Gap Analysis of Security in the Cloud

Afnan Alshahrani
Arab East Colleges,
Riyadh, Saudi Arabia

M.A. El-dosuky
Faculty of Computer and Info, Mansoura University,
Egypt,
Arab East Colleges, Riyadh, Saudi Arabia

ABSTRACT
Cloud Computing (CC) is technical term for providing a plethora of Information Technology services to customers via networks. Usually, those services in CC are provided via third parties who own the infrastructures. It offers a practical business model for any organization to utilize Information Technology services without upfront details. However, an organization may not be in a hurry in adopting CC because of security issues. These issues are an active field that need to be handled in a proper way to avoid attacks and threats for both consumers and service providers. This paper scrutinizes CC attacks and threats with their techniques of mitigation and producing complete list of CC security threats. The paper also scrutinizes CC security gap and focuses on types of service delivery.

General Terms
Cloud Computing, Security, Gap Analysis

Keywords
Cloud Computing, Security, Gap Analysis

1. INTRODUCTION
The field of Cloud Computing (CC) is a network-based environment with a paradigm shift in providing and consuming resources, paving a way for resource sharing regardless of location. This is a consequence of the advancement in computation paradigms such as distributed and grid computing [1].

CC is defined by National Institute of Standards and Technology (NIST) as : a model for on-demand network-based access to a shared collection of resources, with the least intervention by service providers [2].

CC is successful due to its performance, ease-of-use by users, and control [3]. However, CC security still complicated and requires to be handled in a proper way to use the provided services more effectively [4].

CC raises many security issues and vulnerabilities, most of them are connected to data security. The major issues are related to confidentiality [5].

The rest of the paper is as follows. Section 2 is for background on CC. Section 3 is for literature review. Section 4 is for proposed system. Section 5 is for results. Conclusion and future work are in Section 6.

2. BACKGROUND
CC enables any organization to have business with no development or maintenance of Information Technology infrastructure. Web browsers access internet-based services. Amazon, Google, and Microsoft, are among major service providers [6].

Clouds can be classified as Private, Public, Community, and Hybrid [7].

There are 3 models of CC: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a Service (SaaS) [8].

In general and as shown in Fig.1, the architecture of CC can be dichotomized into Front-end and Back-end [9].

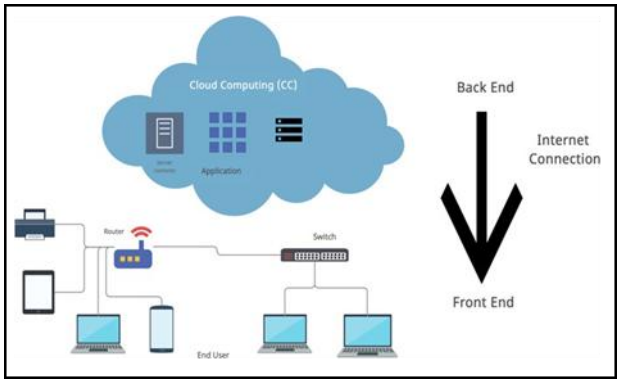

Fig 1: Architecture of CC

In CC, data location is not visible to the users. CC security issues are in one of four layers: user layer, service provider layer, virtualization layer, or physical layer [10].

Top 10 CC security flaws are published by the name "OWASP Top 10". An Organization needs to assess CC flaws and risks to identify use-cases and proper control[11].

3. LITERATURE REVIEW
In 2017, Al-Shqeerat et al. showed that CC has many benefits for higher educational institutions however CC has limitation due to security risks that may act as an obstacle facing the full adoption of CC [12]. They gave recommendation list for avoiding CC security risks.

In the same year, Mushtaq et al. addressed CC security challenges and solution by combining Public-Key Infrastructure (PKI) with Lightweight Directory Access Protocol (LDAP) and Single Sign-On (SSO) [13].

In 2018, Subramanian et al. classified security issues on data in transmission and at rest. A secured system is needed regardless of the underlying Virtual Machines[14]. They recommended using multi-factor authentication to improve hypervisor level security.

