IRJSE *Int. Res. J. of Science & Engineering*, 2020; Special Issue A7: 771-778 SJIF Impact Factor 6.68
ISSN: 2322-0015
RESEARCH ARTICLE **OPEN ACCESS**

Two patterns for cloud computing: Secure Virtual Machine Image Repository and Cloud Policy Management Point.

Kalaskar Keshao D[1], Yadav Shipra[2] and Dhumane Pankaj B[3]

[1]Associate Professor, Dr.Ambedkar College, Chandrapur, (MH), India,
[2]Research Scholar, IICC, RTM Nagpur University Nagpur, (MH), India,
[3]Assistant Professor, Sardar Patel College, Chandrapur, (MH), India,
Email: keshao_kalaskar@yahoo.co.in, shiprayadav621@gmail.com, pdhumane@rediffmail.com

Manuscript Details
Available online on http://www.irjse.in
ISSN: 2322-0015

Cite this article as:
Kalaskar Keshao D[1], Yadav Shipra[2] and Dhumane Pankaj B[3]. Two patterns for cloud computing: Secure Virtual Machine Image Repository and Cloud Policy Management Point., *Int. Res. Journal of Science & Engineering*, February 2020 | Special Issue A7 : 771-778.

ABSTRACT

Two cloud security patterns are given: Secure Virtual Machine Image Repository, which controls the execution or creation of fake virtual machine images, and Cloud Policy Management Point, which defines a security administrator's office to control links to cloud assets.

Categories and Subject Descriptors: D.2.11 [Software Engineering]: Software Architecture—Languages, Patterns; H.1.2 [Management ofComputing and Information Systems]: Miscellaneous—Security.

General Terms: Security Reference Architecture

Keywords: Cloud Computing, Reference Architecture, Security patterns, Misuse patterns.

INTRODUCTION

There are many dangers to [1]. Some are ancient risks that relate to any distributed system that uses the Internet, but a nice amount are fresh people. There are, however, few security patterns to regulate fresh hazards. For this intent, two models are provided here:

- **Secure Virtual Machine Image Repository**: Maintain a strategic separation from harming VM images while creating and releasing touchy information that is incidentally remaining in the VMI by applying archive access control.

- **Cloud Policy Management Point**: Give safety capabilities, including authentication, authorization, cryptography, logging, and monitoring of VM images, a legislative dashboard.
- These models are composite models and are displayed in Figure 1. We use a altered POSA model to define these models[2] Cloud drafters, cloud platform architects and cloud application developers are also our set of viewers. These instances are part of a roster of additional web safety models.

Cloud Reference Architecture (RA) [3], to construct the Security Reference Architecture (SRA). They have importance on their own, of course.

SECURE VIRTUAL MACHINE IMAGEREPOSITORY

Intent: .Avoid the position of VM pictures left inadvertently in the VMI while developing and mixing touch data by enabling access control to the store.

Context: .Cloud computing providers are distributing VMIs in such a way as to allow buyers (clients) to instantiate virtual machines (VMs). In some cloud frameworks, purchasers are alternatively allowed to place VMIs for free use.

Problem: VMIs are important to set up VMs, but an enemy may place malware images in the VMI repository that could infect virtual machines that are created using poisoned images. The answer will be affected by the previous powers:

- **Clean images.** Clean images. Virtual Machine Image (VMI) may involve malware and we need to provide customers with smooth pictures. Virtual Machine (VM) corrupted may misuse client information or abuse other VMs. We need to wash the VMIs before they are used.
- **Data leakage**. Users can keep inadvertently delicate information in the VMI and we need to avoid that leakage.
- **Overhead**. Security controls should not have a significant impact on device efficiency or customers will be hampered in their job.
- **Records.** For safety, accounting, and statistics, the use of a VMI is essential. This behavior should be recorded.

