Journal of Faculty of Engineering & Technology

**Journal homepage:** [**www.pu.edu.pk/journals/index.php/jfet/index**](http://www.pu.edu.pk/journals/index.php/jfet/index)

**SECURITY METRICS FOR CLOUD BASED INFORMATION RETRIEVAL** **SYSTEM**

M. Iftikhar[[1]](#footnote-1), M. Shoaib

Department of CS & E, University of Engineering & Technology, Lahore, Pakistan

**Abstract:**

Cloud storage based information retrieval system has recently emerged to deliver set of documents. To identify security issues and concerns at design level for preventing security breaches during information retrieval from cloud and achieve the secure cloud storage and retrieval of most relevant information is the major objective of this research. Security Metrics at design level a proposed, which includes Maintainability, Reliability, Availability, Serviceability, Integrity and Confidentiality. The result of case study shows that chances of security breaches reduced by prioritizing the corrective actions, using proposed security metrics. By mitigating design level risks, threats and vulnerabilities in the system achieve security goals for decision making in refining the functionality of Cloud based IR System. Further, the outcomes of proposed metrics can automate in future to observer the cloud environment during interaction of users with the cloud storage.

**Keywords:** Security metrics, Cloud based IR system, Information retrieval security metrics, Cloud security concerns.

1. **Introduction**

Cloud based storage and computing is an innovative Information System(IS) architecture that is visualized as a future storage and computing however for risk assessment various characteristics of cloud storage based computing and retrieval must be discuss include availability and reliability of cloud storage, data integrity, privacy auditing and recovery. Metrics derived or formulated at design level are use to prioritize the corrective actions by discovering the risk and issues earlier. For sharing data and computations, cloud is a scalable network of nodes and implementation of a cloud is applicable at private, enterprise and external level to share data storage resources and computing. A large pool of virtualized resources, easily accessible and can reconfigure dynamically to utilize them at optimal scale known as Cloud. There are a few key features of cloud such as cost, reliability, agility, scalability, maintenance, device and location independency and multi-tenancy; taking into consideration of these key features of cloud six security metrics proposed to identify the level risk and threats at design level.

Information Retrieval (IR) System is a process of defined activities to find, trace, locate and deliver a set of documents according to data needs of users.[[1](#_ENREF_1)] The objective of IR is to gather, systematize, characterize information contents and give access to that information contents.[[2](#_ENREF_2)] Numbers of attackers and hackers are increasing with the appearance of novel and advance technologies in the field of IT and those are waiting to attack or hack data over cloud.[[3](#_ENREF_3)] Due to repositioning to the clouds, from security perspective a number of risks, challenges and threats have been introduced and it effects and fades the value of traditional security and protection mechanism. [[4](#_ENREF_4)] There is a basic need of cloud security to keep cloud up and running continuously, security concerns must be addressed at different levels such as Application level, Network level and Host level. Due to some security breaches the data stored in cloud has been lost or modified in recent times.[[5](#_ENREF_5)] In existing data centers and networks these issues has been raised at design, architecture and implementation level.[[6](#_ENREF_6)] To reveal the security, safety, and possible vulnerability of the complex systems there is a need of a foundational science in the field of computer and communications. Suitable security metrics must be device for impartial comparison and estimation of system designs security.[[7](#_ENREF_7)] As users of information retrieval system are not professionals in the documentation and the choice of words to express their actual need, there is need of reformulation of user queries to improve the cloud based IR system and make it more secure.

In the year of 2009, it has estimated that the amount of data engendered by the internet users would be more then the data engendered in the entire history of humankind through the year 2008. Data growth rate is increasing day by day and a massive volume of data is engendered by the individuals daily.[[8](#_ENREF_8)] Assumptions and abstraction are inherently required for metrics, which is the fundamental challenge for any security metric.[[7](#_ENREF_7)] The degree of security goals such as data confidentiality are identified by a useful metric and these goals can achieved and oblige actions can taken to improve the overall security program.[[9](#_ENREF_9)] The term “security metrics” has become a standard as refering the security level, security strenght, security indicators and security performance. Confidentiality, Integrity and Availability CIA model is the most recognized.[[10](#_ENREF_10)] To win the trust of client and customers cloud computing model have to implement acceptable security.[[11](#_ENREF_11)] Pledge of security of information, integrity and authentication are the most significant foundation for implementing the applications based on cloud computing.[[12](#_ENREF_12)] Metrics at Design metrics level obtained as a measurement of particular feature of system performance and effectiveness.[[13](#_ENREF_13)] Metrics are useful for the design of system which is used to measure many characteristics of a module of a system.[[14](#_ENREF_14)]

