Journal of Information Technology & Software Engineering

Reddy et al., J Inform Tech Softw Eng 2018, 8:2
DOI: 10.4172/2175-7866.1000230

Research Article Open Access

Security Measures in Distributed Approach of Cloud Computing

Shirisha Reddy K[1*], BalaRaju M[2] and Ramana N[3]

[1]*Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Telangana, India*

[2]*Department of Computer Science and Engineering, KITE, JNT University, Telangana, India*

[3]*Department of Computer Science and Engineering, Farah Engineering College, Telangana, India*

[*]**Corresponding author:** Reddy KS, Research Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Telangana, India, Tel: 484 255 1319; E-mail: Shirishakasireddy20@gmail.com

Received date: February 25, 2018; **Accepted date:** March 31, 2018; **Published date:** April 10, 2018

Abstract

Cloud computing has given a new approach of data accessing in a distributed manner, where the users has the advantage of higher data accessing feasibility. This approach works on the approach of outsourcing the storage requirements in public provider. The distributed approach has the advantage of low cost data accessing, scalable, location independent and reliable data management. It is observed that Conventional approaches are focused to achieve the objective of reliable and secure data access in cloud computing. However the signaling overhead in these approaches was not explored: in the exchange of control signal in cloud computing, it is needed that lower effort should be made for authentication and data integrity, so as more accessing provision exists. A new monitoring scheme is proposed to minimize the signaling overhead by monitoring record systems. In this paper, security issues also focused. In this process, at each of the data exchange, security risk arises, which are evaluated by different security measure such as Mean failure cost (MFC), and multi dimension failure cost (M2FC) To demonstrate our approach, To develop the suggested objectives, MATLAB interfacing with data feed toolbox was used, Effectiveness of the proposed method has been shown by the experimental results.

Keywords: Cloud computing; MFC; Distributed approach; Matlab; Multi dimension failure cost

Introduction

Cloud computing is an rising model of computing, which give computing an open software. It can be characterized as the conveyance of on-request registering belongings via the Internet on restitution for each utilization premise. Resources (as an example, processor computing time and information garage) are provisioned steadily finished the Internet and their subscribers are charged in mild of the utilization of PC belongings. There are many analogues for Cloud Computing. For ideal, the National Institute of Standards and Technology defines Cloud Computing as "a version which grants handy, on-call for network get right of entry to a shared pool of configurable computing sources (e.g., networks, storage, server, packages and offerings) that can be swiftly provisioned and released with minimum control attempt or service company interplay". Cloud computing affords its administrations as 3 layers of administrations that deliver infrastructure assets, application platform and software program consisting of patron offerings. Infrastructure as a Service (IaaS) gives the essential framework to server registering, getting ready, garage, and structures administration.

The platform as a provider (PaaS) layer shows a layer where clients can send and introduce their packages. Software as a Service (SaaS) offers applications through a web application to a large wide variety of customers without installing on their PCs. Cloud computing provides every one of the blessings of an utility framework as a long way as frugality of scale, adaptability and accommodation, but raises big problems like lack of manipulate and lack of protection. In any case, as extra information about people and businesses are placed in the cloud, troubles are beginning to expand mainly within the range of safety. Truth be told, the outsourcing of records clients makes it tough to hold up the trustworthiness and safety of information, and accessibility, which causes proper results. Security is the extensive take a look at in allotted computing systems [1-9]. Truth be informed, as in line with a look at directed by using International Data Group (IDG) [10], Cloud Computing.

Methodology

First, we developed a reliable link with minimum link overhand in terms of delay factor and data accuracy. The simultaneous signaling overhead to access a cloud server is optimize by allocating a higher reliable link with lower delay constraint and higher access data accuracy. The operational flow is shown in Figure 1.

Next phase, over this link, security concern is focused. When a source sends a data it operates in 2 level of accessing as shown in Figure 2. In this process, client send an request for data to a registered cloud server and intern, the cloud server pass the data to host server to fetch the data. In this process, at each of the data exchange, security risk arises, which are evaluated by different security measure such as Mean failure cost (MFC), and multi dimension failure cost (M2FC) [11].

