Journal of Green Engineering (JGE)

Volume-10, Issue-3, March 2020

Simple Additive Weight-Based Enhanced Hybrid Fuzzy Analytic Hierarchy Process for Detecting Cloud Clients Authority through Computing Energy

[1,*] S.Mercy, [2]R.Nagaraja[2], [3]M.Jaiganesh

[1]*Research Scholar,Department of Information Science and Engineering, Bangalore Institute of Technology, Bangalore, Karnataka, India.*
E-mail:mercy.isaac.abraham@gmail.com
[2]*Professor, Department of Information Science and Engineering,Bangalore Institute of Technology, Bangalore, Karnataka, India. E-mail:prof.rnagaraja@yahoo.com*
[3]*Associate Professor,Department of Computer Science and Engineering,CVR College of Engineering College, Hyderabad, Telangana, India.*
E-mail:jaidevlingam@gmail.com.

Abstract

The cloud clients authority is considered as an indispensable necessity since trusted attacker in a cloud computing environment possesses maximum probability of exploiting the resource energies. Hence, the estimation of cloud consumer legitimacy is essential for preventing the hurdle that emerges during the process of delivering reliable services to genuine cloud consumers. In this paper, a Simple Additive Weight-based Enhanced Hybrid Fuzzy Analytic Hierarchy Process (SAW-EHFAHP) is proposed for detecting Clients authority through computing energy in Cloud. This proposed SAW-EHFAHP continuously supervises the authority of cloud clients and lines them using diverse scales by creating a judgment matrix support on predictable authority index of cloud clients. The predominance of the proposed SAW-EHFAHP is analyze and compared with the baseline FAHP, ART and AHP schemes using Resource level computing energies: CPU utilization, bandwidth consumption, RAM usage and Disk memory and

Journal of Green Engineering, Vol. 10_3,663-683.

examined Accuracy, Specificity, Sensitivityusage under different potential loads. The simulation results also confirm that the proposed SAW-EHFAHP is proved to be improved in terms of accuracy and specificity by 23% and 21% compared to the baseline FAHP, ART and AHP schemes Further, the statistical analysis of the proposed SAW-EHFAHP investigated using ANOVA is confirmed to be superior contrasted with the current methodologies of the literature.

Keywords: Cloud computing, Cloud Client authority, Fuzzy analytical hierarchy process, Simple Additive method, Hybrid technique.

1 Introduction

The core benefits of the cloud computing domain focus on the possibility of facilitating the effective sharing of resources among the cloud users based on an on-demand basis [1]. The cloud service providers in the cloud environment are also potential in ensuring the significant services to their indispensable consumers with improved scalability[2].The cloud service providers along with their consumers establish novel data centers that blossoms the options of provisioning cloud applications independent of locations in order to reduce the probability of redundancy and enhances the rate of reliability [3]. The cloud users need to ensure that the data received with the services and applications from the cloud servers need to be highly secure. The Fuzzy Adaptive Resonance Theory (ART) system utilizes the info factors, for example, (memory, CPU and disk space) for each virtual customer and follows a solo learning technique to prepare and test the virtual customers. With this quick learning calculation, the virtual customers are characterized into four classes, for example, secure, powerless, changed, and oddity dependent on the carefulness limit. Littler the carefulness edge, higher classes are gotten. The customers who expend assets from others are followed out, and the classes of virtual customers are attained [4].The business and persons support cloud applications and thus service supplier vary in their application properties and service clients oscillate into their necessities [5]. The various actors who can conceivably take part in a cloud computing environment are Cloud Consumer who is an individual or organization that acts as a dominant partner in cloud computing services and avail services for cloud service providers [6]. Similarly, the Cloud Service Provider is an organization responsible for delivering services to individuals or other organizations [7]. Cloud Messenger acts a mediator for establishing connectivity between cloud clients and cloud service suppliers through networking. Likewise, the cloud Agent is an organization that acts as an liaison between cloud consumers and cloud providers toward discuss the use,

performance, and delivery of cloud services [8]. Finally, the cloud assessor is a third party that audits cloud services efficiency and performance to validate the agreement. In addition, the Service Level Objectives comprise a negotiated document that outlines a means of measuring the performance of the Service [9-10].

At this juncture, cloud consumer legitimacy refers to the evidence-based trust quantified for each of the user interacting with the cloud computing environment [11]. In this proposed scheme, cumulative cloud consumer legitimacy is used as it is potent in estimating the mean or average trust of the consumer over a period of time. The individual cloud consumer legitimacy is not used, since its value at each instant of time may be uncertain and vary depending on the context in which the consumer is interacting with the cloud environment [12,13 and 14].

In this paper, the proposed SAW-EHFAHP scheme utilizes the benefits of the Fuzzy AHP with Simple Additive Weight approach for preventing ambiguity that hurdles the decision related to the legitimacy of the cloud consumers to the cloud computing environment. The incorporated fuzzy AHP in SAW-EHFAHP scheme is a logical method that evaluates the various alternatives and enables evaluation based on the merits of fuzzy set theory. The main objective of the proposed SAW-EHFAHP scheme concentrates on the ranking the overall choicesthatplayan anchor role in the process of useful decision making for selecting the optimal method.

The major contributions of the paper are presented as follows.

i) The proposed SAW-EHFAHP scheme includes the advantages of Fuzzy AHP with Simple Additive Weight approach for effective classification of cloud client authority through computing energy in the cloud environment.

ii) The proposed SAW-EHFAHP scheme incorporated the benefits of dynamic and updating fuzzy rules for categorizing the authority of the clients based on cumulative consumer legitimacy index computation.

iii) The proposed SAW-EHFAHP scheme is potent enough in investigating the various minor and major resource based computing energy factors that contribute towards effective client trust categorization process.

iv) It is also reliable in estimating cumulative consumer legitimacy index with different aspects based on the previous behavior of clients attributed in the cloud background.

