Analysis of Threats and Attacks on Privacy and Security of Cloud Computing

Ruchi Dubey
Samrat Ashok Technological and Institute
Vidisha (M.P)

Nirmal Gaud
Samrat Ashok Technological and Institute
Vidisha (M.P)

ABSTRACT
Many IT professionals would have the same opinion that cloud computing is the most innovatory information delivery model since the beginning of the Internet. For corporate management and decision makers, cloud computing brings many financial and functional benefits as well as serious security concerns that may threaten business stability and corporate status. But this technology is still uncertain to many security troubles. The definition of cloud computing is still fuzzy in a large part, because of the magnitude of the security risks and the virtually unlimited amount of information being published. With many business ventures, as the use of cloud environments grow day-by-day and for this the risk and the threats associated with a successful use of the model also increase. In this paper we analysis of various threats and attacks on privacy and security of cloud computing.

Keywords
Cloud Computing, Threat Category, Security, Risk Assessment

1. INTRODUCTION
Cloud computing is a new subject at both technological and commercial level, therefore various definitions can be found, focusing on different characteristics of cloud Computing technology, services, and platform [1]. IBM takes a technical instance and defines cloud computing as follows: A cloud is a pool of virtualized resources that hosts a variety of workloads, allows for a quick scale-out and deployment, provision of virtual machines to physical machines, supports redundancy and self-recovery and could also be monitored and rebalanced in real time [2].

The definition of cloud computing delivered by NIST has gained substantialpower within the IT industry. According to this definition: "Cloud computing is a model for enabling suitable, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[3,4]. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. The National Institute of Standards and Technology (NIST) has been designated by the Federal Chief Information Officer (CIO) to accelerate the federal government's secure adoption of cloud computing by leading efforts to identify existing standards and guidelines[5]. Where standards are needed,NIST works closely with U.S. industry, standards developers, other government agencies, and leaders in the global standards community to develop standard. Another way of defining the cloud computing so is to examine its cloud model, which contain five essential characteristics, three service models and deployment models that each cloud model having its own features. In Table 1.1 there is a brief description of about cloud models [6].

Table 1.1: Cloud Models

Five Essential Characteristics	1. On demand self-service 2. Broad network access 3. Resource pooling 4. Rapid elasticity 5. Measured Services
Three Service Models	1. Software as Service (SaaS). 2. Platform as service (Paas). 3. Infrastructure as service (Iaas).
Deployment Models	1. Public Cloud 2. Private Cloud 3. Hybrid Cloud

2. CLASSIFYING CLOUD THREAT CATEGORIES
In this Cloud Threat Categories, we describe how the various threats can be bunched together in six categories [7,8]. In this most of the threats have a domino effect on the other components, where one affects multiple components.

Table: 1.2 Security threats and their categories(C confidentiality, I integrity, A availability)

Threat Category	Factor	Example
External attacks	C,I,A	Carrying out of denial of service (DoS) attack.
Theft	C,I,A	Gaining unauthorized access to system or networks.
System malfunction	A,I	Malfunction of software
Service interruption	C,I,A	Natural Disaster
Human error	C	User error
System specific	C,I,A	Usage control

3. ALGORITHMS FOR SECURITY RISK ASSESSMENT
The algorithms used to measure security risks can be unique depending on the deployment and operation phases [9,10]. These are described below:

Table 1.3: Threat classification with their values [11]

