
Firman Anindra, Meyliana*, Achmad Nizar Hidayanto, Harjanto Prabowo

1 Computer Science Department, BINUS Graduate Program – Doctor of Computer Science
Bina Nusantara University
Jakarta, Indonesia 11480
firman.anindra@binus.ac.id
1 Department of Informatics and Communication
Universitas Nasional
Jakarta, Indonesia 12520
firmananindra@civitas.unas.ac.id

2 Information Systems Department, School of Information Systems
Bina Nusantara University
Jakarta, Indonesia 11480
meyliana@binus.edu

*Corresponding Author

3 Faculty of Computer Science
Universitas Indonesia
Depok, Indonesia 16424
nizar@cs.ui.ac.id

4 Computer Science Department,
BINUS Graduate Program – Doctor of Computer Science
Bina Nusantara University
Jakarta 11530, Indonesia
harprabowo@binus.edu
Abstract
Currently, cloud computing plays a very important role in the development of Information Technology. Every cloud user continues to expect maximum service, especially in security. The absence of standardizing standards in the security framework of the cloud world, especially in cloud computing community becomes an endless problem. This paper presents a Systematic Literature Review (SLR) which sharpens the critical components of the security framework that exists in the Cloud Computing community that will help users and cloud computing service providers determine their service standards. The framework analysis is extracted by comparing the existing security framework when dealing with its implementation in the cloud computing community. The major security components that can be applied in the cloud security framework are found in this paper. Another finding is that critical security components have been adopted in some security frameworks.

Keywords: Cloud Computing Community, Cloud Security, Security Framework, Security Component, Security Standards.

1. Introduction
Nowadays, the use of cloud computing in the industry continues to increase. Implementation of cloud computing in private, public, hybrid and community becomes a common feature in information technology solutions to evolving business needs [2][7]. Cloud computing communities allow the use of cloud services in combination, which combine services hybrid, public or private simultaneously [7]. The main problem that is still often complained by the Chief Information Officer in the implementation of the cloud is security [7][14]. Another thing is the lack of security standards that can be used by the cloud computing service providers in providing services to users of the cloud [1][9][11][17][23]. The current security standards are only used by each the institutions that make these standards [3][16][20][21]. This paper is intended to search for important security framework components in the cloud computing community. We identify the current security framework by deepening its security components in the cloud computing community. Thus the contribution in this paper demonstrates the critical component of the security framework within the cloud computing community that will help cloud users and cloud service providers have similar requirements in terms of security during implementation.

The structure of writing the paper as follows: section 2 describes the research methodology conducted, accompanied by the sources of paper used and demography. Section 3 presents the results of extraction data from selected papers and further discussion of the findings data in the discussion. Finally, the conclusions are in section 4 and the limitations of the study are in Section 5.

2. Research Methodology
This paper uses the methodology systematic literature review [24][25] to review existing literature related to security framework, the security component of cloud computing, especially in cloud computing community.

2.1 Research Question
At this stage, the identification and planning of the research question are identified. Research questions aimed at writing this paper are: What security components on security framework are the most critical in cloud computing community?

2.2 Defining the Review Protocol
With that research question, we developed a way to search for appropriate topics using keyword was extracted. Keywords used for this literature review are a cloud, cloud computing, cloud computing community, security, security framework and security component.

To present a systematic literature review, research was conducted on:
IEEEExplore Digital Library (http://ieeexplore.ieee.org)
Emerald Insight (www.emeraldinsight.com)
Research is emphasized through a combination of exclusion and inclusion criteria. Only scientific writing in the English language of the journal, conference proceeding on a specified topic, is published from 2010 to 2017. The search period is conducted from October to November 2017. Quality Assessment Checklist (QAC) is made for internal research needs. QAC is a collection of questions according to Kitchenham [24]. Questions are made such as a) Does the selected paper have a clear research methodology? b) Does the research methodology fit the issues discussed? (c) Is the analysis correct? If all the questions answered 'yes' paper can be used.

2.3 Data Extraction and Synthesis

Acquired 99 papers are appropriate based on the keywords used and filtering on QAC, these are included in the Found papers group. After screening the suitability of the topics written in the abstract, 49 papers were identified and grouped in the candidate papers. Deepening of conformity is done again to get results in accordance with the research questions that have been set above. Through this process filter 23 papers and grouped as selected papers as shown in Table 1.