The rest of the paper is organized as follows. In Section 2, the predominant existing works of the literature that focuses on the determination of cloud legitimacy are discussed with their pros and cons. Section 3 highlights the comprehensive architecture of the system model used in the implementation of the proposed SAW-EHFAHP scheme. Section 4 presents the step by step process involved in the deployment of the

proposed SAW-EHFAHP scheme attributed towards the estimation of cloud consumer legitimacy. Section 5 depicts the illustration of the proposed SAW-EHFAHP scheme. Section 6reveals the predominant performance of the proposed SAW-EHFAHP scheme based on simulation and statistical investigation facilitated using one way ANOVA and Tukey post-hoc multiple comparison test. Section 7 concludes the paper with major contributions and future scope of implementation and evaluation.

2 Related Works

G. Praveen Babu, B. SushmaRao proposed a different approach for providing security to the data in the cloud by using deception technique. It monitors the different user's search behavior to analyze their search patterns[15]. Using these different patterns detect abnormal data access patterns. Once illegal data access is identified and verified by answering security question, it launches disinformation attack and ensures to minimize data theft and misuse of user's real data [16].

Then, Talal et al. [17] proposed the possible category of cloud service models and comprehensive options of research prototypes that potentially supports the degree of maximum trust management when reliable services in the cloud computing scenario is established. This proposed scheme utilizes a trust assessment which is capable of resolving huge amount of queries generated from trust assessment[18]. This scheme also used a trust comprehensive distributive layer that transmits the evaluated assessment value based on the result distributor module used for communication[19]. Wang et al.[20] contributed a novel scheme that the cloud computing scheme is capable of migrating the databases and application software to the potentially enormous servers that may or may not be reliable. The authors also contributed an influential and adjustable approach that uses two significant features that enables the option of cation over the data user in the cloud environment.

3 Proposed System Model

SAW-EHFAHP is a novel method to provide for public assessment based forecast of client's authority and rating. In particular, the assessor is used in the proposed scheme for determining computing facility utilization of clients from CSP and to react to the CSP through the client's authority facts and their quantification. The professional data review services are done by trusted third party common appraiser. Client's authority and quantification factors: Cloud services are pertained by many factors based on computing

cost, data transfer rate and memory usage. By the bring up points, this method confines the subsequent parameters for attention [21].

- **Computing Probability :**The probability of computing and completing the task within the allocated time limit and resource bound. Usually, the regular consumer will satisfy the time and resource energy consumptions and achieve high probability and other, hand abnormal consumer to over lead the same constraints. These activities are monitored by public assessor to compute completion probability of each consumer.
- **Overrun CSP:**It is able to overshoot the consumer services by providing the required energy resource and type of service. The cloud service is varied like Saas, Paas and Iaas.
- **Vigilance cloud service utilization:**In case of conflicts between providers and consumers, the affected party has to be compensated for repair. If the provider identifies the particular consumer as illegitimate, that consumers is responsible for the issue and has to compensate for its illegitimacy. A similar case holds, when the consumer proves that a specific provider does not offer services with guaranteed energies.

In this paper, a novel privacy preserving mechanism is proposed for supporting public auditing based on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. The ring signature used in the proposed scheme is the first linkable ring signature with unconditional anonymity and forward-secure key update mechanism. In this context, the ring is exploited based on the utilization of a bilinear pairing or multi-linear map that plays an anchor role in improving its strength with multiple increase in epochs or time periods.

3.1 The Proposed Hybrid Simple Additive Weight-based Enhanced Hybrid Fuzzy Analytic Hierarchy Process for Detecting Energy of Consumers Legitimacy

The proposed model utilizes a Simple Additive Weight-based Enhanced Hybrid Fuzzy Analytic Hierarchy Process for detecting Clients authority in Cloud Computing. This proposed (SAW-EHFAHP) derives the benefits of simple additive weighting process for ranking the consumers in order to estimate their legitimacy in a cloud computing environment. This proposed scheme is initiated over the shared data that are stored in the cloud during the process of public auditing. In specific, the ring signatures are exploited for

verifying the metadata that is essential for facilitating the correctness of the audit data that are shared in the cloud computing environment.

In this section, the detailed step by step process of the incorporated Fuzzy AHP process is discussed with an illustration. In the proposed SAW-EHFAHP scheme, five potential steps are incorporated for estimating the degree of consumer legitimacy under cloud computing. In the first step, the major constraints, minor constraints and sub-minor constraints that need to ensured for determining the legitimacy of the consumers are identified. In the second step, the weights of each each level constraint are computed using the method of the Fuzzy mapping function. Then the weights are also calculated based on the method of pairwise matrix in the third step, Further, the priority of each constraint in the global level is computed in the fourth step. Finally, the Comprehensive weight of the constraints is calculated based on the product of comprehensive weight and influential factor-based weights computed in the fourth and the second step. In the final step, ranking is also facilitated in order to adjust the crucial minor parameters that attribute towards decision making.

If suppose, the degree of extension attributed by each criterion over the other influential criterion at different levels of fuzzy AHP is ($E_{ol}^{1}, E_{ol}^{2}, ..., E_{ol}^{k}$) then the quantified degree of fuzzy synthetic value ($V_{FSE(l)}$) based on each criterion 'l' is estimated based on Equation (1)

$$V_{FSE(i)} = \sum_{j=1}^{n} E_{ol}^{j} \otimes [\sum_{l=1}^{k} \sum_{j=1}^{n} E_{j}^{l}]^{-1} \quad (1)$$

Where the value of $\sum_{j=1}^{n} E_{ol}^{j}$ is computed based on the method of the Fuzzy mapping function which depends of E_{ol}^{j} and E_{ol}^{k} that corresponds to the triangular fuzzy member under $1 \leq j \leq 3$ (since there are three levels in the considered fuzzy AHP) and degree of extent quantification of 'l^{th}' criterion towards the k^{th} goal.

