i* (iStar) Security Hierarchy for Cloud Computing

Fiza Saher Faizan
National University of Sciences and Technology (NUST), Islamabad, Pakistan
fiza.saher@yahoo.com

Seemab Latif
National University of Sciences and Technology (NUST), Islamabad, Pakistan
seemab.latif@seecs.edu.pk

Rabia Latif
College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia
rlatif@psu.edu.sa

***Abstract*— The world is advancing with the Cloud Computing technology. The aim of Cloud Computing is to provide improved usage of distributed resources like networks, servers, storage applications, and services. With the advancement, there are some risks involved as well. Whenever a cloud-system is being developed, an entity should be there, which looks-after security threats that may arise for the system. This entity is proposed in this research work and named as "Guard". A framework is proposed, which can elicit functional requirements, as well as security requirements of the system. Online-banking case study is used to verify the proposed framework. To accomplish the task, a survey is also conducted and then results are analyzed from survey to propose a framework. The evaluation result of the proposed framework shows that the system will be protected from multiple security risks of cloud computing.**

Keywords- Requirement Engineering; Cloud Computing; iStar.

I. INTRODUCTION

Banking is the term that is used everywhere nowadays. With the huge involvement of banking in the period of technology, the think-tankers of every bank are trying to cope with the technology to beat their competitors. Therefore, moving towards cloud computing is the new era in the field of banking i.e., online-banking, as well as a great challenge for financial institutions because there are many issues that need to be resolved in cloud computing such as security issues [1].

Security is a major concern in the field of cloud computing [2]. Security leads towards the loss of cloud customer's trust on cloud providers as Forrester Research Consultants did survey of 11 merchant companies offering cloud services concluded that most cloud customers or stakeholder's needs do not meet with the result of the cloud service provider, which causes the loss of customer or stakeholder trust [3][4]. Therefore, if good requirement engineering is performed when transforming the traditional system to the cloud system then security issues can be predicted and resolved during development [5][6].

This paper proposes a framework to identify security issues that can be faced by the developers of the cloud system. The rest of this paper is organized as follows. Section II describes the literature review. Section III describes the research methodology. Section IV presents proposed iStar Security hierarchy. Section V presents results and analysis. And finally research is concluded in Section VI with the future work.

II. LITERATURE REVIEW

According to the Cloud Security Alliance (CSA) reports, security is the major concern in cloud computing [8][9][10]. Figure 1 shows the statistics of these reports.

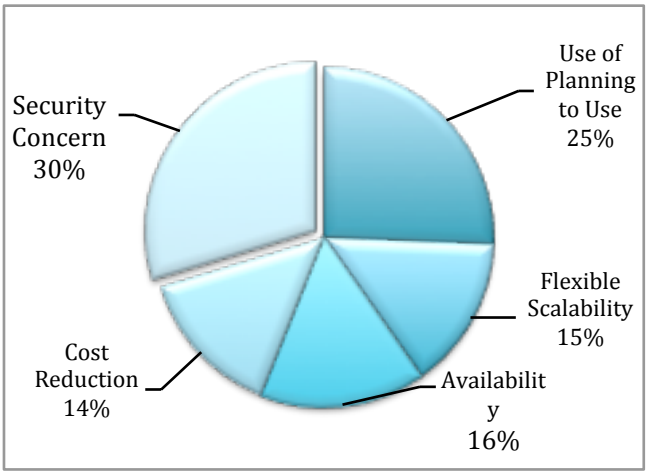

Figure 1: Statistics on Spotlight Reports by CSA

By keeping these reports in view, those techniques are considered in the literature review, which falls in the following four factors:

1) Focused on functional requirements
2) Focused on non-functional requirements
3) Elicits security requirements
4) Inconsistency in technique, which means that technique, persists only for the defined domain.

Therefore, 11 requirements engineering techniques/ methodologies are identified during the literature review and hence they are compared with each other using the above-mentioned factors. This comparative analysis is shown in Table 1.