<table>
<thead>
<tr>
<th>Source</th>
<th>Found</th>
<th>Candidate</th>
<th>Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM</td>
<td>14</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>Emerald</td>
<td>10</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>Google Scholar</td>
<td>13</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>IEEE</td>
<td>18</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Springer</td>
<td>25</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>Sciencedirect</td>
<td>19</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>99</td>
<td>49</td>
<td>23</td>
</tr>
</tbody>
</table>

Types of the 23 selected papers consist of 10 journal papers and 13 conference papers as listed in the reference section. As shown in Table 2, it shows paper title, type, and sorting by year of publication.

<table>
<thead>
<tr>
<th>No</th>
<th>Title</th>
<th>Year</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cloud Security...[3]</td>
<td>2017</td>
<td>J</td>
</tr>
<tr>
<td>2</td>
<td>Security and...[5]</td>
<td>2017</td>
<td>J</td>
</tr>
<tr>
<td>3</td>
<td>Big Data...[3]</td>
<td>2016</td>
<td>J</td>
</tr>
<tr>
<td>4</td>
<td>Cloud Migration...[7]</td>
<td>2016</td>
<td>J</td>
</tr>
<tr>
<td>5</td>
<td>A Conceptual...[10]</td>
<td>2016</td>
<td>J</td>
</tr>
<tr>
<td>6</td>
<td>Cloud security...[2]</td>
<td>2015</td>
<td>C</td>
</tr>
<tr>
<td>7</td>
<td>Cloud Computing...[4]</td>
<td>2015</td>
<td>C</td>
</tr>
<tr>
<td>9</td>
<td>Empirical Evaluation...[8]</td>
<td>2014</td>
<td>J</td>
</tr>
<tr>
<td>10</td>
<td>Cloud Computing...[11]</td>
<td>2014</td>
<td>C</td>
</tr>
<tr>
<td>11</td>
<td>An Enhanced...[12]</td>
<td>2014</td>
<td>C</td>
</tr>
<tr>
<td>12</td>
<td>Cloud Security...[13]</td>
<td>2014</td>
<td>C</td>
</tr>
<tr>
<td>15</td>
<td>The Roles...[9]</td>
<td>2013</td>
<td>C</td>
</tr>
</tbody>
</table>
Distribution / demographics of authors and publishing year already represented in the desired time range that is 2010 - 2017, started when the implementation of cloud computing runs at the industry level, no longer in the academic / researcher only. Table 3 illustrates the year of paper publishing and table 4 of the author country.
Table 3
Publication Year

Table 4
Author Country
3. Results and Discussion

Based on the analysis of all selected papers, 14 components are of special concern to the users when implementing the cloud computing community. The list obtained from all selected papers is as follows in Table 5.

Refer to the data in Table 5 below, the five most common security components appear in the selected paper for further analysis. These five components are always the main choice of previous papers, especially on cloud security topics. Therefore we chose it as a critical security component.

3.1 Authentication and Authorization

Authentication and authorization of cloud consumers using pre-defined identification schemes as defined by [1][6]. One of the big issues that become a constraint is account hijacking [2][9][14]. Entity authentication is not too difficult on a centralized system but poses a potential security risk to the shared system [3][9][10][13][15][18][23].

3.2 Confidentiality, Integrity and Availability (CIA)

Refer to [1] is defined as provides security of data objects, modifications of authorization data and ensures availability of data when to be used. In shared computing environments, it may be possible to collect user information that may violate the privacy and integrity of users by other users, even worse perform data retrieval without permission [3][6][13][14][15][19][23]. Data is a valuable asset that must be maintained properly [9][10][21].

3.3 Identity and Access Management

The concept of cloud computing community allows access to resources shared by all users who have the right to access without any interference with each other. Absolute identity and permissions management must be done properly [1][9][14] to avoid the occurrence of service hijacking [2][9]. Mechanisms for identifying and managing user identities, object clouds, organizational accounts and providing access authorization for resources in accordance with their proprietary rights when not done properly into serious security issues [3][16][18][19][21].

3.4 Security Policy and Management

The suitability of legal aspect in the enforcement of regulation and applicable law and audit process to the implementation of the system in cloud become one of important thing in security [1]. Governance issues occur when the cloud user loses its administrative, operational and security controls to systems placed in the cloud [3][7][11][14][23], this is due to the lack of regulation and standards associated with cloud computing [9][18].

3.5 Multi-tenancy

Cloud computing community allows the use of physical and virtual devices together between different users [1][6]. Some of the risks that arise with this condition include the potential attacker doing a co-location attack to take over other customer services [3], the migration process between cloud providers is done on the cloud computing community scheme due to the standard adjustment between different cloud providers [7][14][16][19], disaster recovery scenario handling and business continuity on multi-cloud providers [11]. These are some of the security issues that arise in multi-tenancy.