Further, the fuzzy addition is made possible by satisfying the condition which is described using Equation (2)

$$\sum_{j=1}^{n} E_{ol}^{j} = (\sum_{j=1}^{n} e_{1j}, \sum_{j=1}^{n} e_{2j}, \sum_{j=1}^{n} e_{3j}) \quad (2)$$

Furthermore, the value of $\sum_{i=1}^{k}\sum_{j=1}^{n} E_{oi}^{j}$ is calculated by facilitating the process of fuzzy addition over $\sum_{j=1}^{n} E_{ol}^{j}$ such that the condition defined in Equation (3) and (4) is satisfied

$$\sum_{j=1}^{n}\sum_{l=1}^{k} E_{l}^{j} = (\sum_{j=1}^{n} e_{1j}, \sum_{j=1}^{n} e_{2j}, \sum_{j=1}^{n} e_{3j}) \tag{3}$$

$$[\sum_{j=1}^{n}\sum_{l=1}^{k} E_{l}^{j}]^{-1} = (\frac{1}{\sum_{j=1}^{n} e_{1j}}, \frac{1}{\sum_{j=1}^{n} e_{2j}}, \frac{1}{\sum_{j=1}^{n} e_{3j}}) \tag{4}$$

Then the degree of alternatives of $E_1 = (e_{11}, e_{12}, e_{13}) \geq E_2 = (e_{21}, e_{22}, e_{23})$ is derived based on the condition portrayed in Equation (5)

$$V_k(E_1 \geq E_2) = \underset{a>b}{Sup}[Min(\mu E_1(a), \mu E_2(b))] \tag{5}$$

When a pair(a, b) exists based on the condition $a \geq b$ and $\mu E_1(a) = \mu E_1(b) = 1$with $V_k(E_1 \geq E_2) = 1$.

In this context, the value of convex fuzzy numbers E_1 and E_2 are determined based on Equation (6) by meeting the condition $V_k(E_1 \geq E_2) = 1$

$$V_k(E_1 \geq E_2) = hgt(E_1 \cap E_2) = \mu E_1(p_d) \tag{6}$$

Where p_d relate to the point in the ordinate that possess maximum intersection between μE_1 and μE_2 respectively. This value of p_d is computed based on Equation (7)

$$p_d = \frac{n_{11} - n_{23}}{(n_{22} - n_{23}) - (n_{12} - n_{11})} \tag{7}$$

In the context, the comparison of E_1 and E_2 necessitates the condition of $V_k(E_1 \geq E_2)$ and $V_k(E_1 \geq E_2)$ to be satisfied. In addition, the the degree of alternatives for each of the derived fuzzy number to be superior than the m^{th} convex fuzzy number is derived based on Equation(8)

$$V_k(E \geq E_1, E_2, ..., E_k) = V[(E \geq E_1) and (E \geq E_2) and (E \geq E_k) = Min V_k(E \geq E_l) \quad (8)$$

under $1 \leq l \leq n$ if $m(P_i) = Min V_k(V_{FSE(l)} \geq V_{FSE(j)})$

Then the global weighted vector of each constraint is computed based on Equation (9) by imposing the constraints defined above.

$$W_f = (m(P_1), m(P_2), ..., m(P_k))^T \quad (9)$$

Where $1 \leq P_l \leq k$

Finally, the normalized weight vectors that portray the comprehensive weight vector is represented through Equation (10)

$$N(W_f) = [W_f(P_1), W_f(P_2), ..., W_f(P_k)]^T \quad (10)$$

In addition, if the value of the comprehensive weights of parameters that pertains to the decision making towards consumer legitimacy and cloud auditing is facilitated when $N(W_f)$ is greater than the threshold defined in [22].

In the forthcoming section, the illustration of the proposed SAW-EHFAHP is discussed based on the considered factors of the computation probability, vigilance cloud service utilization and overshoot service utilization respectively.

3.2 Illustration of the Proposed SAW-EHFAHP Scheme

In this section, the illustration of the proposed SAW-EHFAHP scheme is presented based on the pairwise matrix determined based on Computation Probability(CP), Vigilance Cloud Service Utilization (VCSU) and Overshoot Service Utilization (OSU). The aforementioned CP depends on the minor factors such as bandwidth, CPU cycle, RAM and disk usage. Further, VSCU depends on the amount of bandwidth utilized, CPU cycle utilized for the past, amount of RAM and disk usage considered for accessing the resources of the cloud environment. In addition, OSU depends on excess usage on resources which are virtualized on the network.

Table 1 The pairwise matrix representation of the Computation Probability(CP) that influences Client authority

CP	F1	F2	F3	F4	Weight
F1	4,5,6	1,1,1	4.8.6,7.2	0.119,0.142,0.178	0.390
F2	1,1,1	166,2,25	4,5,6.5	142,166,2	0.008
F3	5,6,7	5.6,7,8.4	1,1,1	125,142,2	0.49
F4	5,7,8	138,166,208	153,2,25	1,1,1	0.112

From the pairwise matrix**,** global weight for each factor is computed based on the fuzzy mapping functionthrough

$$V_{k(1)} = (4+1+4.8+0.119,5+1+6+0.142,6+1+7.2+0.178) = (9.919,12.142,14.378)$$

Similarly, the values of $V_{k(2)}, V_{k(3)}$ and $V_{k(4)}$ are determined as (5.308,6.366,7.95), (11.705,14.142,16.6) and (6.291,8.366,9.455) respectively.