Threat I'd	Threat Classification(A,C,I)	Priority(P)	Likelihood (L)
T1	Carrying out of DoS attacks (T1)	4	3
T2	Hacking(T2)	3	1
T3	Undertaking malicious probes or scans(T3)	4	2
T4	Cracking password (T4)	3	1
T5	Cracking Key (T5)	3	1
T8	Spoofing user identities(T8)	3	1
T9	Modifying network traffic(T9)	2	2
T10	Eavesdropping(T10)	2	1
T11	Distributing computer viruses(T11)	3	1
T12	Introducing Trojan horses(T12)	3	1
T13	Introducing malicious code(T13)	3	3
T15	Distributing Spam(T15)	1	4
T16	Gaining unauthorized access to systems or network(T16)	5	4
T27	Theft of business information(T27)	4	2
T29	Theft of computer equipment(T29)	1	2
T34	Malfunction of software(T34)	1	4
T35	Malfunction of computer network equipment(T35)	1	5
T40	Natural Disaster(T40)	1	3
T41	System overload(T41)	4	3
T42	User error(T42)	5	3
T50	Data Leakage(T50)	5	3
T51	Usage control(T51)		
T52	Hypervisor level attacks(T52)	3	2
T53	Data ownership(T53)		2
T54	Data exit rights(T54)	4	3
T55	Isolation of tenant application(T55)	5	2
T56	Data encryption(T56)	5	3
T57	Data segration(T57)	4	2
T58	Tracking and Reporting service effectiveness(T58)	5	3
T59	Compliance with laws and regulation(T59)	3	2
T60	Use of validated products meeting standards(T60)	3	3

4. ALGORITHM: DEPLOYMENT PHASE SECURITY _risk_at_deployment (CLOUD ECOSYSTEM)

Step1.Calculate the number of threats recorded, at deployment stage and the involved ecosystem [12,13].

Step 2.For each threat, calculate:

a. probability of likelihood given the asset is affected (p (B| A)) = likelihood / 5.0

b. probability of asset priority (p (A)) = priority / 5.0

c. probability of likelihood regardless of asset (p (B)) = p (B | A) * p (A) + p (A′)

d. probability of threat occurring (p (A | B)) = ((p(B | A) * p (A))) / p (B)

Step3. Security risk = sum all probabilities of threats occurring/threats found.

Let A = "Something is wrong with asset with its priority"

Let B = Asset has failed as a result.

The maximum value of the asset priority and the likelihood of it being affected are set in the range 1–5. Based on the list of threats that need to be monitored, these can be assessed based on each asset and the likelihood that each asset actually fails as a result of the threat. Bayes rule can be used to calculate the original probability [14,15].

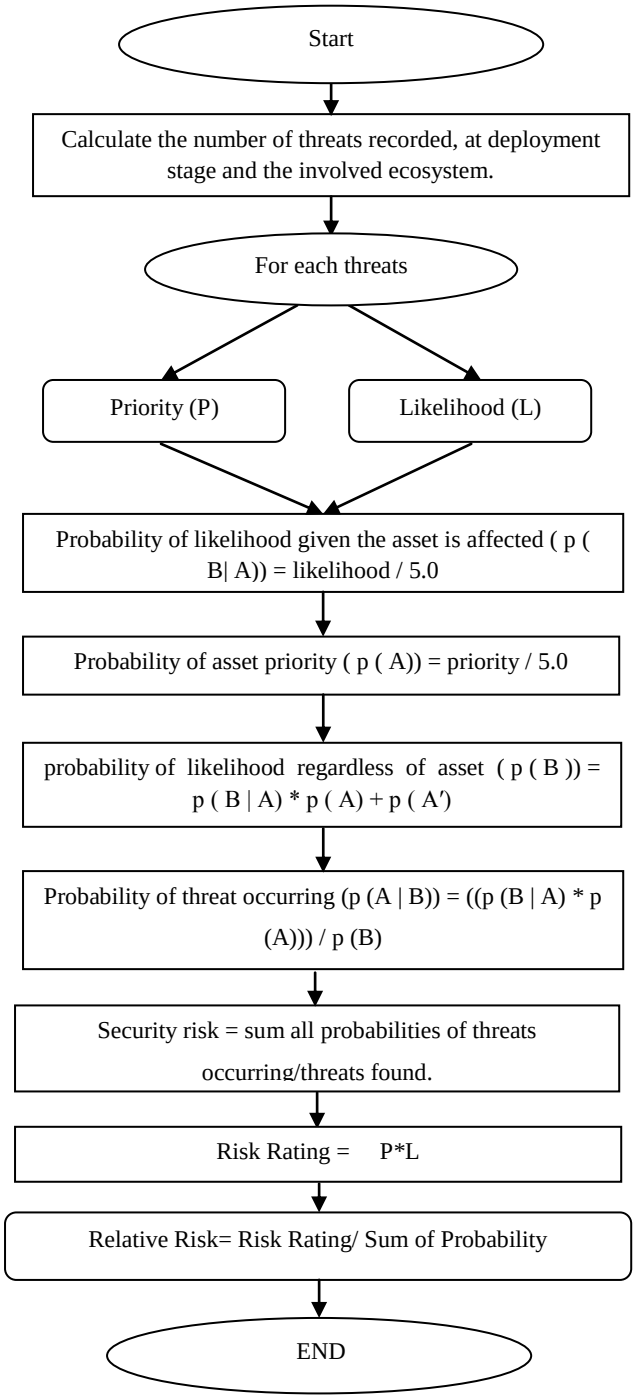
5. SECURITY_RISK_AT_OPERATION (CLOUD_ECOSYSTEM)