Table 5

| Security Components from selected papers |  |  |
Refer to R. Bose, X. (Robert) Luo, Y. Liu [9] and M. Gholami, F. Daneshgar, G. Low et al [17] there is no standard security framework that can be used in the cloud computing community. We found 7 security framework approaches from selected papers. Each author makes security framework with a different approach.

We analyze the security components that are of particular concern in Table 5 in the preparation of each stage of the security framework in cloud computing. It is necessary to describe the stages in each of the existing security frameworks, as shown in table 6.

Chang and Ramachandran [4], developed a framework for the name Cloud Computing Adoption Framework (CCAF) with the goal of helping organizations adopt and deliver every cloud service and project success. Naveed and Abbas [6] designed the framework called as Cloud Security Assurance Framework (CSAF) with the purpose of assisting users by providing a methodology to identify their asset security requirements in the early stages of cloud implementation. ISGcloud framework is intended to prove the author's theory can be applied in order to evaluate and validate its utilization [8]. The generic framework that may help users protect the cloud services used and the datacenter becomes the goal of the security framework created by Aljawarneh and Yassein [10]. The certainty of data storage security in the cloud environment became the main focus of security framework design by Chindamani and Punya [12]. The security framework modeling varies according to the purpose of each author as shown in table 6.

Table 6

Security Framework Cloud Computing
The purpose of this research is to deepen the selected paper and to identify critical components in the security framework. The question most often submitted cloud users in terms of security have focused on certain components only. When it is associated with the current cloud computing community security framework, it is found that these five critical components have been adopted by the majority of existing framework in consideration of creating a standard security framework. CSAF is focused on cloud security in certain environments such as private and public clouds, so it does not include explicitly multi-tenancy components [6]. While the security framework proposed by Cindhamani and Punya [12] only sharpen data security in the cloud. The concept of the security service framework proposed by Cho and Lee [19], emphasizes the security and confidentiality of data, so as not to affirm the position of regulation, governance and policy issues in its security framework.

Table 7 shows the adoption of the current security framework against the critical components previously presented. Compared to other security frameworks, design framework security proposals from Xiaowei, et al is the most complete. Scenario trials are also performed on this framework [17]. The Security Service Framework is designed to move key security functions such as authentication and identity management from cloud to user cloud [19].
4. Conclusion
The main purpose of this paper is to find out the important components of the security framework when implementing cloud computing community. We have applied the SLR methodology to identify key components in 23 selected papers from 99 papers found. The focus of the study and analysis lies in the issue of security in the cloud computing community. Five important security components have been generally adopted within the framework of the security of the cloud computing community.

5. Limitation and Future Research
The reference sources used in this paper are limited to journal papers and conference papers only. Of course, it would be better if also equipped with the implementation standards that have been running in a country for further research. The lack of a standard security framework used becomes a challenge in itself and shows great opportunities for researchers to contribute to this area. The solution to critical security issues in the cloud computing community is also an advanced topic of this research.

References

Journals


Conferences


Authors Biography

Firman Anindra is a student of Doctoral Computer Science Program at Bina Nusantara University, Jakarta, Indonesia. His daily activity is working at one of Indonesia state own company as AVP on IT Strategic Planning Department. Currently still involved as a lecturer at Universitas Nasional, Jakarta, Indonesia. His research focus is in IT Governance, Cloud Computing and Applied IT.

Meyliana has been the faculty member of the School of Information Systems – Bina Nusantara University since 1997. Her research interests are information systems/information technology, business process management, enterprise system, customer relationship management, e-business, knowledge management, blockchain, and user experience. She received her Ph.D in Computer Science from Universitas Indonesia. Currently she is the Dean of School of Information Systems Bina Nusantara University.

Achmad Nizar Hidayanto is the Head of Information Systems/Information Technology Stream, the Faculty of Computer Science, Universitas Indonesia.
He received his PhD in Computer Science from the University of Indonesia. His research interests are information systems/information technology, e-learning, information systems security, customer relationship management, knowledge management, change management, e-commerce and IT adoption.

Harjanto Prabowo is a professor of Information System Management and rector of Bina Nusantara University. He earned his Doctoral degree in Business Management with cumlaude from University of Padjadjaran, Bandung; Master degree in Management Information System from Bina Nusantara University and bachelor degree in Electrical Engineering (best graduate) from Diponegoro University, Semarang. His research focus is in the areas strategic knowledge management and innovation, strategic information systems, and information technology.