Then the global weight of the parameters $V_{SCE(1)}$ is computed through

$$V_{SCE(1)} = (\frac{9.919}{33.243}, \frac{12.142}{41.016}, \frac{14.378}{48.386}) = (0.2040,0.296,0.432).$$

Likewise,the value of $V_{SCE(2)}$, $V_{SCE(3)}$ and $V_{SCE(4)}$ is estimated to be (0.109,0.155,0.239), (0.242,0.344,0.499) and (0.130,0.204,0.284) respectively. Since the value of $V_{SCE(3)} > V_{SCE(1)}$, then the weights is normalized to obtain the final values of (0.390,0.008,0.490,0.112).

The weights for the factor considered for investigation in the following Tables 2 and 3 are also computed as aforementioned in the previous section.

Table 2 The pairwise matrix representation of the influences Vigilance Cloud Service Utilization (VCSU) that influences Client authority

VCSU	G1	G2	G3	Weight
G1	1,1,1	4.6,6,8.2	0.142,0.166,0.208	0.154
G2	3.6,5,6.3	0.121,0.166,0.217	1,1,1	0.290
G3	4.8,6,7.2	1,1,1	0.158,0.2,0.24	0.356

Table 3 The pairwise matrix representation of the Overshoot Service Utilization (OSU) that influences Client authority

OSU	H1	H2	H3	Weight
H1	6.5,8,9	0.135,0.166,0.181	1,1,1	0.56
H2	1,1,1	3,4,5	0.111,0.125,0.153	0.074
H3	1,1,1	5.5,6,7.4	0.2,0.25,0.33	0.356

Further, the global weight of this investigation of the proposed SAW-EHFAHP is computed based on Table 4.

Table 4 The gloabal weight representation of the Overshoot Service Utilization (OSU) that influences Client authority

	CP	VCSU	OSU	Weight
CP	1,1,1	4.5,5,6	0.142,0.166,0.2	0.264
VCSU	6.4,8,9	0.125,0.142,0.161	4.5, 5,6	0.127
OSU	5,6,7	0.138,0166,0.127	3,4,5	0.434

Finally, the overall comprehensive weight calculation is computed and depicted in Table 5.

Table 5 The overall comprehensive weight representation of the Overshoot Service Utilization (OSU) that influences Client authority

Factors	Global weight	Minor parameters	Weight	Comprehensive Weight
CP	0.264	F1	0.390	0.10686
		F2	0.008	0.002192
		F3	0.49	0.13426
		F4	0.112	0.030688
VCSU	0.127	H1	0.56	0.0224
		H2	0.074	0.15450
		H3	0.356	0.15363
OSU	0.434	G1	0.264	0.08801
		G2	0.127	0.0146
		G3	0.434	0.0127

From this illustration, it is proved that vigilance cloud service utilization is determined to be influential in this context compared to the computation probability and overshoot service utilization responsible for justifying the cloud consumer legitimacy.

4 Results and Discussions

The simulation experiments of the proposed proposed SAW-EHFAHP scheme is conducted using the CloudSim simulator version 4 on a physical computer with a Core-i7 2700 CPU,and 16 GB of DDR3 RAM. The CloudSim is considered for simulation and modeling, since they are significant in facilitating the generic and extensible frameworks which are highly necessitated by the cloud computing infrastructures and services. The CloudSim is also predominant in the simulation, monolithic modeling and recent cloud computing infrastructure level testing with application services. Hence, CloudSim is considered as the optimal chioce for simulating the proposed SAW-EHFAHP scheme. In this investigation, the predominance of the proposed SAW-EHFAHP is analyzed and compared with the baseline FAHP, ART and AHP schemes using Accuracy, Specificity, Sensitivity,

CPU utilization, bandwidth consumption and RAM usage under different potential loads. Further, the proposed SAW-EHFAHP approach is compared with the benchmarked FAHP, ART and AHP schemes based on one-way ANOVA and Tukey post-hoc multiple comparison test of statistical investigation.

In the initial part of the investigation, the proposedSAW-EHFAHP scheme is compared with the benchmarked FAHP, ART and AHP schemes using accuracy with varying amount of load introduced in the cloud environment. Figure 1 demonstrates the simulation results of the proposed SAW-EHFAHP approach over FAHP, ART and AHP schemes evaluated based on accuracy percentage. The accuracy of the proposed SAW-EHFAHP approach is realized to be 8%-12% superior to FAHP, 14%-17% better to ART and 19%-23% predominant to AHP schemes. This improvement in the proposed SAW-EHFAHP approach is mainly due to the incorporation of the simple aggregate weighted used in the Fuzzy AHP process used for estimating cloud consumer legitimacy.