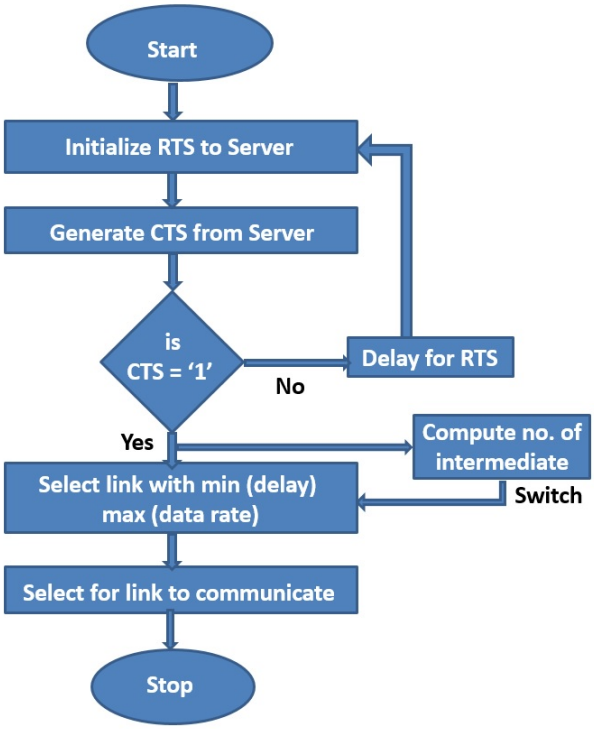

Figure 1: Flow chart for operational flow.

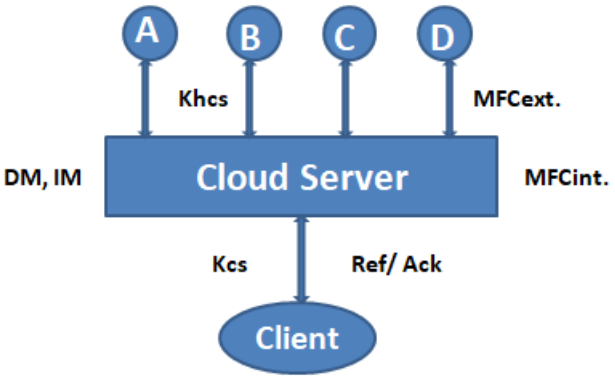

Figure 2: Network modeling of monitoring system.

During the data exchange, 4 security cases were observed, which could be an intentional (due to attacker) or unintentional (due to system or power failure) process.

Cloud server giving true ack. but no data accessed

Cloud server giving false ack. and no data is accessed.

Cloud server true ack. but host false ack.

Cloud server true ack. And host true ack., but no data accessed.

The concept of mean failure cost (MFC) in general is a measure of dependability and in particular a measure of cyber security. The MFC represents to a hypothetical model that evaluates this arbitrary variable regarding commercial loss per unit of working time (eg $/h) because of security dangers. The MFC gives a safety effort that relies upon security prerequisites, stakeholder interest, and the architectural component of a system. Actually, it differs as per the partner and considers the change of wagers that a partner has on the satisfaction of every security necessity, the difference in the cost of disappointment starting with one prerequisite then onto the next, the failure from requirement of one segment to another and the change in the effect of failure of one partner to another. The mean failure cost is represented as [10]:

MFC=ST*DP*IM*PT

MFC is a vector with the same number of contributions as there are framework partners and MFCi is an irregular variable that speaks to the cost to the Hi partner that can come about because of a security rupture.

ST is the wagering grid: a framework where the lines represent the partners, the sections represent to the security necessities, and the ST cell (H, R) is the stake H has in fulfilling the R prerequisite. A wager is a budgetary intrigue that can be lost by an invested individual when R fails. The betting matrix is filled, push by push, by the relating partners.

DP is the unwavering quality network: a cluster where lines represent to system security necessities, sections represent to framework segments, and DP (R, C) is the likelihood that the system does not meet prerequisite R if part C is submitted. The DP lattice is fi lled by the framework engineer who knows the part every segment plays in the accomplishment of every necessity.