In the same year, Basu et al. studied security loopholes and security requirements of a present Cloud system[15]. They scrutinized security issues for gaining an understanding of the CC system and developing appropriate countermeasures.

In 2019, Salehi et al. showed a CC environment for data security [16]. They suggested combining RSA and Digital Signature.

Cloud Security Alliance (CSA) has a security guidance that sheds light on tactical and strategic security in CC, in thirteen domains, which in turn are dichotomized into operations and governance categories as shown in Fig. 2[17].

Fig 2: Adopted Domains of CSA Security Guidance

4. PROPOSED METHODOLOGY

4.1 Requirements

4.1.1 Functional Requirements

1. Service Operation: Infrastructure-as-a-Service makes it easy for the user to access resources such as CPU, and storage. Platform-as-a-Service makes it easy for the user to deploy any application provided by the service provider. Software-as-a Service makes it easy for the user to run applications provided by the service provider on a CC infrastructure.

2. Back-Ups: this enables recovering data recoverability after the failure of the system.

3. Big Data Transfer: Certain CC providers offer big data transfer service.

4.1.2 Non-Functional Requirements

1. Availability: CC services need to be available any time anywhere.

2. Reliability: there are two indicators of reliability: Mean Time To Repair (MTTR) and Mean Time Between Failures (MTBF).

3. Throughput: it is the total work a processer can achieve in a certain time interval.

4. Recoverability: there are two indicators of recoverability from failures: Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

5. Responsiveness: Responsiveness is the time the system takes to reply to inputs.

4.1.3 Management Requirements

1. Fault Management: Diagnosing and correcting faults.

2. Configurability: users can benefit from provided services without interacting with service provider.

3. Reporting: reports provide info on system performance and usage.

4.1.4 Security Requirements:

Many policies are required such as Threat Management, Provider Access Control, End-User Access Control, and Partitioning of Resources.

4.2 Proposed Flowchart

A flowchart is a graphical representation of workflow of step-wise activities. The workflow of proposed methodology is shown in Fig. 3.

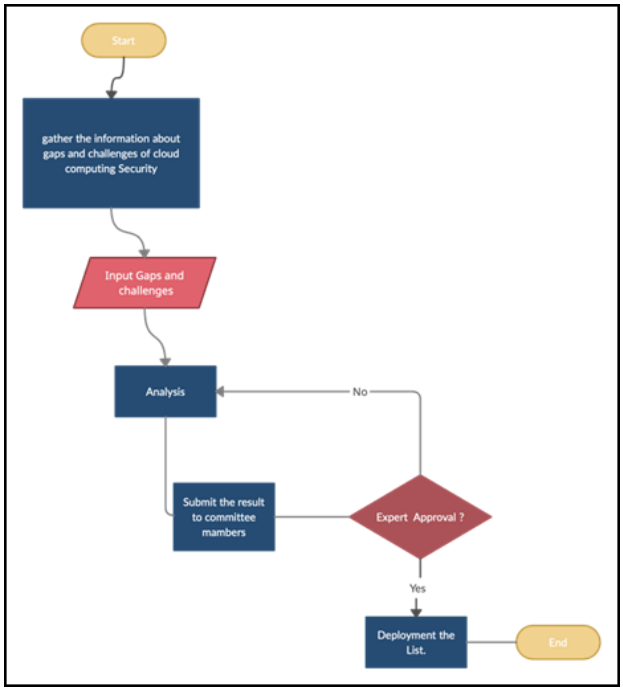

Fig 3: Operational Flowchart

4.3 Methodology

As shown in Fig. 4, research methodology includes three phases for achieving research objectives, which are gathering security gaps in CC, attempting to devise a new list of security gaps in CC and submitting it to committee members to deploy it.

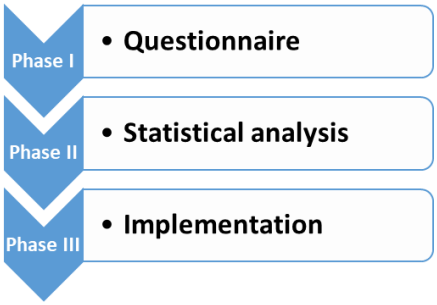

Fig 4: Research Methodology Phases

In phase I, committee members take a questionnaire to gain their responses.