There is clear demand for in-depth discussion on security related issues as these are the primary concerns mostly security concerns like data privacy, data confidentiality, and data safety.[[15](#_ENREF_15)] With the increase in usage of on-demand application cyber attacks also increased and in recent times it has been witnessed that data and information have been lost or modified due to some security breach stored in these clouds.[[5](#_ENREF_5)] Primary goal of information security is to protect information assets against risks and threats.[[16](#_ENREF_16)] A Data center is the centralized location, which stored and holds data in large but processing is performed on data at servers therefore the users have concerns on the availability as well as data security.[[17](#_ENREF_17)] New challenges for information retrieval are creating with the increase in information on the web as well as the rapid expansion of inexperienced users.[[1](#_ENREF_1)] It showed in recent survey related to information security that there is highly a need for information security metric.[[18](#_ENREF_18)] Taking under consideration of user perspective cloud is not secure because administrator of the cloud environment system can access the private data of users in cloud computing.[[19](#_ENREF_19)] There is a need of addressing some concerns for Cloud Security standardization and based on cloud security threats.[[20](#_ENREF_20)] As a security solution to increase the flexibility and security of the system, security metrics are applicable.[[21](#_ENREF_21)]

This manuscript organized as follows. Section II discusses and elaborates the proposed security metrics. Section III discusses the evaluation and experimental results of the proposed metrics by using the PITB Cloud. In the end of manuscript, proposed work concluded and future recommendations for the current research mentioned.

1. **Experimental**

By the emergence of Cloud Based Services, the cost to maintain the resources use for storage and retrieval has reduced. As a result, Cloud Storage and Retrieval System implemented by several businesses for reducing the cost but there are some security concerns about cloud, which become a reason of hesitation to move on cloud. Cloud service providers have a legal agreement (SLA) with the users/clients, which emerge as a key aspect to gain the trust of cloud user or client. Agreed terms and conditions mention in SLA must guarantees by cloud service providers.[[22](#_ENREF_22)] To raise the level of security awareness, information security system and the concerned aspects of security measures at design six security metrics have proposed in terms of Maintainability, Reliability, Availability, Serviceability, Integrity, and Confidentiality.

## **Maintainability Metric (MM)**

## In Cloud Environment Maintainability is a significant aspect as Cloud Service Providers have service level agreements (SLAs) with cloud users. Maintainability of a cloud can distinct in terms of likelihood of successful repair actions performed within the given time or agreed service time. The rate of speed and ease with which a cloud service provider can restore the system in case of failure incidence and make available an operational environment to the cloud users for using cloud is measure by Maintainability. Therefore, Maintainability metric can defined in terms of Mean-Time-To-Restore-Cloud-Services (MTRCS).

$MTRCS = \frac{Total Down Time of Cloud Services}{Number of Breaks}$ (1)

Where *Total Down Time of Cloud*: is the time-period of cloud outage and *Number of Breaks* is the count of interruptions/failures during cloud services down time. Note that maintainability metric needs to include time intervals usually hours. Now considering (1) *Maintainability metric (MM)* can express by the below mention equation.

$MM = \frac{Agreed Service Time -MTRCS}{Agreed Service Time}×100$ (2)

For example, if it said that a particular module of the system design has 70% maintainability for one hour, this means that there is 70% probability that the module of the system design will be repair within an hour.

***2.2 Reliability Metric (RM)***

Reliability define as measure of how long a service or the module of a system design can execute its requisite functionality and give services to the cloud user without interlude and interval as agreed. To gain trust of cloud user, cloud service providers must take care of reliability, as cloud users need access of 24/7 to their services and information, so reliability is a challenge. One of the security fears in making decision to shift away from traditional on ground solutions to cloud based storage and retrieval solutions is Reliability. Reliability can express in terms of Mean-Time-Between-Cloud-Incidents (MTBCI).