Solution: Provide a system for controlling entry to VMIs to avoid putting or generating toxic pictures by attackers. Scan and filter it before putting a fresh picture or using an current image.

- The Virtual Machine Image Repository includes many Virtual Machine Images (VMI) that can be used to install a virtual machine. Before being distributed or collected, the Reference Monitor utilizes a filter to produce all VM pictures. Authenticator is an Authenticator Pattern activity that enables the Reference Monitor to check clients entering the vault who can distribute or collect pictures if they are authorized by the Authors. The Reference Monitor instance shall implement the authorization privileges set out in the Authorizer. The Security Logger Auditor is going to the store.

Dynamics: Use cases include: publishing a VMI (adding a VMI to the repository), recovering a VMI from the repository, modifying a VMI, and others. Figure 3 demonstrates the "Publish a VMI" use situation. In this use case, a person records in and authenticates himself in the position of Publisher. After being checked by the Reference Monitor, after authentication, he publishes a VMI (stores it in the VMI Repository).

Implementation: We can use various permission schemes to monitor entry to the VMI Repository, e.g. access matrix, RBAC, or multilevel [4]. If we use RBAC to monitor storage, we need to attribute tasks to cloud customers. Only a few functions can add / modify VMIs. Only pictures can be retrieved from other positions.

Some applications, e.g. [5] also monitor the source of pictures and provide main-tenance database facilities. In some instances, an Update Checker recognizes obsolete hardware applications in VMIs [6].

Known uses:

- [5] Proposes secure repository architecture for VMIs depending on threat analysis. Their strategy to addressing attacks is to monitor picture entry

and provide effective image filters and scanners capable of detecting prospective attacks and repairing the associated vulnerabilities.

- [6] Addresses the issue of patching software to maintain it up-to-date, particularly when patching vulnerabilities. In virtual machine pictures, an Update Checker recognizes outdated software components.
- [7] .Indicates the significance of managing image entry and suggests that there is a need for administrative privileges to identify, collect and handle VM image.
- The NIST Security Reference Architecture discusses requirements for VMIs [8].

Consequences: The alternative has the previous benefits:

- **Clean Images**. Scan and filter VMI to inspect and extract malware if available.
- **leaked data.** Check and extract fresh VMI for delicate information that is accidentally-left.
- **Repository Access.** By authenticating customers first and then implementing RBAC or a comparable model, we can regulate entry.
- **Overhead.** It is not a very frequent effort to access pictures, so the cost should be small.
- **Records.** Use the Security Logger / Auditor to record and audit accesses subsequently [9].

Its **liabilities** include:

- **Additional administrator operate**. The administrator now has to maintain track of pictures and how they are handled. It is essential to have a functional GUI.
- **Cost and sophistication**. It is necessary to buy or design the fresh processes and contribute some difficulty to the architecture.
- **Limited access**. We can also allow the publication of VMIs by trusted users.

Related patterns:

- Architecture of Cloud Reference [3]. Can be used to determine where to place safety checks in the database.—Security Logger/Auditor [10].
- Authenticator, Authorizer, and Reference Monitor. They control access to the VMI repository [10].
- Malicious Virtual Machine Creation [11]. This misuse model may not occur if entry to the database of pictures is closely monitored.
- Malicious Virtual Machine Migration Process (misuse pattern) [11]. The content of the transferred VM may have a malicious code and the receiving node may be damaged. This malware may have been introduced by compromising images.
- Cloud Policy Management Point (in this paper). It involves the Secure VMI Repository as portion of the cloud administrator's safety checks.

CLOUDPOLICY MANAGEMENT POINT

Intent provides a safety functional administrative dashboard including authentication, permission, cryptography, logging, and monitoring of VM images.

AKASecurity Dashboard, Security Administration Point.

Context: Cloud computing devices extend to any distributed system, but most of the features exist.