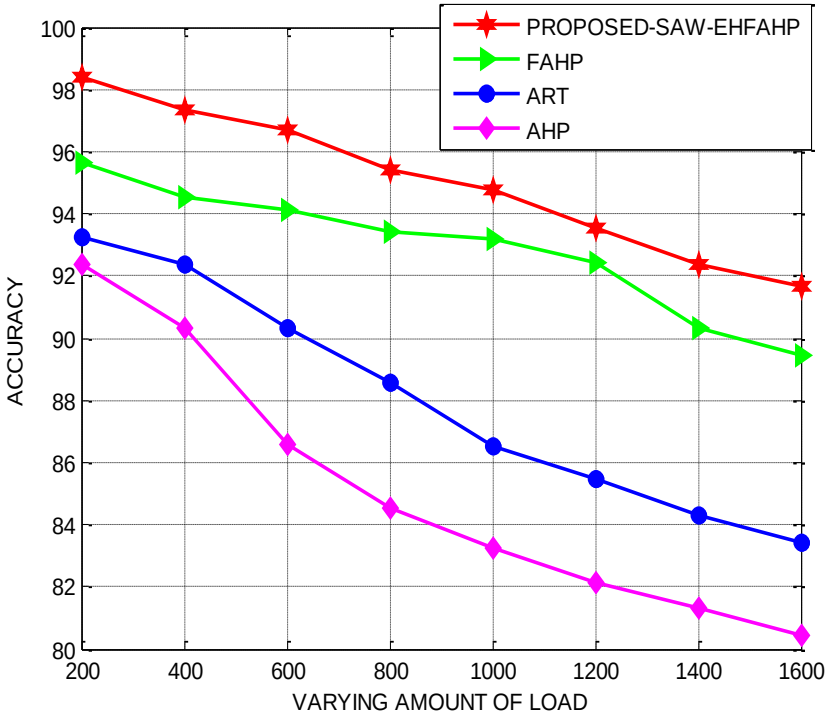


Figure 1 SAW-EHFAHP-accuracy percentage based on varying load

Further, Table 6 depicts the statistical results of the proposed SAW-EHFAHP approach over the compared FAHP, ART and AHP schemes in terms of accuracy using Tukey post-hoc multiple comparison test of statistical investigation. The results demonstrated confirmed that the proposed SAW-EHFAHP approach in an average is 13%, superior in its significance over the compared FAHP, ART and AHP schemes used for comparison. This Tukey post-hoc multiple comparison test clearly portrays that the proposed SAW-EHFAHP is phenomenal in the accurate detection of consumer legitimacy indices independent to the amount of load introduced in the network. .

Figure 2 highlights the simulation results of the proposed SAW-EHFAHP approach over FAHP, ART and AHP schemes based on sensitivity. The sensitivity of the proposed SAW-EHFAHP approach is determined to be 11%-14% superior to FAHP, 18%-20% better to ART and 22%-26% predominant to AHP schemes. This improvement in the proposed SAW-EHFAHP approach is mainly due to the incorporation of the multiple dimension-based comprehensive weights determined and used in the Fuzzy AHP process used for estimating cloud consumer legitimacy. Further, the proposed SAW-EHFAHP scheme is determined to be a potent in accurate estimation of cloud consumer legitimacy index as it alternates between the multiple metadata that are exploited for quantifying the evident trust of the cloud users.

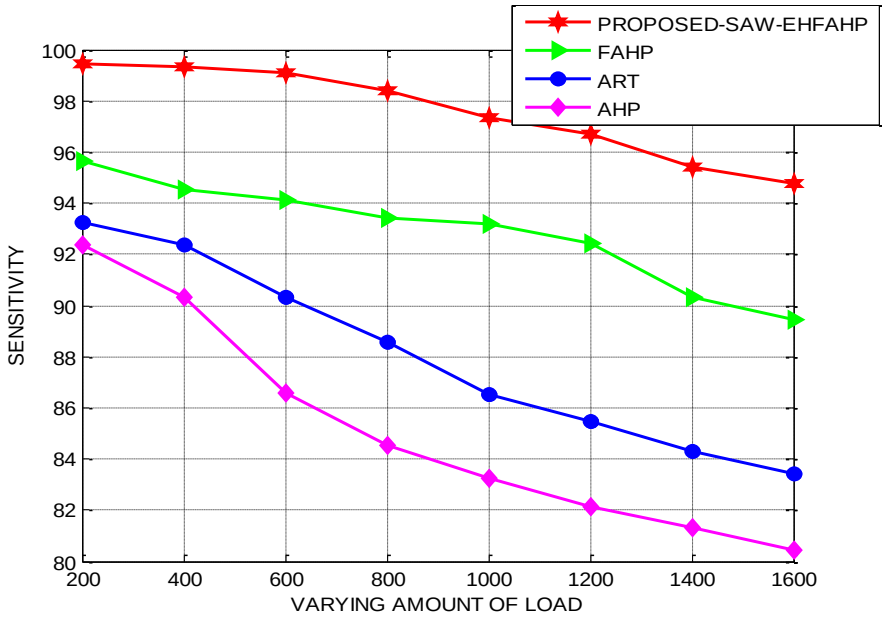


Figure 2 SAW-EHFAHP-sensitivity based on varying load

The results that the proposed SAW-EHFAHP approach in an average 23% excellent in its significance over the FAHP, ART and AHP schemes used for comparison. Further, Figure 3 highlights the simulation results of the proposed SAW-EHFAHP approach over FAHP, ART and AHP schemes based on specificity. The specificity of the proposed SAW-EHFAHP approach is determined to be 7%-10% superior to FAHP, 13%-19% better to ART and 21%-24% predominant to AHP schemes. This enhancement of the specificity in the proposed SAW-EHFAHP approach is mainly due to the incorporation of the multi-perspective number of different level of factors that form the vital part in identification of the cloud consumer legitimacy.