 ISBN: 978-1-61208-752-8

TABLE I: COMPARATIVE ANALYSIS OF REQUIREMENT ENGINEERING TECHNIQUES FOR CLOUD COMPUTING

Frameworks/Techniques	1	2	3	4
Crowd-Centric RE [11]	✓	×	×	×
UML based Structure [12]	✓	✓	✓	×
Improved RE Framework [6]	✓	×	×	×
Fuzzy Galois Lattice [13]	✓	×	×	×
i* (iStar) [14]	✓	×	×	✓
Security Requirement Engineering and Mechanism [15]	×	✓	✓	✓
Cloud Framework [16]	✓	×	×	×
Security Requirement Elicitation Technique [17]	×	✓	✓	×
Cloud Framework [18]	×	✓	✓	×
Modeling Non-functional Requirements Technique [19]	×	✓	×	✓
RE for Developing Business Process Model Technique [5]	✓	×	×	✓

It is concluded from the literature review that requirement engineering has a very significant role in gathering security requirements for cloud-based systems. For instance, a framework and/or technique is required to elicit security requirements. Traditional requirement engineering techniques are not adequate to elicit the security requirements of cloud-based systems [4]. Hence, this research work is conducted to develop a framework used to elicit the security requirements of cloud-based systems.

III. RESEARCH METHODOLOGY

This research work is based on qualitative research methodology that includes descriptive and case study research methodologies.

To accomplish this research work, a literature review has been conducted to identify all RE techniques and methods used in cloud system development. This literature review is based on the methodology described by Kitchenham [7]. From the literature review, research questions are identified and according to the identified research questions, existing techniques are analyzed to accomplish this research work. After analyzing techniques, an on-ground survey has been performed in which multiple banks are involved to gather the information. The results of the survey are then merged into i* hierarchy and hence the proposed framework is obtained.

The proposed framework has been implemented in a case study. The existing RE techniques and the proposed framework are compared with respect to the factors, which will be discussed in the Section 5. These factors are considered according to domain area of research i.e., requirement elicitation technique to resolve security issues in the cloud-based system, which may arise after the execution of the system.

IV. ISECURITY HIERARCHY

The proposed framework is grounded on two techniques i* Hierarchy and Security Requirement Elicitation and Assessment Mechanism (SecREAM) [14][15]. SecREAM is used to find the security threats, which can weaken the cloud system that is being developed for banking. The results are then merged into i* hierarchy, which shows the elicitation of functional, as well as security requirements for online banking. Figure 2 shows the main i* Security Hierarchy. In i* hierarchy three layers are involved as shown in Figure 2. According to the case study, banks and cloud providers are the main actors of the hierarchy, and a guard is the new actor introduced in this research work and plays a vital role because the purpose of this actor is to locate security requirements with functional requirements at each layer.

On the layer of directors, the goal of Guard is to provide security to online banking. On the manager layer, its goal is to provide security requirements to the bank operational manager and cloud provider manager, as well as an actor working parallel to it at the administration layer. At this layer, the guard finds the assets of the system then finds what security parameters belong to these assets. Afterward, it generates misuse cases against parameters and stores them in the security pool so that the system would be secure. Table 2 gives indicated requirements by these parameters, and these are the result of SecREAM.

TABLE II: PARAMETERS AND SECURITY REQUIREMENTS

Parameters	Security Requirements
Authentication	How do account details access? How do account is protected from unauthorized access?
Authorization	The customer views his account details. What things he has allowed? What if he tries to view other things?
Availability	How much downtime is allowed for the system? When the downtime prolongs then what system should do?
Maintainability	Does a system backup it's data? When the last up-gradation of account details has been done? Which architecture is provided by the service provider?
Configurability	How did an online-banking service provide to the customers either through mobile applications or web services?
Scalability	Does the system allow upgrading to meet technological changes?
Integrity	Does data encrypt? Who will decrypt the data and how? Is digital signature allowed customers to add on their account?