$MTBCI = \frac{Cloud Service Available Time}{Number of Breaks}$ (3)

Where *Cloud Service Available Time:* is the total uptime of cloud services and *Number of Breaks:* is the count of interruptions/failures during cloud services uptime. Note that reliability metric needs to include time intervals usually hours. Considering (1) and (3) Reliability can expressed in terms of *Mean-Time-To-Restore-Cloud-Services (MTRCS)* and *Mean-Time-Between-Cloud-Incidents (MTBCI).*

$RM = \frac{MTBCI -MTRCS}{MTBCI} ×100$ (4)

##  **2.3 Availability Metric (AM)**

## Ability of a service or a module to execute its requisite functionality when needed or likelihood of a system to work according to the requirements during the required work period is term as availability of service or module. Availability also includes the non-operational interval linked with reliability and maintainability. Availability express in terms of nine and measured in percentage.[[23](#_ENREF_23)] Cloud Service Providers have 99.0% – < 99.9% uptime SLA [[24](#_ENREF_24)] so Availability is almost faultless in cloud environments. A substantial cost imposed in cloud environment due to the downtime time of a cloud. The traditional metric for cloud availability is Uptime, which expressed as a fraction of time a cloud service provider is handling traffic. Uptime expectation express in terms of nine so cloud uptime expressed as

$Cloud Uptime = \frac{MTBF -MTRCS}{MTBF}$ (5)

Where *MTBF*: Mean-Time-Between-Failure, *MTRCS*: Mean-Time-To-Restore-Cloud-Services

Mean-Time-Between-Failure (*MTBF*) can be define as

$MTBF = \frac{CSAT -TDTCS}{Number of Breaks}$ (6)

Where *CSAT*: *Cloud Service Available Time* is the total uptime of cloud, *TDTCS:* *Total Down Time of Cloud Services* is the time of cloud outage, *Number of Breaks:* is the count of interruptions during cloud uptime

Note that availability metric needs to include time intervals usually hours. Cloud service provider can get better the uptime either by tumbling the time to fix the issues or by tumbling the frequency of failure by using *cloud uptime. Here* Availability metric proposed in two ways in first metric calculate the availability of cloud in terms of nine and second metric calculate the availability in terms of percentage. First, Availability of Cloud Services expressed in terms of *MTBF* and *MTRCS* shown in (7). Second, Availability of Cloud Services expressed in terms of as percentage shown in (8).

$Availability = \frac{MTBF}{MTBF +MTRCS}$ (7)

Where

*MTBF*: Mean-Time-Between-Failure

*MTRCS*: Mean-Time-To-Restore-Cloud-Services

$AM = \frac{Agreed Service Time -TDTCS}{Agreed Service Time}×100\%$ (8)

Where

*TDTCS:* *Total Down Time of Cloud Services* is the time of cloud outage.

*Agreed Service Time:* is the time agreed on provided service mentioned in SLA.

## **2.4 Serviceability Metric (SM)**

## Both planned and unplanned cloud storage outages tried to avoided by cloud Service providers that provide services to the cloud users to maintain a focus on cloud uptime. However, the major hindrance for high serviceability is high fault tolerance, since fault tolerance plays a vital role in order to guarantee serviceability of cloud service provider. The ability of cloud service provider to meet SLA and contracted support commitments in terms of maintainability, reliability and availability is define as Serviceability. Consequently, Serviceability correlates with high maintainability, reliability and availability so the relationship of Serviceability and maintainability, reliability, availability expressed in (9), (10) and (11) respectively

$Serviceability ∝ Maintainability $ (9)

$Serviceability ∝ Reliability$ (10)

$Serviceability ∝ Availability$ (11)

Above equations indicates that serviceability is directly proportional to maintainability, reliability and availability. Maintainability of a cloud service provider increase then serviceability of a cloud service provider also increase and vice versa. Reliability of a cloud service provider increase then Serviceability of a cloud service provider also increase and vice versa. Availability of a cloud service provider increase then serviceability of a cloud service provider also increase and vice versa.