Problem: Security management needs control of who is able to join the scheme, who is able to obtain what funds and associated features. How can we assess whether to allow a customer to join our scheme? How can we identify which funds can be accessed by the customer? How can we safeguard cloud-based information and our customers ' data?

The solution is constrained by the following forces:

- **Expressiveness.** In order to decide on entry, we should be prepared to portray any strategies or restrictions.
- **Security.** Information about access and identification should only be changed by approved individuals.
- **Usability**. Access data should be provided clearly and systematically to the safety administrator.
- **Scalability**. It should be possible to increase conveniently the number of users and the number of roles.
- **Extensibility**. We should be prepared to conveniently incorporate fresh leadership features.
- **Flexibility.** Changing safety policy should be simple

Solution: Defines separately and with appropriate operations each conceptual element of verification, authorization and registration. Provide usage case application data Figure 4.

- **Structure.** In Figure 5, the Cloud Policy Management Point (PMP) manipulates RBAC permission model data including role, resource, and right (RBAC pattern) data. A role involves a User Collection, some of which are Administrative Roles. The Authenticator monitors user authentication information (Authenticator model). The appropriate features are included in a Security Logger / Auditor model. The appropriate cryptographic features (Encryptor and Signer/Verifier) needed by the PMP are included in a cryptographic module.

Dynamics: Figure 6 demonstrates the use scenario: "Create roles and their freedoms." After the security administrator signs in, he will get a token to establish a meeting where he can develop a position and delegate privileges to it.

Implications: All functions of Figure 5 are replicated at PaaS and SaaS levels, with the exception of the VMI repository, to be used by the respective administrators.

Known uses:

- [12] .describes a safety dashboard that uses XACML to monitor the safety of a cloud middleware system.
- Amazon's AWS [13].
- The Oracle Cloud Reference Architecture includes all the functions of this pattern [14].
- Fujitsu's cloud includes a security dashboard with similar functions [15].

Consequences:

- The pattern has the following **advantages**:
- **Expressiveness:** We may constitute any policy or restriction on entry by defining it using functions and liberties. We can use the Access Matrix instead of RBAC to identify the authorizations.
- **Security:** Administrators are unique functions and entry to administrative data is monitored, as is the case for any other customer.
- **Usability:** The classes correspond to logical units of access and other security functions and their use cases define a logical view of security.
- **Scalability:** We can increase the number of users and the number of roles just by creating objects in the respective classes.
- **Extensibility:** New leadership features can be added by incorporating courses or activities to the Figure 5 model.
- **Flexibility**. Changing security policies only involves adding / delete courses or activities in these courses.

Its **liabilities** include:

Complexity: We need a lot of additional courses. The elements of usability are very crucial.