With respect to the case study, the assets of online banking are data storage and data processing and their parameters are authentications, authorization, availability, maintainability, configuration, scalability, and integrity. Forouzan says that these are the security parameters of any system, which may be targeted by an attacker hence security requirements are derived from these parameters [20]. Figure 3 illustrates the working of Guard at the manager's layer. On the administrator layer, its goal is to provide security parameters to the respective actors to be deployed. The working of an actor guard at the administration layer is elaborated in Figure 4. It analyzes what security parameters according to the requirements are deployed on the system and then fetches new security parameters from the pool to be deployed.

 ISBN: 978-1-61208-752-8

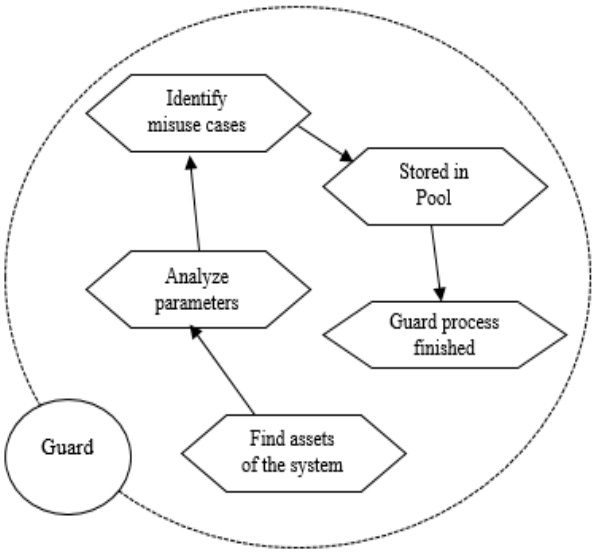

Figure 3: i* Hierarchy "Strategic Rationale of Guard at Manager Layer"

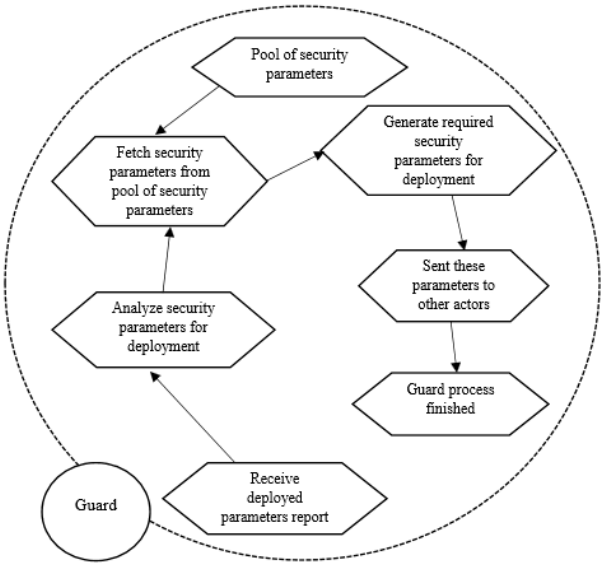

Figure 4: i* Hierarchy "Strategic Rationale of Guard at Administration Layer"

i* hierarchy is goal-oriented and SecREAM is asset-based methodology when combine they can elicit requirements more deeply. SecREAM declares that an asset of the online-banking system is data storage with security parameters mentioned in Table 2. i* evaluate these parameters according to the goal of an actor Guard. For example, at the manager's layer Guard finds that authentication is the most critical security parameter for data storage then it identifies misuse cases for authentication like "How do account details access? and How to do account is protected from unauthorized access?". Similarly, for scalability "Does system allow to upgrade to meet technological changes?". At the layer of administration, the Guard assures that "How the system will behave when a fake person access data with authentic information?" and "What security measures are taken for software viruses when system upgraded?

V. RESULTS AND ANALYSIS

By comparing CSA report discussed in Section 2 and security parameters gathered in Table 2, it can be derived that those security issues can be targeted during the initial stage of system development i.e., requirements elicitation. Table 3 shows security threats that are targeted by security parameters to resolve security issues that might be faced after the execution of the system.