As discussed Serviceability is directly proportional to maintainability, reliability and availability, so it can express in terms of maintainability metric (MM), reliability metric (RM) and availability metric (AM) as

$SM = \frac{MM +RM +AM}{3}$ (12)

***2.5 Integrity Metric (IM)***

A critical aspect to a system design based on cloud is information integrity, which defined as preserving and assuring the correctness and reliability of stored information on clouds, which are used to store or retrieve information. Integrity employs to assess the stability of stored information upon later on retrievals, guarantee the fact that the information was same with the originally stored information. Integrity averts a system from involuntary alteration to information that is a significant facet of information security stored on cloud storage. Cloud service provider has to guarantee the integrity of stored information to get confidence of cloud users. Cloud environment posses the privacy concern as an imperative facet of security fear in cloud as cloud service providers may possibly access the stored information but it is gratify by using cryptography techniques. However to enable the information integrity in cloud environment the authentication method be obliged to function correctly. Authentication method entails authentication actions taken or force by cloud service providers to validate and authorize the identification of the genuine cloud users. Authentication is a method adopts to validate the claim of retriever to access the stored information on cloud, so the cloud retriever can get the information according to its need. Integrity errors consist of illicit addition, deletion, alteration, subscription and publishing the information stored on cloud storage. Integrity Metric can expressed in terms of Authentication Actions (AUA) and Integrity Errors (IE) as

$IM= \frac{AUA}{AUA +IE}$ (13)

Where *AUA*: total number of authentication actions, *IE*: number of integrity errors.

***2.6 Confidentiality Metric (CM)***

 Information Confidentiality defines as the property to bind the access of information and averts the disclosure of information to unauthorized users. There are many concerns associated to confidentiality such as security, privacy and trust. Confidentiality is a measure of security of cloud storage from malicious attacks. Confidentiality of information can express in terms of information privacy from liabilities and security attacks. Since the information stored on cloud storage can be sensitive, thus cloud service providers provide assurance to the cloud users about the vulnerabilities, liabilities and external attacks by malicious attackers by implementing and ensuring confidentiality. Confidentiality is a significant facet to preserve the privacy of the cloud users whose information stored in data centers of cloud service providers. To determine the confidentiality many factors are considers in proposed metric that showed in Table 1.

Table 1: Factors to Measure Confidentiality

|  |  |
| --- | --- |
| **Symbols** | **Confidentiality Measuring Factors (CMF)** |
| CPCA | Cryptographic Protection of Cloud Confidentiality Algorithm |
| CPEK | Cryptographic Protection of Encryption Keys |
| AC | Access Controls of Cloud Service Providers |
| AM | Authentication Mechanisms |
| SCI | Security Classification for information |

Confidentiality Metric can express in terms of function of proposed Confidentiality Measuring factors (CMF) as

$CM = \sum\_{i=1}^{n} f\left(CMF\_{i}\right) ∴n=total no. of CMFs $ (14)

Where

$f\left(CMF\_{i}\right) = f\left(f\_{1},f\_{2} ,f\_{3} ,f\_{4} ,f\_{5}\right) ∴ n=5$ (15)

*f(CMF)* is the function of independent factors that impact the confidentiality of a cloud. For evaluating these factors following equations are considered

$f\_{1} = w\_{1}× CPCA $ (16)

$f\_{2} = w\_{1}× CPEK $ (17)

$f\_{3} = w\_{2}× AC $ (18)

$f\_{4} = w\_{2}× AM $ (19)

$f\_{5} = w\_{3}× SCI $ (20)

Weights assigned based on the relative significance of Confidentiality Measuring Factor (CMF). The weights used above assumed equivalent to the following values

$w\_{1}=3$, $w\_{2}=2$, $w\_{3}=1$.

Above equations indicates that if the strength of Confidentiality Measuring Factor (CMF) identified then confidentiality achieve by the cloud service provider can computed.

1. **Results and Discussions**

To evaluate proposed security metrics PITB Cloud “Punjab Information Technology Board (PITB) Cloud” [[25](#_ENREF_25)]has been analyzed. PITB Cloud is the project of Punjab Information Technology Board (PITB), which was setup by the government of Punjab Pakistan to provide secure cloud computing services. PITB Cloud uses Microsoft System Center 2012[[26](#_ENREF_26)] application service model to provide cloud-based services in Pakistan. To measure level of risk, threat and vulnerabilities in an Information Retrieval System based on PITB Cloud “Maintainability Metric (MM), Reliability Metric (RM), Availability Metric (AM), Serviceability Metric (SM), Integrity Metric (IM) and Confidentiality Metric (CM) are evaluated to measure the security aspects of PITB Cloud based IR System.