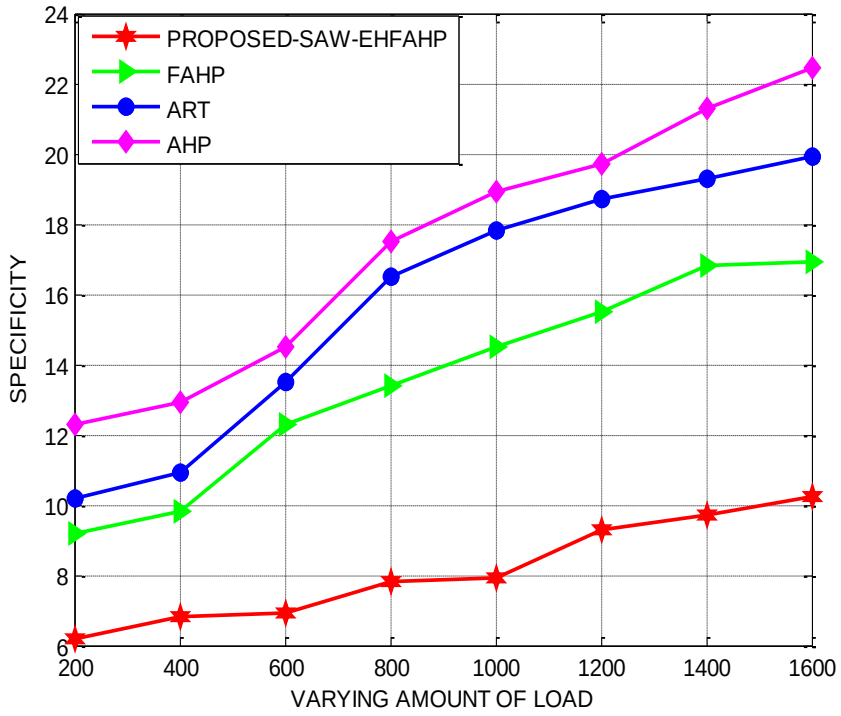


Figure 3 SAW-EHFAHP-Specificity based on varying load

The results that the proposed SAW-EHFAHP approach in an average 16% superior in its performance over the existing FAHP, ART and AHP schemes used for comparison. Figure 4 highlights the simulation results of the proposed SAW-EHFAHP approach over FAHP, ART and AHP schemes based on CPU Utilization.The CPU Utilization of the proposed SAW-

EHFAHP approach is determined to be 9%-13% superior to FAHP, 17%-19% better to ART and 23%-27% predominant to AHP schemes. This enhancement of the CPU Utilization in the proposed SAW-EHFAHP approach is mainly due to the incorporation of the multiple number of weights used in the estimation of the cloud consumer legitimacy.

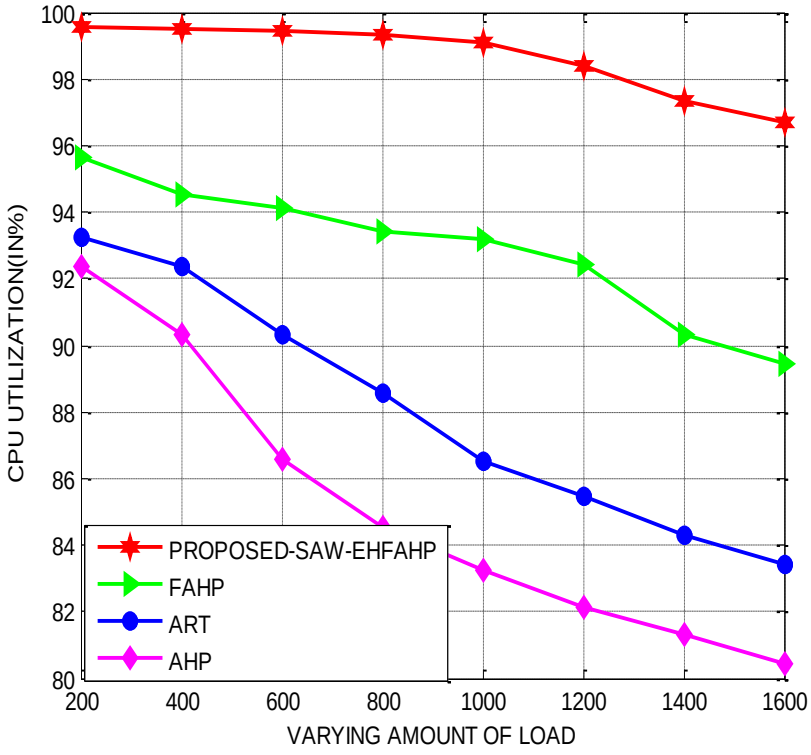


Figure 4 SAW-EHFAHP-CPU Utilization based on varying load

The results that the proposed SAW-EHFAHP approach in an average 14% superior in its performance over the existing FAHP, ART and AHP schemes used for comparison. Figure 5 highlights the simulation results of the proposed SAW-EHFAHP approach over FAHP, ART and AHP schemes based on Bandwidth Consumption. The Bandwidth Consumptionof the

proposed SAW-EHFAHP approach is determined to be 11%-15% superior to FAHP, 19%-23% better to ART and 26%-29% predominant to AHP schemes.