1. Make a list of threats to be monitored at operation stage for the particular eco-system.
2. Make a list of the affected threats to be monitored.
3. For each asset make observation4s Oi for every 10 min.
4. Return the sample to the risk assessor, which records the probability of the event occurring.
5. Calculate total_event_rate = events_found/total monitored time.
6. Relative risk (RR) = total_event_rate/risk (risk from catalogue).
7. If RR = 1 do nothing, RR < 1 accept risk, if RR >1 apply mitigation strategy.

6. PROBLEM DEFINITION

The security risk at operation phase is post assessment algorithm which analyses the threats which may cause during attacks by calculating risk rating of each. However, it's better to do pre assessment of the threats by analyzing the behavior of threats attacks from past data. Also, in previous algorithm, the major concerns are assets involved. But in case of pre assessment, we may only consider threats behavior and prepare evaluation chart which helps in calculating risk rating easily and guide us before to be cautious for the risk evolved by them.

7. PROPOSED METHODOLOGY



Now we propose our algorithm which is based on pre assessment analysis of the threats and attacks of security and privacy in cloud computing in following ways:

8. ALGORITHM: DEPLOYMENT AND OPERATION PHASE (PRE ASSESSMENT)

Input: The number of threats.

Output: Relative Risk between the threats of different years.

1. Make a list of number of threats.

2. Make a list of each threat likelihood L(i) and priority P(i).

3. For each threat, Calculate:

- **a.** Probability of Likelihood given the threat is affected (p(i)) = L(i) / 5.0
- **b.** Probability of threat Priority p1(i) = P(i) / 5.0
- **c.** Probability of likelihood regardless of threat p2(i) = p(i) * p1(i) + (1 – p1(i))
- **d.** Probability of threat occurring p3(i) = (p(i) * p1(i)) / p2(i)
- **e.** Sum of all probability of threat occurring.

4. Return the sample to the risk assessor, which records the probability of the event occurring.

5. Calculate, Risk Rating of the each threat.

RR = L(i) * P(i)

6. Then calculate Relative Risk RLR = RR / sum of all probability of threat occurring.

9. EXPERIMENTAL RESULT

In this experimental result we first explain each single year classification with its datasets, we calculate probability of each threat according to our algorithm the main point is to calculate relative risk of each threat after calculating relative risk of each threat comparison is done between the different year is by its relative risk. In this we conclude data sets of 2014 and 2015 year and comparing it with original datasets. According to comparison analysis we draw a graph for each table which is given below:

Some key points:

P: Priority

L: Likelihood

RR: Risk Rating

RLR: Relative Risk

Formula:

$$\textbf{RLR} = \frac{\textbf{RR}}{\textbf{Sum of Probability(Prob)}}$$

Table 1.4: Threat Classification with 2015 Datasets

Threat I'd	P)	(L)	Prob (2015)	RR (P*L)	RR/sum Prob
T1	4	2	0.61	8	0.49
T2	3	4	0.54	12	0.74
T3	4	4	0.76	16	0.99
T4	3	4	0.54	12	0.74
T5	3	3	0.47	9	0.55
T8	3	5	0.6	15	0.93
T9	2	1	0.16	2	0.12
T10	2	3	0.28	6	0.37
T11	3	5	0.6	15	0.93
T12	3	2	0.37	6	0.37