IM is the impact matrix: an exhibit where lines are framework segments, segments are security dangers, and IM (C, T) is the likelihood that the C part is bargained if a T. danger appears. IM is filled by the check and approval group, who know how the different security dangers compromise segments.

PT is the threat vector: a vector that has the same number of contributions as dangers in our risk model, and PT (T) is the likelihood that the T. PT danger is brimming with security gear, which knows the setup of the risk likelihood of event of every risk per unit of working time) inside which the framework works. The MFC demonstrate is utilized to evaluate security holes in some genuine word applications, for example, A web based business framework [10] and a Cloud Computing (CC) framework [12-14].

In the MFC coding, to govern the security measure Dependency matrix (DM) and Impact matrix (IM) is suggested. These 2 matrixes are used for data routing and security access. Where in DM is used for trafficking the data from a reliable Host to Source as per the entry of DM, the IM is used to record the data failure conditions arise.

Wherein DM and IM are used for link selectively and failure observation, there is a need to maintain a security metric for each link to define the trustiness property in cloud computing [15-17].

In this work to derive a trustiness factor, IM is used. IM consist of all data failure records observed during data exchange. Wherein in the conventional model it is used as a administrative record to define the link reliability, we define a security trust factor called 'multidimensional trust factor' (M2TF) to improve the security concern in CC.

The M2TF builds a reputation for each of the link from a source to a host at cloud server using 2 reputation factor α, and β (=1) Where α defines the positive trust factor, and β is used for negative trust factor. A higher value of α is selected for data exchange on a request.

In this approach, an updation factor 'ki' is used as a reputation updation factor which is set as one for a successful data exchange or a zero for unsuccessful exchange.

$\alpha := \alpha + k_i$

$\beta := \beta + (1 - k_i)$

Case 1, Occurs, k_{cs}

(CS) is set 0., $K_{cs}=0$

Case 2, $K_{cs}= 1$;

Case 3, $K_{ch}=1$;

Case 4, $K_{ch}=0$; $K_{cs}= 1$;

At each of the data access request, the two security metrics is observed and a link with ($\alpha > \beta$) is trusted for data exchange.

MATLAB simulation results and observation

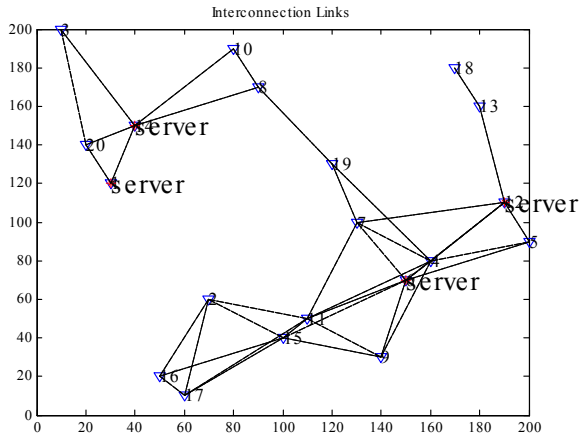

Figure 3: Interconnection links for the network topology.

Figure 3 illustrates the link connections for a cluster network with deployed server and client nodes. The communication links are built on the possible communication range o each unit node. The client node communicates with the host server via registered cloud server to the host server. In this process, the client server request for a link to the host server via a cloud to exchange data between two nodes [18-20].

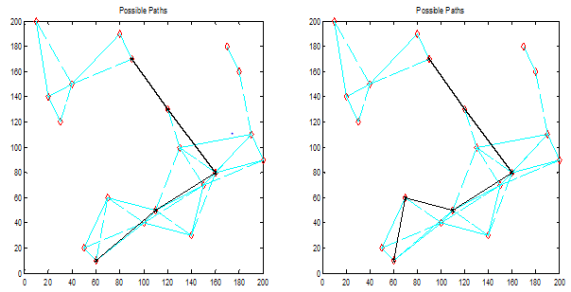

Figure 4: Possible link paths from source to sink.