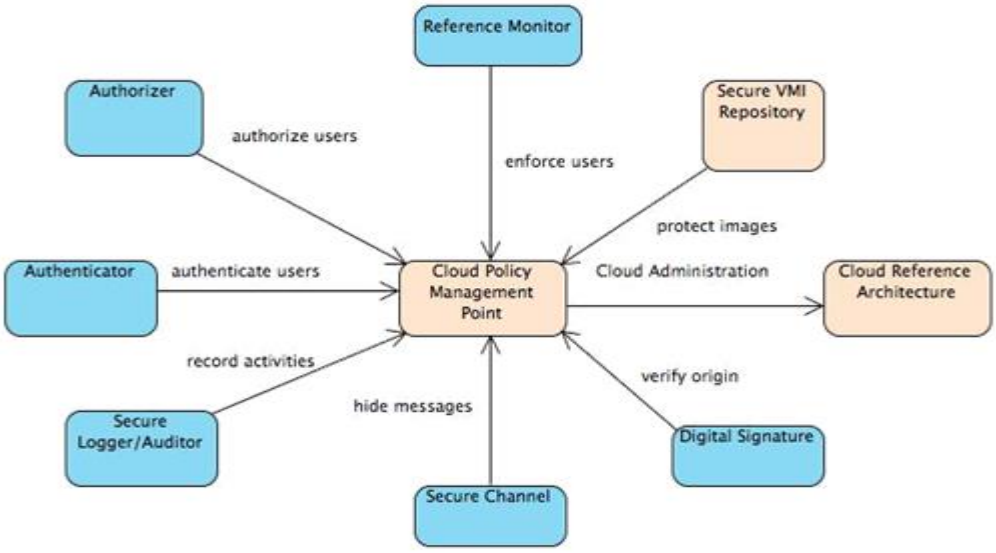

Figure 1: Pattern diagram for the Cloud Policy Management Point and the Secure VMI Repository