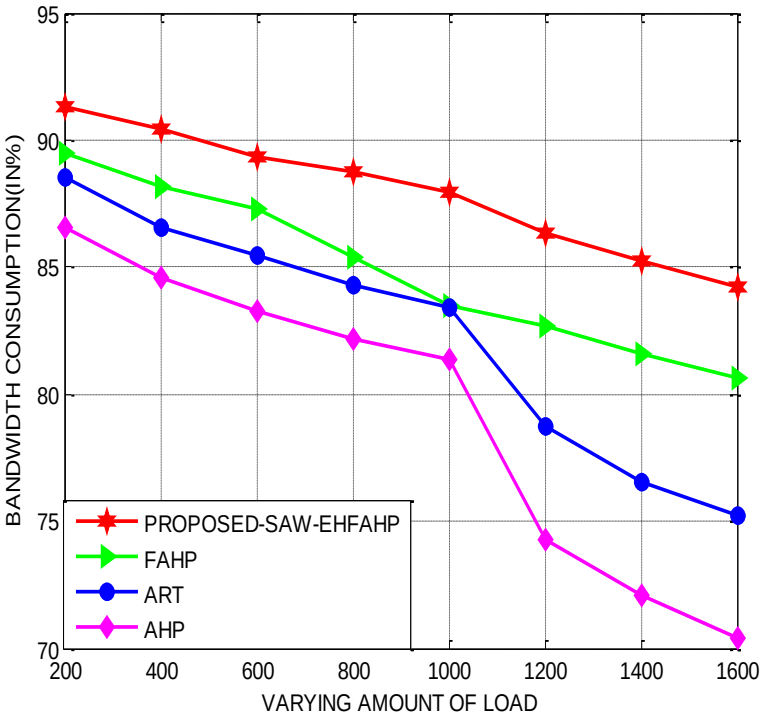


Figure 5 SAW-EHFAHP-CPU Utilization based on varying load

The results that the proposed SAW-EHFAHP approach in an average 17% superior in its performance over the existing FAHP, ART and AHP schemes used for comparison. Figure 6 highlights the simulation results of the proposed SAW-EHFAHP approach over FAHP, ART and AHP schemes based on RAM usage.The RAM usageof the proposed SAW-EHFAHP approach is determined to be 11%-14% superior to FAHP, 16%-18% better to ART and 21%-24% predominant to AHP schemes.

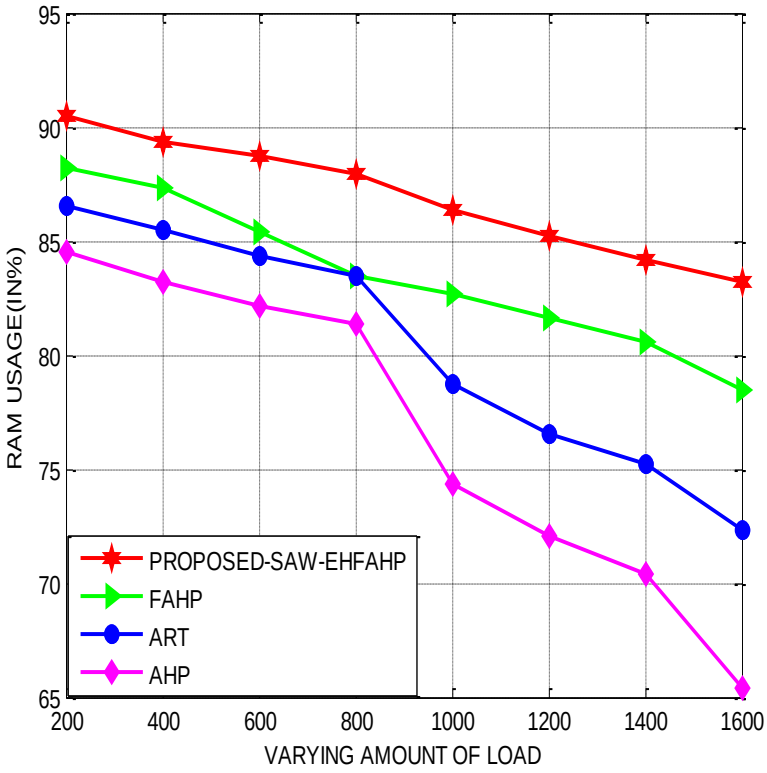


Figure 6 SAW-EHFAHP- RAM usage based on varying load

The results that the proposed SAW-EHFAHP approach in an average 12% superior in its performance over the existing FAHP, ART and AHP schemes used for comparison.

5 Conclusion

The proposed SAW-EHFAHP schemeis presented as an attempt for preventing the cloud attackers to the development of cloud computing based on the estimation of client authority through three factors of influence. The degree of utilization of CPU time, bandwidth, RAM and disk memory, cloud client authorities are evaluated such that that the genuine cloud cleints are

prioritized by the establishment of ranking mechanism. The Statistical investigation of the proposed SAW-EHFAHP scheme enabled with one-way ANOVA and Tukey post-hoc tests prove it predominance over the compared FAHP, AHP and ART schemes. In the future scope of this work, it is also planned to formulate an exponential average weighting-based AHP process for testing the cloud clients authority for facilitating reliable sharing of resources.

References

[1] P.J.M. van Laarhoven, W.Pedrycz, "A fuzzy extension of Saaty's priority theory", Journal Fuzzy Sets and Systems. vol. 11, no. 1-3, pp.199-227, 1983.

[2] Qian Zhou, Jiong Yu, and Feiran Yu, "A Trust Based Defensive System Model for Cloud Computing", Lecture Notes in Computer Science. . vol. 6985, pp. 146-159, 2011.

[3] Xiaonian Wu, Runlian Zhang, Bing Zeng, Shengyuan Zhou, "A trust evaluation model for cloud computing", Proc. Computer Science, vol.17, pp.1170-1177, 2013.

[4] P. S. Pawar, M. Rajarajan, S. Nair, T. Dimitriakos, A. Zisman, "Trust Model for Optimized Cloud Services", Proc. IFIP, vol. 374, pp 97-112, 2012.

[5] Fahad F. Alruwaili, T. Aaron Gulliver, "Trusted CCIPS: A Trust Security Model for Cloud Services Based on a Collaborative Intrusion Detection and Prevention Framework", International Journal of Latest trends in computing, vol. 5 no.1, pp. 162-171, 2014.

[6] WenAn Tan, Yong Sun, Ling Xia Li, Guang Zhen Lu, Tong Wang, "A Trust Service Oriented Scheduling Model for Workflow Applications in Cloud Computing", IEEE Systems Journal,vol.8 no.3, pp. 868-878, 2014.

[7] Hyukho Kim, Hana Lee, Woongsup Kim, Yangwoo Kim, "A Trust Evaluation Model for QoS Guarantee in Cloud Systems", International Journal of Grid and Distributed Computing, vol.3 no.1, pp 1-10, 2010.