Figure 4 illustrates all possible paths from source to sink, which could be used for communication. The one hope links are used for the data communication based on communication range, a broadcasting of link request is generated, and all the possible links capable of data exchange acknowledge to offer a communication path for data exchange. In the process of communication, one of the best fit path is selected for communication [21].

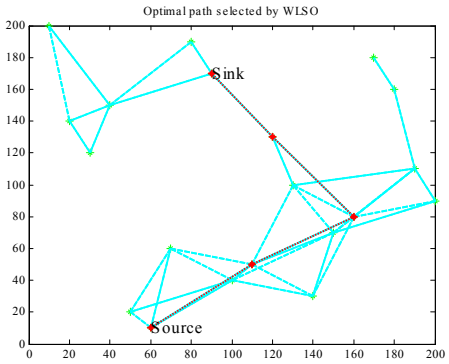

Figure 5: Selected path from a source to sink.

The best-fit selected path is illustrated in Figure 5. The possible paths a optimized based on the suggested weighted link optimization scheme, proposed in our earlier work. This selected path is used in data exchange, where the source node called 'client' forward the data from source to sink called 'Host' to fetch requested data. In this communication process, single or multiple cloud network servers were used in data exchange [22,23].

In the selection of this optimal link, the trustiness factor of the selected links is derived. A higher value of positive link forwarding factor (α) is selected, satisfying the condition of ($\alpha > \beta$). The optimization process allocate the server switching to a link with higher reliability which result in faster data exchange. the impact of measuring metric on the trustiness based link switch is as presented below.

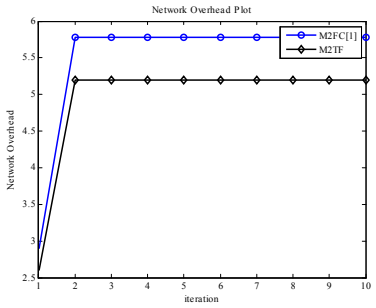

Figure 6: Network overhead plot.

The network overhead is defined as the number of request generated over the number of request been successfully acknowledged. To validate the proposed M2TF approach, a conventional M2CF [1] approach is compared. The overhead is minimized by about 0.7% for the proposed approach, due to the faster data exchange as carried out on a reliable communication path. The initial overhead in this case is observed to be lower to a value of 2.5, however in the increase in communication iteration, the overhead get increase due to repetitive link contention for the failure paths. This repetitive contention leads to higher overhead in the network, whereas a faster clearance due to reliable path leads to lower in overhead (Figure 6).

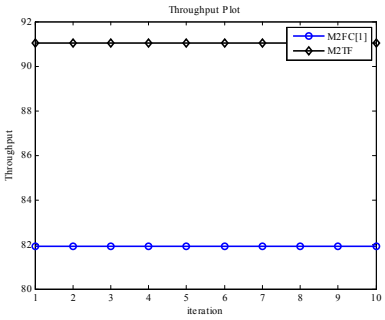

Figure 7: Network throughput plot.

The network throughput observed for the two methods is illustrated in Figure 7. It is observed that, the throughput of the proposed approach is increased by 9% as compared to the conventional M2CF coding. In the proposed approach, the path with highest trust factor is chosen, which leads to lower in delivery failure and improves the network throughput. The two methods retains a steady throughput with course of communication iteration, as the link reliability are defined with observed successful data exchange, and links with M2TF approaches are observed to be more reliable compared to the conventional M2CF [11] approach.

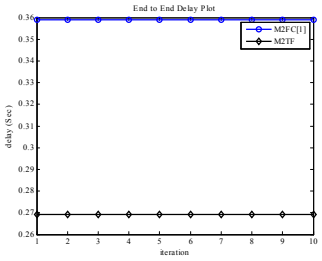

Figure 8: End to end delay

The link reliability directly impacts on the communication delay. The end to end delay is a measuring unit to define the delay factor in data exchange. This delay is defined as the total time taken for data exchange from a source to sink. The delay factor in the proposed approach is observed to be 0.09Sec lower in comparison to the conventional M2FC approach. The delay minimization in due to a lower failure rate for the proposed approach due to higher link reliability. A similar case analysis is carried to observe the impact of higher client density in the network. The increase in number of client node increases the contention probability which effects the measuring metrics. The observed parameters are as illustrated below. The network density in this case is taken for 45 units (Figures 8-14).