In phase II, the researchers conduct statistical analysis on responses from committee members.

In phase III, simulation tools will implement the proposed CC model. Simulation tools are CloudSim, and Cloud Analyst. The former is a framework for simulating and modeling CC environments that is implemented in Java [18]. The main problem of CloudSim is lacking Graphical User Interface (GUI). Cloud Analyst is a GUI-based improvement of CloudSim.

4.4 Implementation & Testing

Used Tools are Apache NetBeans Building tools, Cloudsim 3.0.3, and Cloud Analyst.

Questionnaire : respondents are postgraduate-level students or working in the field of cybersecurity and are assumed to understand CC governance and security. The questionnaire has 11 operations questions and 14 governance questions.

Study Design : the conducted study is descriptive cross-sectional to enhance our understanding of CC governance and security.

Population: members of the committee.

Study area : postgraduate-level students or working in the field of cybersecurity in the Kingdom of Saudi Arabia.

Sample size : 100 members of the committee, with different job fields (Info Technology, Network Security, Cybersecurity, or Not Technical).

Sampling technique : using 95 % confidence interval & 5 % margin of error, the sample is selected randomly, and numbered 100 members of the committee.

The questionnaire is decomposed of three categories:

1. Socio-demographic data: age & Career field.
2. CC Governance consisting of 14 items
3. CC Operations consisting of 11 items.

Data collection technique : Once all permissions are obtained, questionnaire is sent electronically to member of the committee.

Data entry & analysis : using SPSS version 23. Data is processed to measure descriptive statistics such as frequencies and percentages. Ratio data is presented as mean and standard deviation. ANOVA test is used to compare ratio data between ANOVA test for age and career filed. The significance level was selected to be ($p<0.05$).

Study tool Reliability: questionnaire reliability means to produce the the same result if it is redistributed many times under the same conditions. The authors confirmed questionnaire reliability by using Cronbach's alpha method

It is obvious from Table 1 that Cronbach's alpha coefficient ranges between 87 % and 91 %, and the value of the Cronbach's alpha coefficient for all items of the questionnaire is 94 %. This means that reliability is high, which allows us to use the questionnaire with confidence.

Table 1. Cronbach's Alpha Coefficient

Questionnaire Section	Count of Items	Cronbach's Alpha Coefficient
First Section	**14**	**0.87**
Second Section	**11**	**0.91**
Total	***25***	***0.94***

Cloud Gap-scale (CGS) : Based on a questionnaire, the authors proposed a scale for determining cloud gap severity, as follows:

1. Score of 6 or less →Severe gap
2. Score of 7 through 10→Moderate gap
3. Score of 11 through 13→Mild gap

Implementation: implementation is as a project in NetBeans IDE in Java programming language. Fig. 5 shows structure of the project.

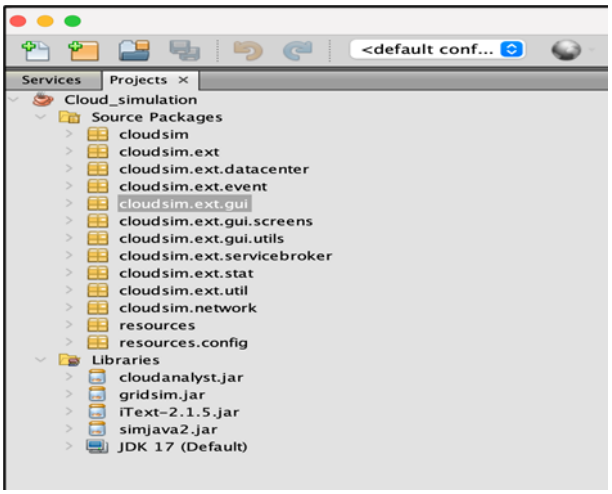

Fig. 5: Structure of the Project

Main GUI is modified. Fig. 6 offers the GUI of Cloud Analyst.