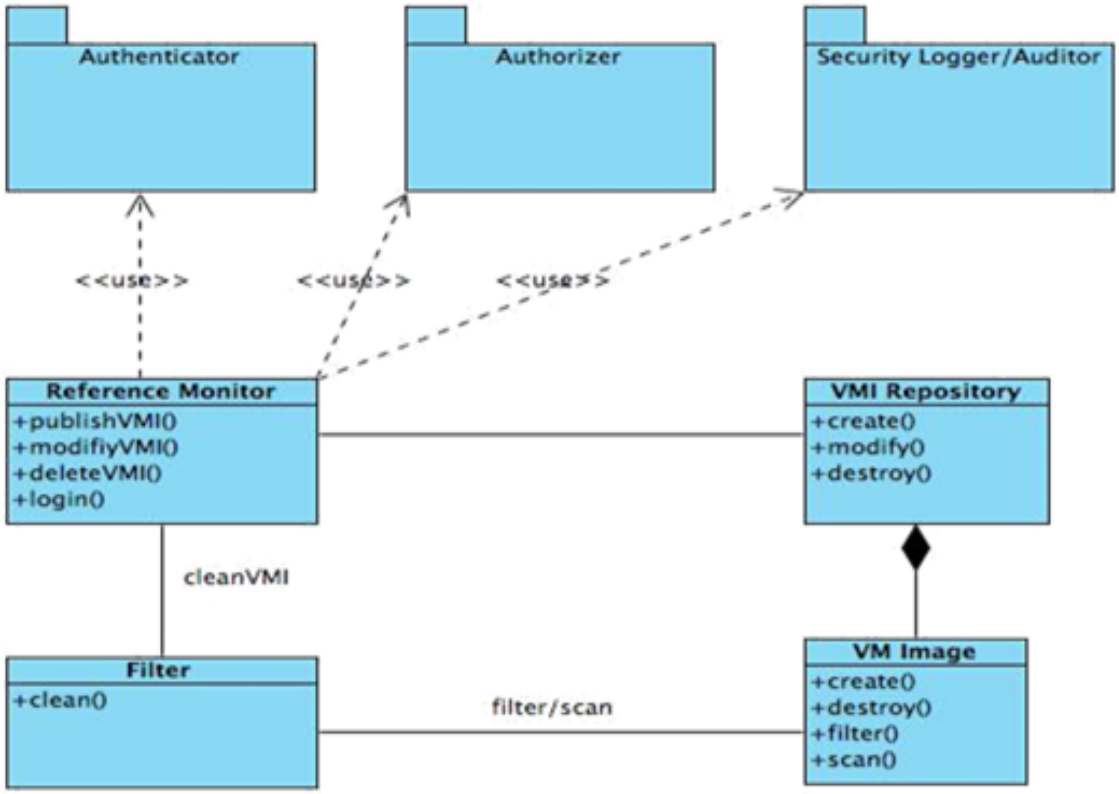

Figure 2: Class diagram of the "Secure VMI Repository

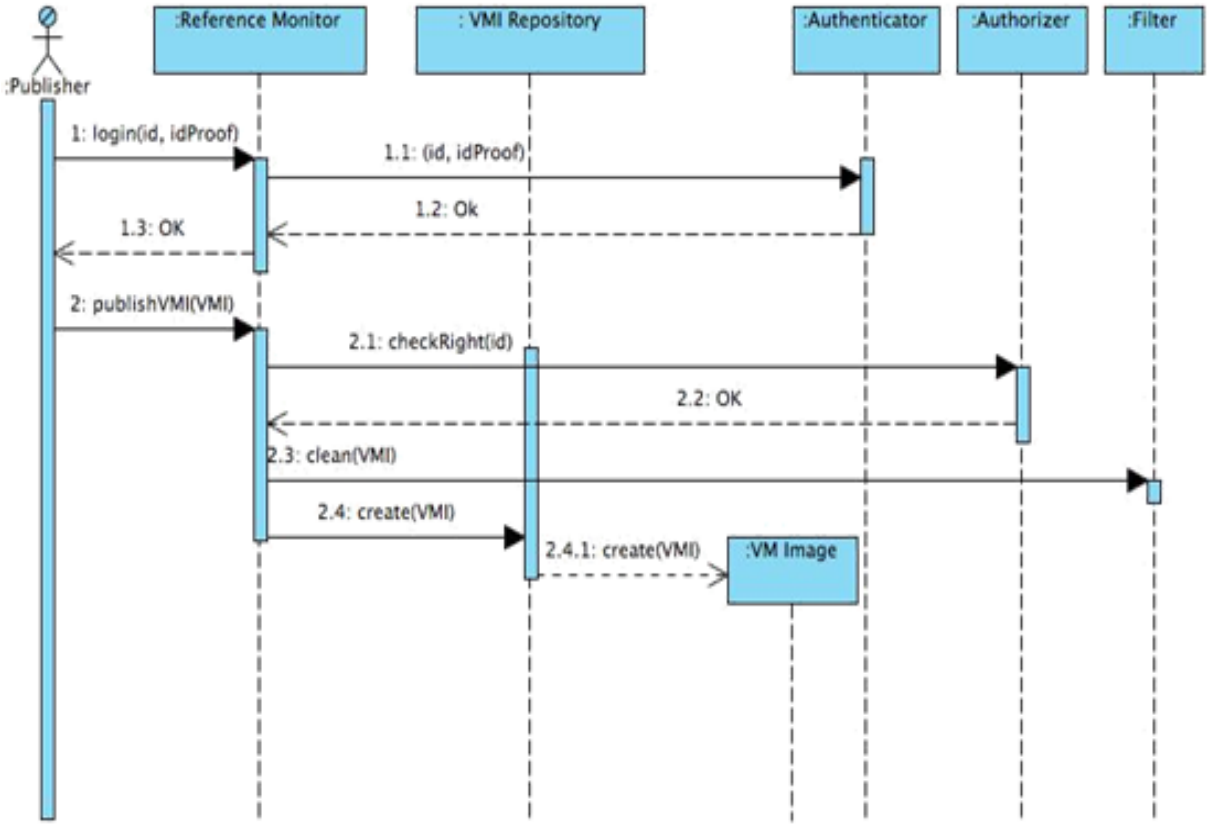

Figure 3: Use case "Publish a VMI"