##  **3.1 Maintainability Metric (MM) Evaluation**

## As maintainability is the mean time a cloud service provider take to restores its services, thus maintainability can be measure in terms of Mean-Time-To-Restore-Cloud-Services (MTRCS). Maintainability measure needs to include time interludes that are usually hours.

*Total Down Time of Cloud Services = 1 hour*

*Number of Breaks = 2*

By equating the value in (1) *MTRCS = 0.5 hours.* It means a cloud take 0.5 hours or 30 minutes to restore its services if the numbers of breaks (count of interruptions/failures during cloud services down time) is 2. Now the percentage value of maintainability of cloud can be measure by using (2)

*Agreed Service Time = 24 hours*

By equating the value in (2) MM = 97.92 % it means that the services of PITB Cloud is 97.92% maintainable for one hour of downtime, so it can be stated that there is a 97.92% probability that the services of Cloud will be repaired within an hour. The value of maintainability of a Cloud storage based IR system can improved if the percentage value of maintainability known which eventually increase the customer gratification of storing data on cloud and recognize the concerns in cloud based IR system.

##  **3.2 Reliability Metric (RM) Evaluation**

## As Reliability is a measure of how long a cloud service can perform its requisite functionality and deliver the services to the cloud user without intermission. Reliability can be measure in terms of Mean-Time-To-Restore-Cloud-Services (MTRCS) and Mean-Time-Between-Cloud-Incidents (MTBCI). MTRCS is already measure in evaluation of Maintainability Metric and MTBCI can be measure by using (3).

*Cloud Services Available Time = 23hours,* as Services of Clouds are down for 1 hour

*Number of Breaks = 2*

By equating the value in (3) *MTBCI = 11.5 hours.* It means that the average value between PITB Cloud incidents is 11.5 if the numbers of breaks (count of interruptions/failures during cloud services uptime) is 2. Now the percentage value of reliability of a Cloud can be measure by using (4)

*MTBCI = 11.5 hours*

*MTRCS = 0.5 hours*

By equating the value of *MTBCI* and *MTRCS* in (4) the value of RM = 95.65 %. It means that the services of PITB Cloud have 95.65% reliability for Mean-Time-To-Restore-Cloud-Services (*MTRCS*) of 0.5 hours and Mean-Time-Between-Cloud-Incidents (*MTBCI*) of 11.5 hours. Thus, it can be state that there is 95.65 % probability that the services of PITB Cloud perform its requisite functionality and deliver the services to the cloud user without interlude. The reliability of a Cloud based IR system can improved if the percentage value of reliability known which eventually increase the trust of customer to store data in cloud and to recognize and decrease the vulnerability faced by the cloud based IR system.

## **3.3 Availability Metric (AM) Evaluation**

## As Availability defined as the service ability to perform its requisite functionality when needed, therefore the availability of a Cloud defined in terms of Cloud Uptime. Cloud Uptime is one of the traditional metric for availability that define as fraction of time a cloud service provider is handling traffic. Uptime expectation are usually measured in terms of nines so cloud uptime can measured by (5) but before measuring the Cloud Uptime, there is a need of measuring Mean-Time-Between-Failure (MTBF) using (6)

*Cloud Services Available Time = 23hours,* as Services of Clouds are down for 1 hour

*Total Down Time of Cloud Services = 1 hour*

*Number of Breaks = 2*

By equating the value in (6) *MTBF = 11 hours.* It means that the average value time among PITB Cloud failures is 11 hours if the numbers of breaks (count of interruptions/failures during cloud services uptime) is 2. Now the Cloud Uptime of PITB Cloud can be measure by using (5)

*MTBF = 11 hours*

*MTRCS = 0.5 hours*

By equating the value of *MTBF* and *MTRCS* in (5) *Cloud Uptime* = 0.95 it means that if PITB Cloud uptime is 0.95 then after expressing Cloud Uptime in terms of nine[[27](#_ENREF_27)] the downtime per year, per month and per week is shown in Table 2.