T13	3	4	0.54	12	0.74
T15	1	5	0.2	5	0.31
T16	5	3	1	15	0.93
T27	4	2	0.61	8	0.49
T29	1	2	0.09	2	0.12
T34	1	3	0.13	3	0.18
T35	1	3	0.13	3	0.18
T40	1	2	0.09	2	0.12
T41	4	2	0.61	8	0.49
T42	5	3	1	15	0.93
T50	5	4	1	20	1.24
T51	0	0	0	0	0
T52	3	4	0.54	12	0.74
T53	0	0	0	0	0
T54	4	2	0.61	8	0.49
T55	5	4	1	20	1.24
T56	5	4	1	20	1.24
T57	4	3	0.7	12	0.74
T58	5	5	1	25	1.55
T59	3	3	0.47	9	0.55
T60	3	3	0.47	9	0.55

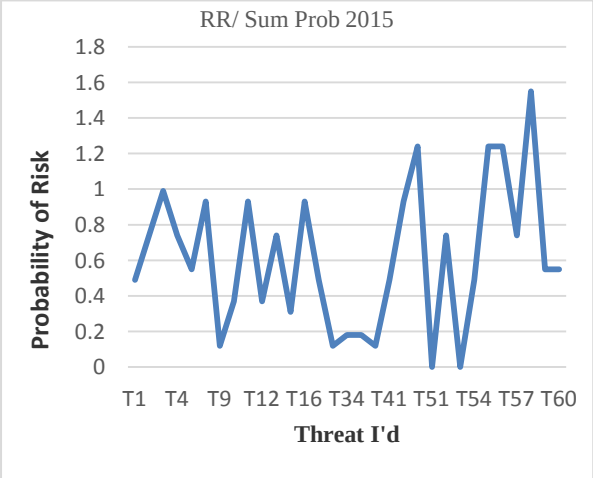


Table 1.5: Threat Classification with 2014 Datasets

Threat I'd	P)	(L)	Prob (2014)	RR (P*L)	RR/sum Prob
T1	4	2	0.61	8	0.51
T2	3	3	0.47	9	0.58
T3	4	5	0.8	20	1.29

T4	3	3	0.47	9	0.58
T5	3	3	0.47	9	0.58
T8	3	3	0.47	9	0.58
T9	2	1	0.12	2	0.13
T10	2	3	0.28	6	0.38
T11	3	4	0.54	12	0.77
T12	3	2	0.37	6	0.38
T13	3	2	0.37	6	0.38
T15	1	4	0.16	4	0.25
T16	5	3	1	15	0.97
T27	4	1	0.44	4	0.25
T29	1	2	0.09	2	0.13
T34	1	3	0.13	3	0.19
T35	1	3	0.13	3	0.19
T40	1	2	0.09	2	0.13
T41	4	2	0.61	8	0.51
T42	5	2	1	10	0.64
T50	5	3	1	15	0.97
T51	0	0	0	0	0
T52	3	3	0.47	9	0.58
T53	0	0	0	0	0
T54	4	3	0.7	12	0.77
T55	5	3	1	15	0.97
T56	5	3	1	15	0.97
T57	4	3	0.7	12	0.77
T58	5	3	1	15	0.97
T59	3	3	0.47	9	0.58
T60	3	3	0.47	9	0.55