Fig.6 : GUI of Cloud Analyst

Cloud Gap scale (CGS). Fig. 7 presents a sample of scale question.

Fig. 7 a sample of scale question

The result shown after answer all questions of scale. Fig. 8 presents a sample of scale Classification.

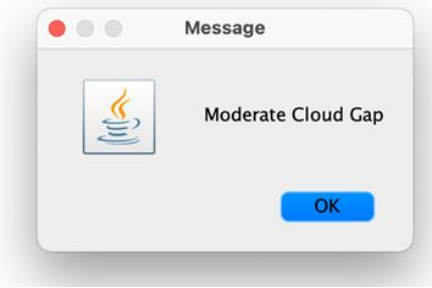

Fig. 8 a sample of scale Classification

CC reliability is measured in terms of Mean Time To Repair (MTTR) and Mean Time Between Failures (MTBF).

Fig. 9 shows MTBF class.

```
class  MeanTimeBetweenFailures {
   public static void main(String[] args) {
       int totalUPtime=24;
   int n=22;
   for(int i=2;i<=n;i+=2){
   float MTPF=(float)totalUPtime/i;
   System.out.println(MTPF);
}

   }
}
```

Fig. 9 MTBF class

Fig. 10 shows MTTR class

```
class  MeanTimeToRepair {
   public static void main(String[] args) {
   int totalDowntime=24;
   int n=22;
   for(int i=12;i<=n;i+=2){
   float MTTR=(float)totalDowntime/i;
   System.out.println(MTTR);
}

   }
}
```

Fig. 10 MTTR class

5. RESULTS

5.1 Demographic Characteristics:

1. Age

Age is analyzed by measuring percentage of each category of age. Table 2 and Fig. 11 declare the distribution.

Table 2: Age distribution

Age	*Percentage*
18 through 25	*3%*
25 through 35	*38%*
35 and Up	*59%*
Total	***100%***

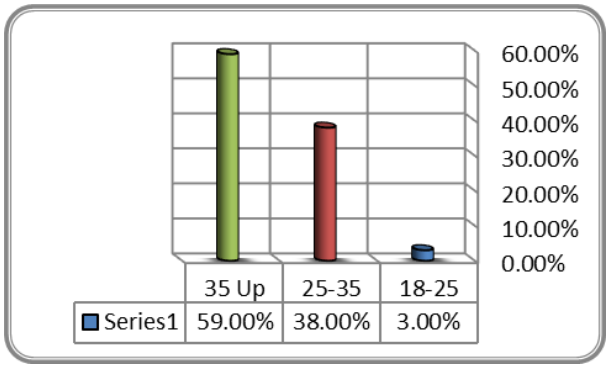

Fig. 11: Age distribution

2. Career field

The Career field is analyzed by measuring percentage of each category of career field. Table 3 and Fig. 12 declare the distribution.

Table 3 Career field distribution

Career field	*Percentage*
Info. Technology	*51%*
Network Security	*16%*
Cybersecurity	*26%*
Non Technical	*7%*
Total	***100%***

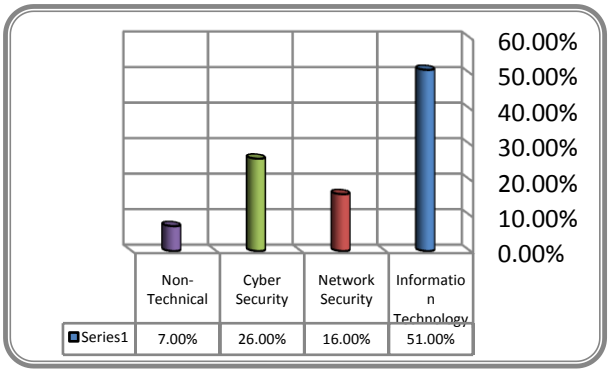

Fig. 12: Career field distribution

5.2 Cloud Gap scale (CGS)

Table 4 shows CGS Scale Classification Scenarios.