Table 2: Uptime and downtime in terms of nine

|  |  |  |  |
| --- | --- | --- | --- |
| **Uptime** | **Downtime per Year** | **Downtime per month** | **Downtime per week** |
| 0.95 | 18.25 days | 36 hours | 8.4 hours |

Availability of Cloud Services can be measure either by using (7) or (8).

*Total Down Time of Cloud Services = 1 hour*

*Agreed Service Time = 24 hours*

By equating the value in (7) and (8) Availability = 0.956 and AM = 95.83 % it means that the services of PITB Cloud have 95.83 % availability for one hour of down time, this means that there is a 95.83 % probability that services of PITB Cloud will work according to the requisite during the required period of work. The availability of a Cloud based IR system can improve if the percentage value of availability known which help to maintain the uptime of cloud based IR system to recognize and decrease the threats.

***3.4 Serviceability Metric (SM) Evaluation***

As high serviceability is high fault tolerance and guarantees of cloud service providers in terms of maintainability, reliability and availability. Therefore, Serviceability correlates with high maintainability, reliability and availability. Thus serviceability is directly proportional to maintainability, reliability; availability shown in (9), (10) and (11) respectively, and can be measure by using (12). By equating the value of MM = 97.92 %, RM = 95.65 % and AM = 95.83 % in (12) the value of serviceability metric is evaluated as SM= 96.47 %. It means that the PITB Cloud have 96.47 % serviceability for 97.92 % maintainability, 95.65 % reliability and 95.83 % availability. Therefore, it can stated that there is a 96.47 % probability that of cloud service provider is able to meet their Service Level Agreements (SLA) and contracted support commitments in terms of maintainability, reliability and availability.

***3.5 Integrity Metric (IM) Evaluation***

As Integrity is a measure of preserving and assuring the correctness and reliability of stored information on cloud storage. Integrity of Cloud based IR system can be measure in terms of Authentication actions and integrity errors. Authentication actions taken or imposes by cloud service providers to authenticate and confirm the identification of the genuine cloud customers and Integrity errors include illicit addition, deletion, alteration, subscription and publishing the information kept on cloud storage. Integrity provided by cloud service provider can be measure using (13).

*AUA = 15*

*IE = 2*

By equating the value in (13) IM = 88.24 % it means that a PITB Cloud have 88.24 % integrity for 15 *Authentication Actions (AUA)* and *2 Integrity Errors (IE).* Therefore, it can stated that there is 88.24 % probability that a Cloud preserve and assure the correctness and reliability of stored information on its cloud storage and sustain the consistency of stored information upon later retrievals, confirming the fact that the information was same with the originally stored information in cloud based IR system. The integrity level of Cloud based IR system can be improve if the percentage value of integrity is known which help to sustain the integrity of cloud storage and program the remedial actions to preserve correctness and reliability of stored information on cloud.

***3.6 Confidentiality Metric (CM) Evaluation***

As Confidentiality of information is a measure to provide limited access of information and prevents the disclosure of information to unauthorized users, confidentiality can be measure with the help of Confidentiality Measuring factors (CMF). To measure the confidentiality of PITB Cloud, the values of Confidentiality Measuring factors for PITB Cloud based on application service model of Microsoft system center 2012 shown in Table 3. [[28](#_ENREF_28), [29](#_ENREF_29)]

Table 3: Confidentiality Measuring Factors Values

|  |  |
| --- | --- |
| **Symbols** | **Confidentiality Measuring Factors (CMF)** |
| Cryptographic Protection of Cloud Confidentiality Algorithm(CPCA) | Triple Data Encryption Algorithm(3DES),Secure Hash Algorithm (SHA-1, SHA-2), AES and RSA algorithms |
| Cryptographic Protection of Encryption Keys(CPEK) | [Advanced Encryption Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard) (AES-256) |
| Access Controls of Cloud Service Providers (AC) | Network Access Protection (NAP) Role-based access control |
| Authentication Mechanisms(AM) | PKI certificates, Self-signed certificates, Service certificates and  Identity certificate |
| Security Classification for information on Cloud (SCIC) | Public, Sensitive, Private, Confidential |

To evaluate the Confidentiality Metric the first step is to find out the values of Confidentiality Measuring factors (CMF).