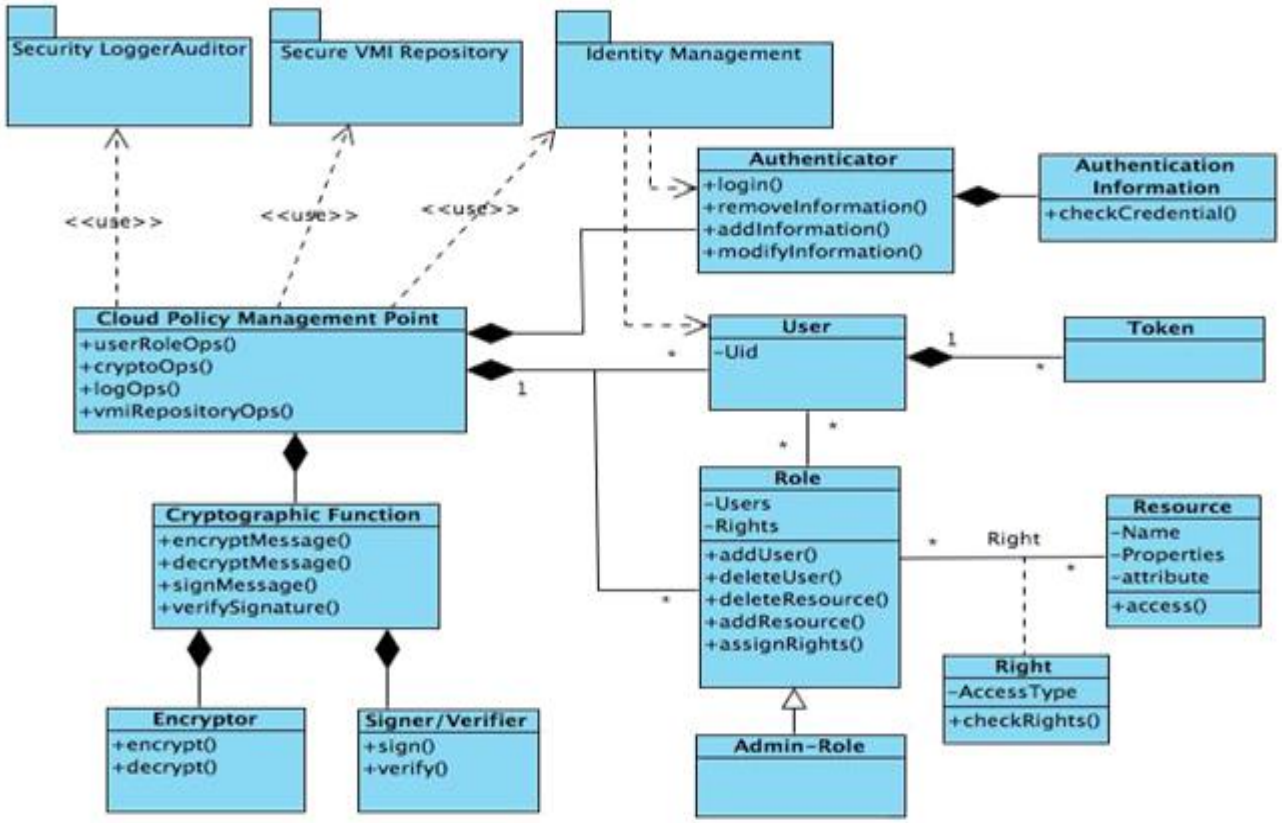

Figure 4: Use cases for the Policy Management Point

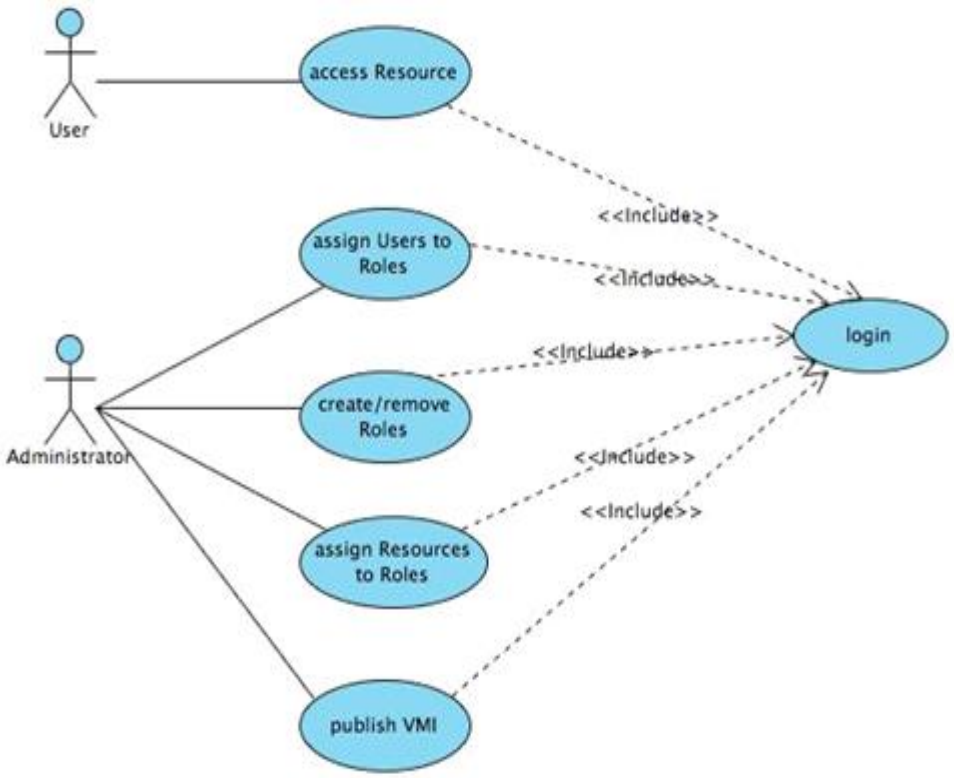

Figure 5: Class diagram for the Policy Management Point

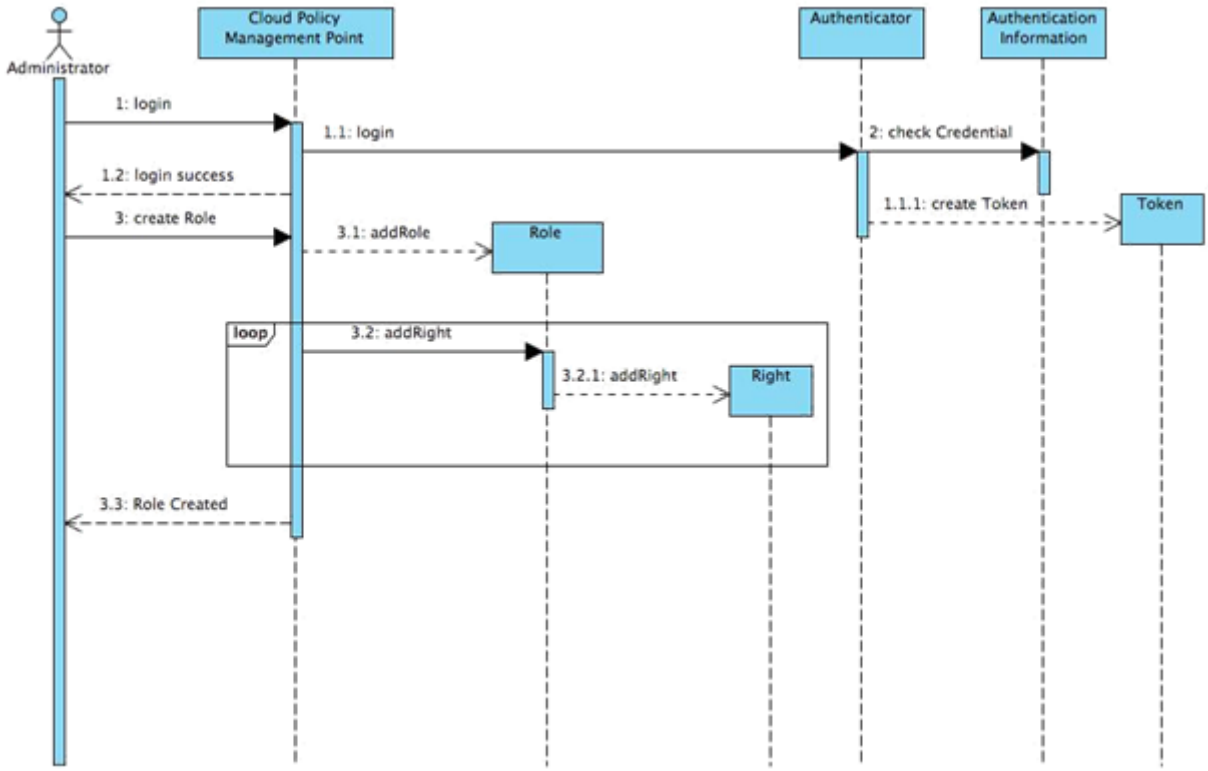

Figure 6: Creating a role and its rights

CONCLUSION

These models are added to cloud pattern database, which will include models for SDN, O Auth, OVF, Secure Migration, and others.

Conflicts of interest: The authors stated that no conflicts of interest.

REFERENCES

1. Keiko Hashizume, David G. Rosado, Eduardo Fernandez-Medina, and Eduardo B. Fernandez 2013a. An Analysis of Security issues for Cloud Computing. Accepted for the Journal of Internet Services and Applications, Springer.
2. F. Buschmann, R. Meunier, H. Rohnert, P. Sommerland, and M. Stal 1996. Pattern-Oriented Software Architecture – Volume 1: A System of Patterns. Volume 1, Wiley, 1996.
3. K. Hashizume, E. B. Fernandez, and M. M. Larrondo-Petrie 2013c. A Reference Architecture for Cloud Computing. Sent for publication.