Table 4 CGS Scenarios

Scenario ID	*Number of Yes's*	*Number of No's*	*Cloud gap Classification*
Scenario1	4	9	Severe

Scenario2	8	5	Moderate
Scenario3	12	1	Mild

In Scenario1, the number of Yes's are 4/13, Fig. 13 presents the severe response.

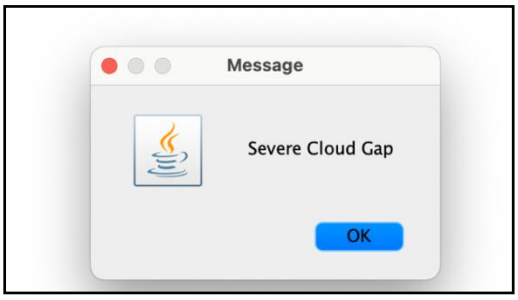

Fig 13: Severe response

In Scenario2, the number of Yes's are 8/13, Fig 14 presents the Moderate response.

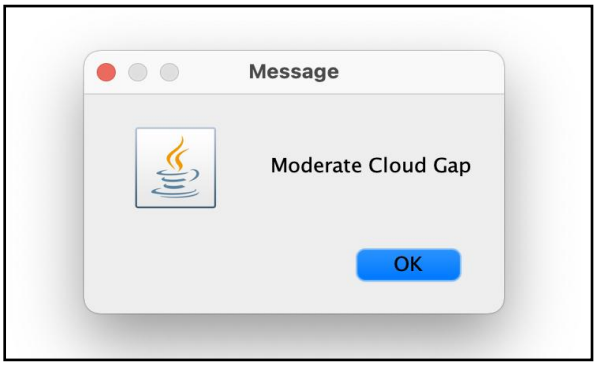

Fig 14: moderate response

In Scenario3, the number of Yes's are 12/13, Fig 15 presents the Mild response.

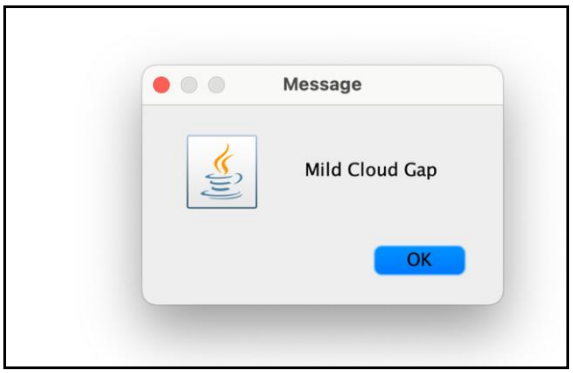

Fig 15: mild response

5.3 Reliability

Fig. 16 shows inverse relation between MTTR and number of failures.

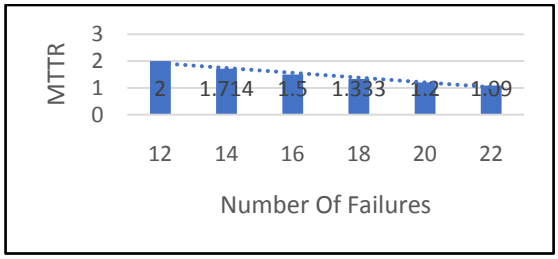

Fig 16: MTTR at Total Downtime 24

Fig. 17 shows inverse relation between MTBF and number of failures.

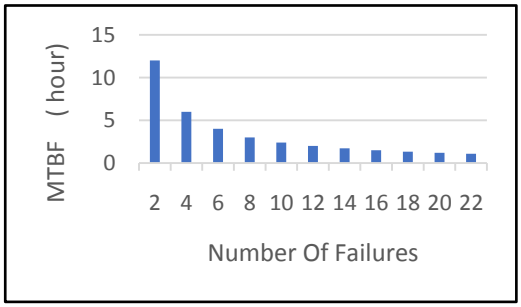

Fig17:MTBF at total uptime 24

Fig. 18 shows relation between failure rate (per hour) and number of failures.