* There are five cryptographic algorithms that are used for the protection of cloud confidentiality so the value of CPCA = 5.
* If the Encryption Standard used by a cloud is AES-128 bits then the value of CPEK = 1 and if AES-256 bits used then CPEK = 2.
* Access controls provided by cloud service provider are of two types so the value of AC = 2.
* Four Authentication Mechanisms are used to authenticate the user or machine so the value of AM = 4.
* Security of information on cloud is classify into four levels so the value of SCIC = 4.

The next step is to evaluate the function of confidentiality measuring factors *f(CMF)* via calculating the values of independent factors that impact the confidentiality of a cloud by using (16-20).

For CMF 1: $f\_{1 }= 3×5= $ 15

For CMF 2:$f\_{2 }= 3×2=6$

For CMF 3: $f\_{3 }= 2×2=4$

For CMF 4: $f\_{4 }= 2×4=8$

For CMF 5:$f\_{5 }= 1×4=4$

By equating the value of independent factors that impact the confidentiality in the function of confidentiality measuring factors *f(CMF)* using (14).

$CM =15+6+4+8+4$ = 37

By equating the value in (14) CM = 37 it means that the higher the value of confidentiality measuring factors the higher will be cloud confidentiality, so it can stated that if the strength of *CMFs* is high then the confidentiality attain by the cloud service provider is high and vice versa.

**Conclusion**

The espousal of Information Retrieval Process with the growth of World Wide Web (WWW) and need of retrieving information of user surpass day by day. The process of information retrieval based on retrieving information from cloud storage known as Cloud based Information Retrieval (IR) System. To inhibit security breaches during information retrieval from cloud storage, there is a need to identify security issues and concerns faced by Cloud based Information Retrieval (IR) System. For the solution of this problem, six security metrics proposed to achieve security goals for decision making in refining the functionality of Cloud based IR System. To evaluate the proposed metrics the PITB Cloud based on Microsoft System Center 2012 application service model analyzed to measure the security aspects. As a result, security of Cloud based IR System is measure to reduce the current complexity and to mitigate the risks, threats and vulnerabilities in the system, which helps in, prioritize the proactive and corrective actions.

An inspiring issue regarding the enhancement of this research work is to automate the outcomes of proposed metrics so that a cloud service provider can observer the cloud environment when user interacts with the cloud storage. These metrics computed automatically to illustration the maintainability, availability, reliability, serviceability and confidentiality level of a Cloud. Additional issue which can be address to conduct a comparative study of Cloud based IR system based on the comparison of the performance of Cloud based IR system of several Cloud service providers with proposed metrics.

**Acknowledgement**

This research paper extracted from the M.Sc. thesis of first author which has been published at University of Engineering and Technology Lahore in 2014.

**References**

[1] Bouramoul A., Kholladi M.-K.and Doan B.-L., "PRESY: A Context based query reformulation tool for information retrieval on the Web", Journal of Computer Science (JCS); 6 (4), 470-477 (2011).

[2] Qureshi M.M. and Shoaib M., "An Efficient Indexing and Searching Technique for Information Retrieval for Urdu Language", Pakistan Journal of Science; 62 (3), 172-176 (2010).

[3] Porwal A., Maheshwari R., Pal B.and Kakhani G., "An Approach for Secure Data Transmission in Private Cloud", International Journal of Soft Computing and Engineering (IJSCE) ISSN; 2231-2307 (2012).

[4] Zissis D. and Lekkas D., "Addressing cloud computing security issues", Future Generation Computer Systems; 28 (3), 583-592 (2012).

[5] Bhadauria R., Chaki R., Chaki N.and Sanyal S., "A survey on security issues in cloud computing", Journal of Computer Science (JCS); (2011).

[6] Pallis G., "Cloud computing: the new frontier of internet computing", Internet Computing, IEEE; 14 (5), 70-73 (2010).

[7] Stolfo S., Bellovin S.M.and Evans D., "Measuring security", Security & Privacy, IEEE; 9 (3), 60-65 (2011).