[8] Shouxin Wang, Li Zhang, Na Ma, Shuai Wang, "An Evaluation Approach of Subjective Trust Based on Cloud Model", Journal of Software Engineering and Applications,vol.1 no.1 pp. 44-52, 2008.

[9] Ries S, Habib SM, Muhlhauser M, Varadharajan V. "Certain logic: A logic for modeling trust and uncertainty", Lecture Notes in Computer Science, vol. 6740, no.1, pp.254-261, 2011.

[10]R. Butkiene, G. Vilutis, I. Lagzdinyte-Budnike, D. Sandonavicius, K. Paulikas, "The QoGS Method Application for Selection of Computing Resources in Intercloud", Elektronika Ir Elektrotechnika, vol.19, no. 7, pp 98-103, 2013.

[11]G. Zhang, M. De Leenheer, A. Morea, B. Mukherjee, "A survey on OFDM-based elastic core optical networking", IEEE Commun. Surv. Tutorials,vol.15 no.1 pp. 65-87, 2013.

[12]J. Sole-Pareta, S. Subramaniam, D. Careglio, S. Spadaro, "Cross-layer approaches for planning and operating impairment-aware optical networks", Proc. IEEE, vol. 100, no.5, pp.1118-1129, 2012.

[13]Lombardi, F, Pietro, RD, "Secure virtualization for Cloud computing", Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1113 – 1122, 2011.

[14]Xiaonian Wu, Runlian Zhang, Bing Zeng, Shengyuan Zhou, "A trust evaluation model for cloud computing in Information Technology and Quantitative Management, Procedia computer science, vol.17, no. 1, pp. 170-1177, 2013.

[15]G. Praveen Babu, B. SushmaRao, "Secure Data Access control in Cloud Environment" International Journal of Computer Science and Information Technologies, vol.5, no. 2, pp. 1734-1737, 2013.

[16]Wang, L, Zhan, J, Shi, W, Liang, Y, Yuan, L. "In Cloud, do MTC or HTC Service Providers Benefit from the Economies of Scale?", Proc MTAGS, pp. 7-11, 2009.

[17]Sathya Vishnu and S.Selvakumar. "Verification of Trust Worthiness of the User Data in Green Cloud Environment using Data Auditing Method". Journal of Green Engineering, vol.10, no. 1, pp. 118-130, 2020.

[18]Talal H Noon, Quan Z Sheng, SheraliZeadally, JianYu,"Trust management of services in cloud environments: Obstacles and solutions", ACM Computing Surveys (CSUR), vol. 46, Issue 1, 2013.

[19]Wenjuan Fan, Harry Perros, "A novel trust management framework for multi-cloud environments based on trust service providers" Knowledge-Based Systems, vol.70, no. 11, pp. 392-406, 2014.

[20]WenAn Tan, Yong Sun, Ling Xia Li, Guang Zhen Lu, Tong Wang, "A Trust Service Oriented Scheduling Model for Workflow Applications in Cloud Computing", IEEE Systems Journal,vol.8 no.3, pp. 868-878, 2014.

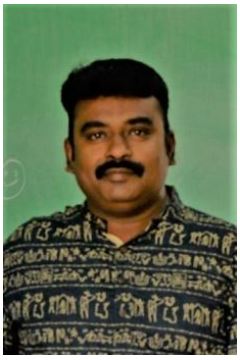
[21]Jaiganesh M, Sivakami R, Vincent Antony Kumar A, "Secure isolation of cloud consumers legitimacy using fuzzy analytical hierarchy process (AHP)", The Journal of Analysis, vol.27, no. 2, pp. 311-326, 2019.

[22]RizwanaShaikh, M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing" Procedia computer science, vol.45, no. 3, pp. 380-389, 2015.

Biographies

S.Mercy, is a Ph.D Scholar with VTU Belagavi. She received her B.E degree in Electrical and Electronics Engineering from Manonmaniam Sundaranar University, Tirunelveli and M.E degree in Computer Science and Engineering from Anna University, Chennai. She has more than fourteen years of teaching experience and one year of industrial experience. She has published one paper each in an International Journal and Conference. She is working as Assistant Professor in Information science and Engineering Department in Bangalore Institute Of Technology, Bangalore. She is a member of IE and ISTE. Her research interests include Cloud Computing and Security.

Dr R Nagaraja, working as professor, PG and Research Coordinator has 30 years of teaching undergraduate and post graduate students. He has published around 25 papers in national and international journals. He is IT consultant and trainer for many IT company employees. He is also academic consultant for BITS, Pilani programs. He has established many IGNOU study centres for computer programs. He is contributing to academic activities as LIC, BOS and BOE member in VTU and other autonomous engineering colleges in Karnataka. He is guiding many PG and PhD scholars in various domains like cloud computing, pervasive computing, wireless networks, machine learning, deep learning, etc. His area of interest Pervasive Middleware, Computer Networks, Component Based Technology, Cloud Computing, Mobile Cloud Computing, Opportunistic Networks, Algorithms, Graph Database, Big Data Analysis, Machine Learning.



Dr.M.Jaiganesh is working as an Associate professor in CVR College of Engineering Hyderabad. He completed his PhD from Anna University, Chennai during the year 2014. He has 15 years of teaching for undergraduate, post graduate students and Research scholars. He has published around 15 papers in national and international journals. He has published books in the area of embedded systems and Pervasive computing. He is guiding many PG and PhD scholars in various domains like cloud computing, pervasive computing, wireless networks, machine learning, deep learning, etc. He has visited countries of Singapore and Malaysia. His area of interest Mobile Adhoc Networks, Cloud computing, Big data analytics.