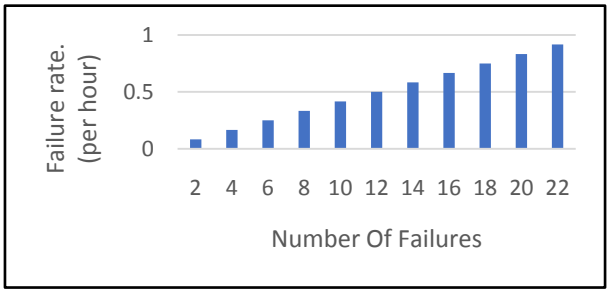

Fig 18: Failure rate

6. CONCLUSION & FUTURE WORK

Due to complexity and dynamicity of CC, it requires special care in handling security as compared to traditional computing. A huge body of research has been done on CC security for resolving its issues.

Cloud Security Alliance (CSA) has a security guidance that sheds light on tactical and strategic security in CC, in thirteen domains, which in turn are dichotomized into operations and governance categories.

Based on a questionnaire, the authors proposed a scale for determining cloud gap severity. Reliability was measured in terms of MTTR and MTBF.

The paper in hand scrutinizes and categorizes CC security threats into Cloud Gap-scale (CGS).

A possible future direction regarding CGS may be disseminating it with the aim of being adopted. Another future direction may improve the simulation. Finally, the authors may suggest a set of guidelines and policies to match the three cases of the security gap.

7. REFERENCES

[1] Alam, T. (2021). Cloud Computing and its role in the

Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1, 108-115.

[2] Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., ... & Sarkar, P. (2018, January). Cloud computing security challenges & solutions-A survey. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 347-356). IEEE.

[3] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42.

[4] Amara, N., Zhiqui, H., & Ali, A. (2017, October). Cloud computing security threats and attacks with their mitigation techniques. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 244-251). IEEE.

[5] Shaikh, A. H., & Meshram, B. B. (2021). Security issues in cloud computing. In Intelligent Computing and Networking (pp. 63-77). Springer, Singapore.

[6] Ahmed, I. (2019). A brief review: security issues in cloud computing and their solutions. Telkomnika, 17(6).

[7] Tadapaneni, N. R. (2017). Different Types of Cloud Service Models. Available at SSRN.

[8] Jaiswal, M. (2017). Cloud computing and Infrastructure. International Journal of Research and Analytical Reviews (IJRAR), E-ISSN, 2348-1269.

[9] Deepa.B, Srigayathri.S, & Visalakshi.S (2018). A Review on Cloud Computing. International Journal of Trend in Research and Development

[10] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42.

[11] Choudhary, A. (2021, February 23). OWASP Cloud Top 10 - FAUN Publication. Medium. https://faun.pub/owasp-cloud-top-10-db4a3a8e0a8f .

[12] Al-Shqeerat, H. A. K., Al-Shrouf, F. M., Hassan, M. R., & Fajraoui, H. (2017). Cloud computing security challenges in higher educational institutions-A survey. International Journal of Computer Applications, 161(6), 22-29.

[13] Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud computing environment and security challenges: A review. International Journal of Advanced Computer Science and Applications, 8(10), 183-195.

[14] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42.

[15] Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., ... & Sarkar, P. (2018, January). Cloud computing security challenges & solutions-A survey. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 347-356). IEEE

[16] Salehi, A. W., Noori, F., & Saboori, R. (2019). Cloud Computing Security Challenges and its Potential Solution. American Journal of Engineering Research, 8(10), 165-175

[17] Mogull, R., Arlen, J., Gilbert, F., Lane, A., Mortman, D., Peterson, G., & Rothman, M. (2021). SECURITY GUIDANCE for critical areas of focus in cloud computing, v4. 0. Tokyo, Japan: Cloud Security Alliance.

[18] Silva Filho, M. C., Oliveira, R. L., Monteiro, C. C., Inácio, P. R., & Freire, M. M. (2017, May). CloudSim Plus: A cloud computing simulation framework pursuing software engineering principles for improved modularity, extensibility, and correctness. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (pp. 400-406). IEEE.