TABLE III: PARAMETERS AND TARGETED SECURITY THREATS

Parameters	Security Threat
Authentication	Verification and Permission issues
Authorization	Usage and Data Protection from Leakage
Availability	Denial of Service
Maintainability	Veracity (Accuracy), privacy and backups
Configurability	Web Browsers, Protocols, Remote connections
Scalability	Technological issues
Integrity	Malicious attacks

Hence, the proposed framework secures the system from data loss, account hijacking, denial of services, inside attacks and shared technology issues.

The comparison has been taken between existing techniques, discussed in the Section 2, and the proposed framework with respect to the following factors that are derived based on the research area.

- **F1.** The technique is a traditional methodology.
- **F2.** The technique is used for cloud-based systems.
- **F3**. The technique is focused on functional requirements for cloud systems.
- **F4.** The technique is focused on non-functional requirements for cloud systems.
- **F5.** The technique is specifically proposed to elicit security requirements for cloud computing.

These factors are recorded as following and then recorded in Table 4:

1) ✓ (Yes), score points = 1, if paper considered the factor.
2) ✗ (No), score points = 0, if paper does not consider the factor.

 ISBN: 978-1-61208-752-8

TABLE IV: COMPARISON OF FRAMEWORKS

Sr.	Techniques	F1	F2	F3	F4	F5	SP
T1	Crowd Centric Requirement Engineering	✓	✓	×	×	×	2
T2	UML based Structure	✓	✓	✓	×	×	3
T3	Improved RE Framework for Cloud	×	✓	✓	×	×	2
T4	Requirement Elicitation Cloud Framework	✓	✓	✓	×	×	3
T5	Software Security RE and Management as an Emerging cloud Service	×	✓	✓	×	✓	3
T6	Proposed Framework	✓	✓	✓	×	✓	**4**

Hence, it is derived that a traditional technique can be modified to elicit requirements for cloud-based systems. The proposed framework focused on functional and non-functional requirements specifically security requirements. In Figure 5, statistics shows that Techniques 1 and 4 satisfy two factors and hence secure 2 score points whereas Techniques 2, 3 and 5 satisfy three factors and hence secure 3 score points. The proposed framework satisfies four factors and hence secure 4 score points, which are the highest score in comparison. The proposed framework also satisfies the factor F4 to some extent because security issues categorized as a non-functional requirement.

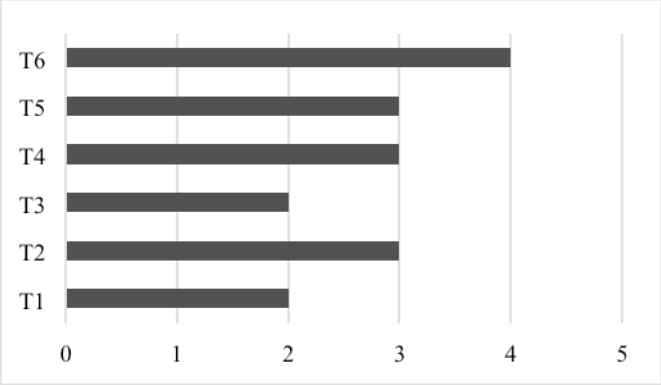

Figure 5: Statistics of Comparison

VI. CONCLUSION AND FUTURE WORK

The proposed framework is based on i* hierarchy and SecREAM and named as "i* Security Hierarchy", which helps to elicit functional requirements with the most demanding requirement i.e., security requirements. An online-banking case study is used to manipulate this work. This framework elicits both functional and non-functional requirements as security is in the non-functional requirements category. The proposed framework concentrates on the requirement elicitation process; hence, it is not involved in all processes of requirement engineering. The proposed framework also proves the flexibility of based techniques.

In the future, the proposed work will be applied to different domains and make it appropriate to involve all processes of requirement engineering, which are (i) requirement analysis, (ii) requirement prioritization and (iii) requirement specification.