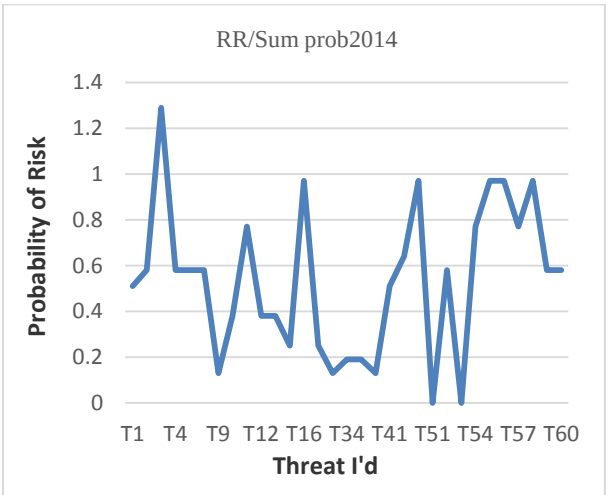


Table 1.6: Threat Classification with its original Datasets

Threat Id	(P)	(L)	Prob of original data	RR (P*L)	RR/Prob
T1	4	3	0.7	12	0.73
T2	3	1	0.64	3	0.18
T3	4	2	0.61	8	0.48
T4	3	1	0.64	3	0.18
T5	3	1	0.64	3	0.18
T8	3	1	0.64	3	0.18
T9	2	2	0.21	4	0.24
T10	2	1	0.12	2	0.12
T11	3	1	0.64	3	0.18
T12	3	1	0.64	3	0.18
T13	3	3	0.47	9	0.54
T15	1	4	0.16	4	0.24
T16	5	4	1	20	1.21
T27	4	2	0.61	8	0.48
T29	1	2	0.09	2	0.12
T34	1	4	0.16	4	0.24
T35	1	5	0.2	5	0.3
T40	1	3	0.13	3	0.18
T41	4	3	0.7	12	0.73
T42	5	3	1	15	0.91
T50	5	3	1	15	0.91
T51			0	0	0
T52	3	2	0.37	6	0.36
T53		2	0	0	0
T54	4	3	0.7	12	0.73
T55	5	2	1	10	0.6
T56	5	3	1	15	0.91
T57	4	2	0.61	8	0.48
T58	5	3	1	15	0.91
T59	3	2	0.37	6	0.36
T60	3	3	0.47	9	0.54

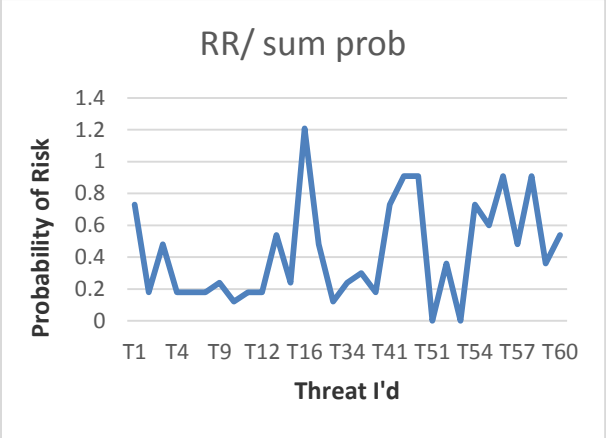
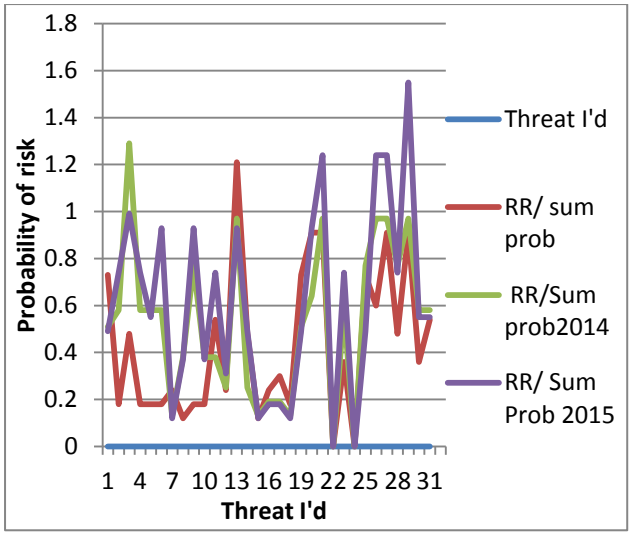