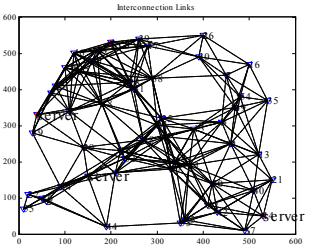

Figure 9: Network layout with 45 communicating units.

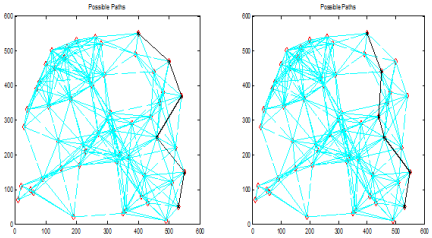

Figure 10: Possible paths for selection from a source client to host sink.

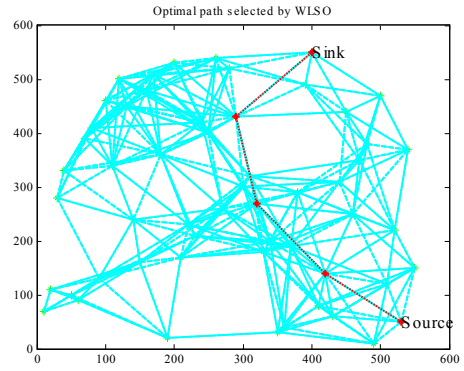

Figure 11: Optimal path with highest trustiness factor for data exchange.

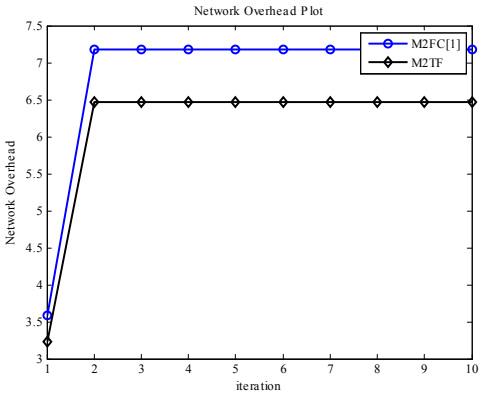

Figure 12: Network overhead plot for the developed approaches at network density = 45.

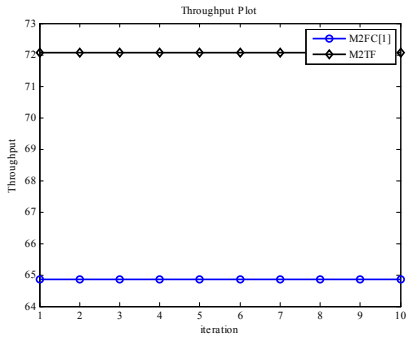

Figure 13: Network throughput plot for the developed approaches at network density = 45.

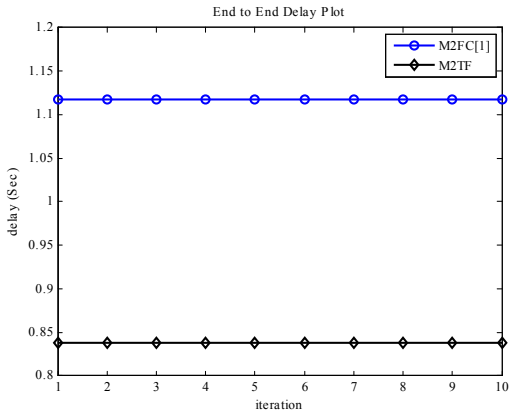

Figure 14: End to end delay plot for the developed approaches at network density = 45.