REFERENCES

[1] N. Ikram, S. Siddique, and N. F. Khan, "Security Requirement Elicitation Techniques: The Comparison of Misuse Cases and Issue-Based Information Systems", pp. 36-43, IEEE 2014.

[2] A. Alshammari, S. Alhaidari, A. Alharbi, and M. Zohdy, "Security Threats and Challenges in Cloud Computing", International Conference on Cyber Security and Cloud Computing, pp. 46-51, IEEE 2017.

[3] Forrester, TechRadar for infrastructure & operations professionals, Cloud Computing, Forrester, 2009.

[4] H. Schrodl, and S. Wind, "Requirements Engineering for Cloud Computing", Journal of Communication and Computer Vol. 8 pp. 707-715, 2011.

[5] M. Nosrati, "Exact requirements engineering for developing business process models," 2017 3th International Conference on Web Research (ICWR*)*, 2017, pp. 140-147.

[6] M. E. Rana, J. Dauren, and S. Kumaran, "An improved Requirements Engineering framework for cloud based application development," 2015 IEEE Student Conference on Research and Development (SCOReD), 2015, pp. 702-709.

[7] B. A. Kitchenham, "Guidelines for performing Systematic Literature Reviews in Software Engineering", 2007.

[8] H. Schulze, "Cloud Security", Spotlight Report powered by Cloud Passage Information Security Community on LinkedIn, 2015.

[9] H. Schulze, "Cloud Security", Spotlight Report powered by Cloud Passage Information Security Community on LinkedIn, 2016.

[10] H. Schulze, "Cloud Security", Spotlight Report powered by Cloud Passage Information Security Community on LinkedIn, 2017.

[11] R. Snijders, F. Dalpiaz, M. Hosseini, A. M. Shahri, and R. Ali, "Crowd-Centric Requirements Engineering", IEEE/ACM International Conference on Utility and Cloud Computing, 2014, pp. 614-615.

[12] M. Ficco, F. Palmieri, and A. Castiglione, "Modeling Security Requirements for Cloud-based System Development", Special issue Paper, 2014, pp. 2107-2124.

[13] I. T. Koitz, and M. Glinz, "A Fuzzy Galois Lattices Approach to Requirements Elicitation for Cloud Services," in IEEE Transactions on Services Computing, vol. 11, no. 5, pp. 768-781, 1 Sept.-Oct. 2018.

[14] Sandfreni, N. R. Oktadini, and K. Surendra, "Requirement Engineering for Cloud Computing Using i* (iStar) Hierarchy Method", International Journal of Information Science and Applications, 2015, pp. pp 885-890.

[15] R. Goel, M. C. Govil, and G. Singh, "Security Requirements Elicitation and Assessment Mechanism (SecREAM)", IEEE

 ISBN: 978-1-61208-752-8

International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015, pp. 1862-1866.

[16] J. Vijayashree, P. U. Ivy, and J. Jayashree, "Requirement Elicitation Framework for Cloud Applications", International Journal of Engineering Research and General Science, Vol. 3, Issue 1, 2015, pp. 729-733.

[17] M. Ramachandran, "Software Security Requirements Management as an Emerging Cloud Computing Service", International Journal of Information Management, 2016, vol. 36, pp 580-590.

[18] S. A. Aljawarneh, A. Alawneh, and R. Jaradat, "Cloud Security Engineering: Early Stages of SDLC", International Journal of Future Generation Computer Science, 2016, pp. 385-392.

[19] S. Devata, and A. Olmsted, "Modeling Non-Functional Requirements in Cloud Hosted Application Software Engineering", International Conference on Cloud Computing, GRIDs, and Virtualization, 2016, pp. 47-50.

[20] S. Harbajanka, and P. Saxena, "Survey Paper on Trust Management and Security Issues in Cloud Computing", IEEE Symposium on Colossal Data Analysis and Networking (CDAN), 2016, pp. 1-3.