Table 1.7: Relationship between the datasets of 2014, 2015 and original data

Threat I'd	Original (RLR)	2014 (RLR)	2015 (RLR)
T1	0.73	0.51	0.49
T2	0.18	0.58	0.74
T3	0.48	1.29	0.99
T4	0.18	0.58	0.74
T5	0.18	0.58	0.55
T8	0.18	0.58	0.93
T9	0.24	0.13	0.12
T10	0.12	0.38	0.37
T11	0.18	0.77	0.93
T12	0.18	0.38	0.37
T13	0.54	0.38	0.74
T15	0.24	0.25	0.31
T16	1.21	0.97	0.93
T27	0.48	0.25	0.49
T29	0.12	0.13	0.12
T34	0.24	0.19	0.18
T35	0.3	0.19	0.18
T40	0.18	0.13	0.12
T41	0.73	0.51	0.49
T42	0.91	0.64	0.93
T50	0.91	0.97	1.24
T51	0	0	0
T52	0.36	0.58	0.74
T53	0	0	0
T54	0.73	0.77	0.49
T55	0.6	0.97	1.24
T56	0.91	0.97	1.24
T57	0.48	0.77	0.74
T58	0.91	0.97	1.55
T59	0.36	0.58	0.55
T60	0.54	0.58	0.55



10. CONCLUSION

Cloud computing refers to on-demand access to a shared pool of computing resources, providing reduced costs, reduced controlling tasks and increasein business agility. For these reasons, it is a popular example to be used by end users from different works. Security is, however, a major player in thisequation as it can make or break deals for Cloud users and infrastructure providers alike.In this paper, we analysis each threat with its likelihood and the priority value of all the data of 2014 and 2015 year,but in the original data analysis is done by each threat assets value according to that it is calculated. After all the analysis, we compare within it and plot a graph according to an analysis and provide a result. For future we can analysis it by using some simulator for more improvement of security and we take one threat under the observe for some time and not the result what effects are on its assets and threat value regarding with its original data.

11. REFERENCES

[1] Lim, C., Suparman, and A.: Risk analysis and comparative study of the different cloud computing providers in Indonesia. In: 2012 International Conference on Cloud Computing and Social Networking (ICCCSN). IEEE (2012).

[2] Mell, P., Grance, T.: The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Information Technology Laboratory (2011).

[3] Mahesh U. Shankarwar and Ambika V. Pawar:"Security and Privacy in Cloud Computing: A Survey.

[4] Mazhar Ali, Samee U. Khan ,Athanasios V. Vasilakos:"Security in cloud computing: Opportunities and challenges.

[5] M.D. Ryan, Cloud computing security: the scientific challenge, and a survey of solutions, J. Syst. Software. 86 (09) (2013) 2263–2268.

[6] M. Sadiku, S. Musa, O. Momoh, Cloud computing: opportunities and challenges, IEEE Potentials 33 (1) (2014) 34–36.

[7] Kiran M, Khan AU, Jiang M, Djemame K, Oriol M, Corrales M (2012) Managing security threats in Clouds, Digital Research 2012 .

[8] Khan AU, Kiran M, Oriol M, Jiang M, Djemame K (2012) Security risks and their management in Cloud computing. CloudCom, pp 121–128, 2012.

[9] Mariam Kiran; "A Methodology for Cloud Security Risks Management" Springer International Publishing Switzerland 2014.

[10] 2015-isbs-technical-report-blue:" 2015 Information Security Breaches Survey" survey conducted by pwcIn association with info security Europe.

[11] Kiran M, Khan AU, Jiang M, Djemame K, Oriol M, Corrales M (2012) Managing security threats in Clouds, Digital Research 2012.

[12] Khan AU (2013) Data confidentiality and risk management in Cloud Computing, PhD thesis, Department of Computer Science, University of York, 2013.

[13] Whiteside F, Badger L, Iorga M, Shilong Chu JM (2012) Challenging security requirements for US government Cloud computing adoption (draft), Special publication 500-296, NIST, May, 2012.

[14] Catteddu D, Hogben G (2009) Cloud computing: benefits, risks and recommendations for information security, Technical Report, European Network and Information Security Agency (ENISA) 2009.

[15] Information Security Forum (ISF), Information risk analysis methodology (IRAM Accessed April 2014.