4. E. B. Fernandez, R. Monge, and K. Hashizume 2013b.A Security Reference Architecture. Submitted for publication. D. GOLLMANN 2006. Computer security (2nd Ed.), Wiley, 2006.
5. J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning 2009. Managing security of virtual machine images in a cloud environment. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW09), Chicago Illinois, USA, ACM 2009, 91–96.
6. R. Schwarzkopf, M. Schmidt, Ch. Strack, S. Martin, and B. Freisleben 2012. Increasing virtual machine security in cloud environments. Journal of Cloud Computing: Advances, Systems and Applications, Springer, 2012, 1–12.
7. Enterprise Management Assocs.(EMA) 2010. Securing the administration of virtualization.Market research report, March 2010.
8. NIST 2013.NIST Cloud Computing Security Reference Architecture. 2013. On-Line: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_01.16.2013-clean. pdf
9. E. B. Fernandez, Nobukazu Yoshioka, Hironori Washizaki, and Michael Vanhilst 1996. An approach to model-based development of secure and reliable systems. In Sixth International Conference on Availability, Reliability and Security (ARES 2011), August 22-26, Vienna, Austria.

10. E. B. Fernandez 2013a. Security patterns in practice – Designing secure architectures using software patterns. Wiley Series on Software Design Patterns, 2013.
11. K. Hashizume, Nobukazu Yoshioka, and E. B. Fernandez 2013b. Three Misuse Patterns for Cloud Computing. In Security Engineering for Cloud Computing: Approaches and Tools, D. G. Rosado, D. Mellado, E. Fernandez-Medina, and M. Piattini (Eds.), IGI Global, 2013, 36–53.
12. W. Joosen, B. Lagaisse, and E. Troyen 2011. Towards application driven security dashboards in future middleware.In Internet Serv. Appl., Nov. 2011, DOI 10.1007/s13174–011–0047–6.
13. Amazon 2013. Amazon Web Services: Overview of security processes. June 2013. On-line: http://aws.amazon.com/security.
14. Oracle Corp. 2013. Cloud Reference Architecture. November 2012.
15. M. Okuhara, T. Shiozaki, and T. Suzuki 2010. Security architectures for cloud computing. Fujitsu Sci. Tech. Journal, vol. 46, No 4, October 2010, 397–402.