[8] Thuraisingham B., Khadilkar V., Gupta A., Kantarcioglu M.and Khan L., "Secure data storage and retrieval in the cloud", CollaborateCom; 1-8 (2010).

[9] Juneja M.D., Arora M.K.and Duggal M.S., "Developing Security Metrics for Information Security Measurement System", (2011).

[10] Savola R., "A Security Metrics Taxonomization Model for Software-Intensive Systems", JIPS; 5 (4), 197-206 (2009).

[11] Chow R., Golle P., Jakobsson M., Shi E., Staddon J., Masuoka R.and Molina J., "Controlling data in the cloud: outsourcing computation without outsourcing control", ACM workshop on Cloud computing security; 85-90 (2009).

[12] Tsai C.-L., Lin U.-C., Chang A.Y.and Chen C.-J., "Information security issue of enterprises adopting the application of cloud computing", Networked Computing and Advanced Information Management (NCM); 645-649 (2010).

[13] Shazia, M. Shoaib, Iqra, K. Kalsoomand S. Majid A.F.M., "Software Metrics for an Efficient Design of Ontologies", Pakistan Journal of Science; 63 (1),(2011).

[14] Shazia, M. Shoaiband A. Shah A.F.M., "Software Design Quality Metrics for Web Based Applications", Pakistan Journal of Science; 63 (1),(2011).

[15] Kulkarni G., Gambhir J., Patil T.and Dongare A., "A security aspects in cloud computing", Software Engineering and Service Science (ICSESS); 547-550 (2012).

[16] Popovic K. and Hocenski Z., "Cloud computing security issues and challenges", MIPRO; 344-349 (2010).

[17] Kandukuri B.R., Paturi V.R.and Rakshit A., "Cloud security issues", IEEE International Conference; 517-520 (2009).

[18] Kowalski S., "Modelling Static and Dynamic Aspects of Security: A Socio-Technical View on Information Security Metrics", Models and Modeling Methodologies in Science and Engineering International Conference (2011).

[19] Reddemma Y., Thirupathi L.and Gunti S., "A Secure Model for Cloud Computing Based Storage and Retrieval", SIGCOMM Computer Communication Review; 39 (1), 50-55 (2009).

[20] Lee K., "Security Threats in Cloud Computing Environments1", International Journal of Security and Its Applications; 6 (4),(2012).

[21] Blasi L., Savola R., Abie H.and Rotondi D., "Applicability of security metrics for adaptive security management in a universal banking hub system", Fourth European Conference on Software Architecture; 197-204 (2010).

[22] Patel P., Ranabahu A.and Sheth A., "Service level agreement in cloud computing", (2009).

[23] "Availability (system) <[http://en.wikipedia.org/wiki/Availability\_(system)>"](http://en.wikipedia.org/wiki/Availability_%28system%29%3E%22).

[24] "Google Cloud Storage, Google Prediction API, and Google BigQuery SLA <https://developers.google.com/storage/docs/sla>".

[25] "PITB Cloud <[http://www.pitbcloud.pk/>"](http://www.pitbcloud.pk/%3E%22).

[26] "Microsoft System Center 2012 <[http://technet.microsoft.com/>](http://technet.microsoft.com/%3E), <[http://technet.microsoft.com/en-us/library/cc507089.aspx>"](http://technet.microsoft.com/en-us/library/cc507089.aspx%3E%22).

[27] "High availability <[http://en.wikipedia.org/wiki/High\_availability>"](http://en.wikipedia.org/wiki/High_availability%3E%22).

[28] "Technical Reference for Cryptographic Controls Used in Configuration Manager <<http://technet.microsoft.com/en-us/library/hh427327.aspx#BKMK_crypographics_server>">.

[29] Rouse M., "Microsoft System Center Configuration Manager 2012 <[http://searchwindowsserver.techtarget.com/definition/Microsoft-System-Center-Configuration-Manager-2012>"](http://searchwindowsserver.techtarget.com/definition/Microsoft-System-Center-Configuration-Manager-2012%3E%22).

1. Corresponding Author email: masoomazafri\_046@yahoo.com

 Phone Off: 0092-42-99231257 [↑](#footnote-ref-1)