have proposed the secure design patterns for the problems that exist in cloud computing Information retrieval system. These Patterns overcome Information Retrieval problem and remove the security issues related to Information Retrieval system.

REFERENCES:

1. Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, Elaine Shi, Jessica Staddon. “data in the cloud: Outsourcing computation without outsourcing control”, . In Computer Supported Cooperative Work , 2009.
2. Cong Wang ,NingCao ,JinLi ,KuiRen , and Wenjing Lou, “Secure ranked keyword search over encrypted cloud data,”, Department of ECE, Illinois Institute of Technology, Chicago, In Proceeding of International Conference on Distributed Computing Systems, 2010.

3. Armbrust M., Fox A., Griffith R., Joseph A. D., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., Zaharia M, "Above the Clouds: A Berkeley View of Cloud Computing" , is available at http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009 - 28.html
4. Twenty one experts define cloud computing, Virtualization. Electronic Magazine, article available at http://cloudcomputing.syscon.com/node/612375?page=0, August 2008.
5. Vaquero L. M., Rodero-Merino L., Caceres J., Lindner M..: A Break in the Clouds: Towards a Cloud Definition, SIGCOMM Comput. Commun. Rev. 39(1) 2009: 50-55.
6. Yue-Shan Chang, Chao-Tung Yang, Yu-Cheng Luo, "An Ontology based Agent Generation for Information Retrieval on Cloud Environment" , Journal of Universal Computer Science, Vol. 17, No. 8, Pages: 1135-1160. Retrieved October 25, 2011.
7. Joseph Yoder and Jeffrey Barcalow, "Architectural patterns for enabling application security", In International Conference on Pattern Language of Programs, Computer Supported Cooperative Work , 1997.
8. Alexander M.Braga, Cecilia M. F. Rubira, and R. Dahab, " Tropyc: A pattern language for cryptographic software" , Conference on Pattern Language of Programs, 1998.
9. F. Lee Brown, Jr. James DiVietri, Graziella Diaz de Villegas, "The authenticator pattern", Computer Supported Cooperative Work , 1999.
10. Eduardo B. Fernandez and Rouyi Pan, "A pattern language for security models", Dept. of Computer Science and Eng, Florida Atlantic University, Computer Supported Cooperative Work , 2001.
11. Darrell M. Kienzle, Matthew C. Elder, "Final technical report: Security pattern for web application development" , May 2002.
12. BobBlakley and CraigHeath, "Security design pattern" ,tech report g031. OpenGroup, 2004.
13. Spyros T. Halkidis, Alexander Chatzigeorgiou, and George Stephanides, "A quantitative evaluation of security patterns",Department of Applied Informatics, University of Macedonia, International Conference on Information and Communication Security(International Conference on Information and Communication Systems), 2004.
14. C. Steel, R. Nagappan, and R. Lai. Best Practice and Strategy for J2EE, Web Service and Identity Management. Prentice Hall, 2005.
15. Munawar Hafiz, "pre-forking- a pattern for performance and secuirty", Universityof IllinoisatUrbana-Champaign, PLoP, 2005.
16. Sandra Haraldson, Mikael Lind , "Securing the broken pattern", In 11th European Conference on Pattern Language of Programs (EuroPLoP). International Conference on Pattern Language of Programs, 2006.
17. Markus Schumacher, Eduardo Buglioni Fernandez, Duane Hybertson, and Frank Buschmann. "Security Patterns: Integrating Security And System Engineering", John Wiley and Sons Inc, 2006.
18. Lorrie Faith Cranor, Sasha Romanowsky, Jason Hong, Alessandro Acquisti, Batya Friedman, "Privacy pattern for online interaction", In PLop 2006 Conference. International Conference on Pattern Language of Programs, 2006.
19. Eduardo B. Fernandez, Juan C. Pelaez and Maria M. Larrondo-Petrie, "Security pattern for voice over ip network", Florida Atlantic University, Department of Computer Science & Engineering, Journal of software, VOL. 2, NO. 2, AUGUST 2007