 ISBN: 978-1-61208-752-8

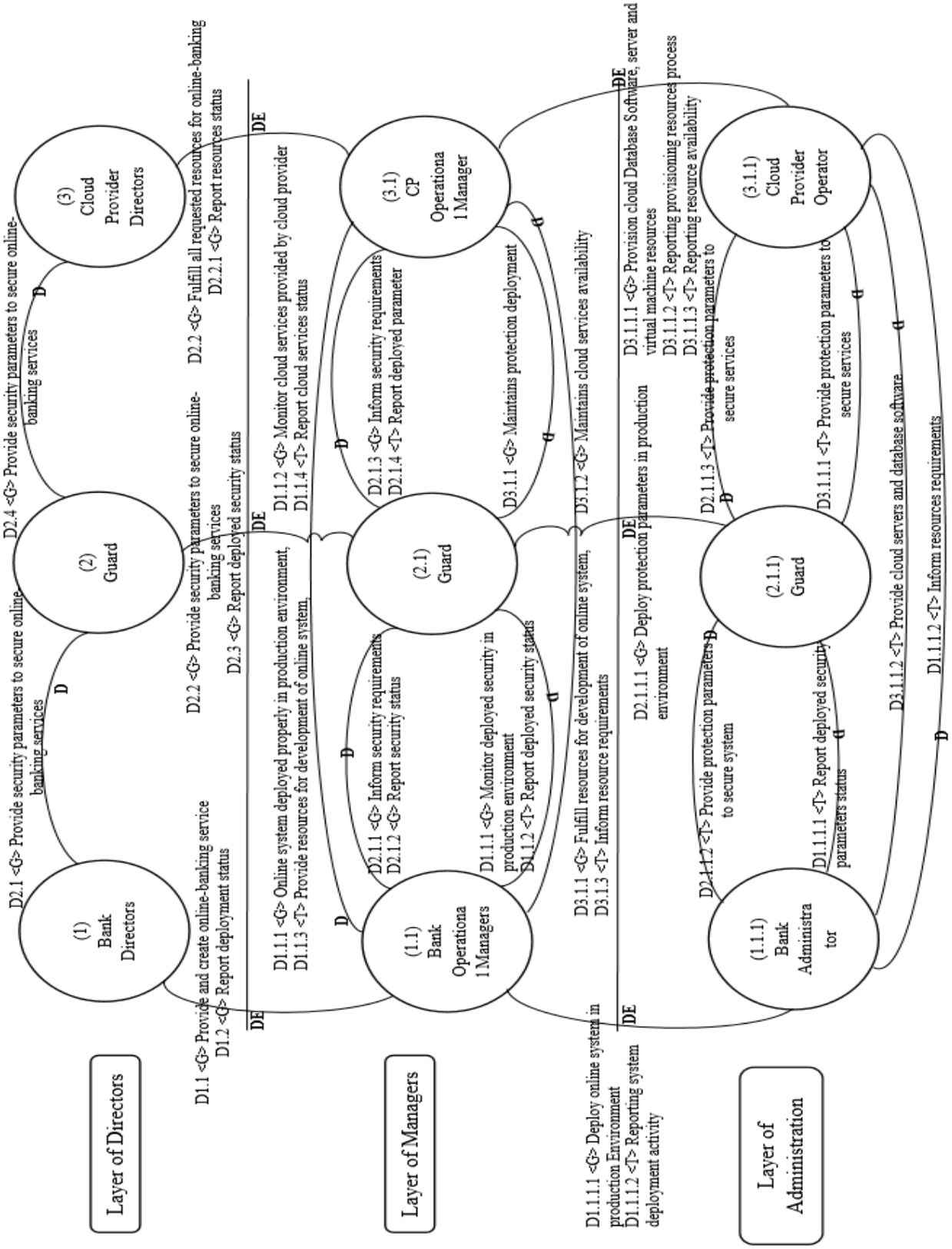

Figure 2: i* Hierarchy “Strategic Dependency of Actors with Guard