Conclusion

Sharing data in cloud when the cloud service provider is mistrusted is an issue. Risk assessment is a imperative system in Information Security Management. Enterprise has to adopt systematic and well-designed process for determining information security risks to its properties. However, we illustrated some approaches that protect data seen by the cloud service provider while getting shared among many users. The end to end delay is a measuring unit to define the delay factor in data exchange. This delay is defined as the total time taken for data exchange from a source to sink. The delay factor in the proposed approach is observed to be 0.09Sec lower in comparison to the conventional M2FC approach. The delay minimization in due to a lower failure rate for the proposed approach due to higher link reliability.

Acknowledgement

I thank for the facilities provided by VBIT-FIST R&D for my research and implementation.

References

1. Demchenko Y, Gommans L, De Laat C, Oudenaarde B (2000) Web Services and Grid Security Vulnerabilities and Threats Analysis and model. IEEE 403: 262-267.
2. (2008) Amazon s3 availability event.
3. Fomin VV, Vries HJ, Barlette Y (2007) information technology-security techniques-information security risk management, Int'l Org Standardization.
4. Boehme R, Nowey T (2008) Economic security metrics. Dependability Metrics, pp: 176-187.
5. Wang JA, Xia M, Zhang F (2009) Metrics for information security vulnerabilities. Proceedings of Intellect base International Consortium 1: 284-294.
6. Saripalli P, Walters B (2009) A quantitative impact and risk assessment framework for cloud security. IEEE 3rd International Conference on Cloud Computing Oulu Finland, pp: 280-288.
7. Mell P, Grance T (2009) Effectively and securely using the cloud computing paradigm. ACM Cloud Computing Security Workshop, pp: 1-69.

8. Khaba MV, Santhanalakshmi M (2010) A multiple-replica remote data possession checking protocol with public verifiability.
9. https://www.idg.com/news/cloud-continues-to-transform-business-landscape-as-cios-explore-new-areas-for-hosting/
10. Jouini M, Aissa AB, RabaiLBA, Mili A (2012) Towards quantitative measures of information security: A cloud computing case study. IJCSDF 1: 265-279.
11. Jouini M, Rabai LBA (2016) Comparative study of information security risk assessment models for cloud computing systems. Procedia Computer Science 83: 1084 – 1089.
12. Guttman B, Roback E(1995) An introduction to computer security: The NIST handbook. Gaithersburg Maryland.
13. Hale ML, Gamble R(2012) Sec Agreement: Advancing security risk calculations in cloud services. IEEE International Conference on Bio-Medical Engineering and Informatics Honolulu.
14. Emam AHM (2013) Additional authentication and authorization using registered email-id for cloud computing. IJSCE 3: 110-113.
15. Aldossary S, Allen W (2016) Data security, privacy, availability and integrity in cloud computing: issues and current solutions. IJACSA 7: 489-498.
16. Ben Aissa A, Abercrombie RK, Sheldon FT, Mili A (2010) Quantifying security threats and their potential impact: a case study. Innovation in systems and software engineering. Springer-Verlag, New York. pp: 269–281.
17. Rabai LBA, Jouini M, Aissa B, Mili A(2013) A cybersecurity model in cloud computing environments. Journal of King Saud University Computer and Information Sciences 25: 63-75.
18. Jouini M, Rabai LBA (2014) A security risk management metric for cloud computing systems. IJOCI 4: 1-21.
19. Jouini M, Rabai LBA (2014) Surveying and analyzing security problems in cloud computing environments. 10th International Conference on Computational Intelligence and Security Kunming China.
20. Jouini M, Ben Arfa Rabai LBA (2015) Mean failure cost extension model towards a security threats assessment: A cloud computing case study. JCP 10: 184-194.
21. Jouini M, Rabai LBA, Aissa AB (2014) Classification of security threats in information systems. Procedia Computer Science 32: 489-496.
22. Jouini M, Ben Arfa Rabai LBA, Khedri RA (2015) Multidimensional approach towards a quantitative assessment of security threats. Procedia Computer Science 1: 507-514.
23. Chonka A, XiangY, Zhou W, Bonti A (2011) Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications 34: 1097-1107.