IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 7, July 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

ANFIS Based Multi-Tenant Cloud Management by TrustEvaluation Technique

Surendranath Singh.B.G., Dr. Sunil Phulre

Ph.D. Scholar, Dept. of CSE, LNCT University, Bhopal MP, India

Dept. of CSE, LNCT University, Bhopal MP, India

ABSTRACT: Importance of digital world increases after pandemic, as most of service get online and need services. Cloud infrastructure requirement for management of various services indirectly depends on virtual machine acting as tenants. Chance of attack in cloud infrastructure is high hence monitoring of tenants' activity to identify suspicious machine is done by this work. Proposed model has created a virtual window to evaluate Leicht Holme Newman trust value of each tenant present in cloud. As per Leicht Holme Newman value trained ANFIS mathematical model evaluate the behavior of tenants in virtual window to identify malicious nodes. Experiment was done on various set of real and malicious tenants. Result shows that proposed model has increases the precision value by %, recall by % and accuracy by % as compared to other comparing models in same environmental conditions.

KEYWORDS: Cloud computing, Social trust, Machine Learning, Classification, Trust Model.

I. INTRODUCTION

With the enormous capability of resource sharing and enhanced user experience cloud computing has become one of the major research issues in the IT industries and its commercial value is gradually increasing[1,2]. But this cloud computing systems are prone to security problems. For example, in the year 2016, Cloudflare a famous security service provider has claimed that a bug which was present in its software has led to leakage of data from over 2 million websites including well-known service providers such as 1password and Uber. Also, the failure of Microsoft Azure public cloud storage has affected the clod business for nearly 8 hours. A security problem in the web services of the Amazon also leaked the personal information of nearly 200 million voters of the US. As per the report released by the Fujitsu nearly 88% customers that are using cloud services are often worried regarding the data leakage.

Trust in cloud computing has gained a lot of attention these days. Several trust models are present [3] that gives the trust factor in cloud computing. Each of this trust models are limited with certain features only. So, it is important for the organization to develop such models that solve most of the issues regarding cloud computing. People are now realizing the trust in cloud computing. Several researches are going on for the evaluation of the present trust models. For example, Kanwal et al [4] studied 12 trust models and divided it into 5 mechanisms. They evaluated seven parameters for twelve trust models and categorized them into high, medium, and low. Corradini and et al[5] studied fourteen trust models and categorized theminto3 mechanism in search for their weakness in trust. They have concluded that reliability and efficiency is the major barrier for using the services of cloud.

II. RELATED WORK

Atoosa and Mostafa in [6] given a model that finds the most suitable trust source to provide the cloud services. Time of implementation, processor speed, cost, etc. is some of the parameters that were used to calculate trust. Turn around trust of the cloud resources is evaluated through combination of trust factor and speed of its implementation. Analytical hierarchy process was used to select the most reliable trusted resources in the environment of cloud. Gokulnath and

Rhymend in [7] primary task is to identify trust resource at the boot load level. The main aim was to find trust worthiness of resources and users. The model has better efficiency then other models as it uses risk parameters and proper mapping of the users.

Udaykumar and Latha et al in [8] given a trust model which was cloud attestation protocol based. It measures the integrity of the cloud service to find the trust value. Parameters such as successful service completion, successful service initialization, etc. were determined. Different weights were calculated with the help of Analytical Hierarchy process to compute the trust value. The use of attestation protocol was the key to success as it guarantees the correctness.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

Christian et alin [9] used fuzzy set theory to depict the cloud storage service which also involves game theory approach along with usage of fuzzy interferences theory. The storage service was chosen randomly by fuzzy inferences and for truth telling service providers' gametheoretic approach was used. As distributed approach was used this approach was cost saving.

DE KOuicem ei al in[10] Given a scalable and hierarchical based trust management protocol which was block chain based together with mobility support in vast distributed IoT systems. In this protocol mobile smart object finds the trust related information of the service providers in the block chain. By this all service provider will have a global view of each service provider so that they can easily trust them without wasting much time. Also, This protocol is safe from malicious attack such as\textit{cooperative attacks}, textit{ballot-stuffing} and
\textit{bad-mouthing}.

J. Jiang et. al. in [11] provided a trust evaluation and updated mechanism specially for the wireless sensors(underwater) which was based on C4.5 decision making algorithm or TEUC. In this in the first stage trust evidence such as node based, linked based and data base are collected and these are used to train the decision tree that is C4.5. The penalty and reward factors are also given that are used to be updated on the sliding time window. P.Huang given a block chain framework for the storage of cloud data. In this all nodes collectively collected for the single third party to execute auditing and finally to record them permanently. By this the entities are saved from deceiving each other. Analysis showed that this method was effective to protect the integrity of data from malicious attack. The performance analysis also showed that this method is much more resource friendly and functional then other comparable techniques.

III. PROPOSED METHODOLOGY

Proposed Leicht Holme Newman Adaptive Neural Fuzzy Interference System (LHN-ANFIS) was detailed in this section of paper. Explanation of blocks shown in fig. 1 are detailed. Paper has used different abbreviation for the representation of variable weredetailed in table 1.

Table 1 LHN-ANFIS abbreviation list.

Abbreviation	Meaning
CC	Clock Cycle
T	Tenants
V	Virtual Packet Count
RB	Resource Belief
∧	Cock Count
NT	Number of T
TD	Trust
L	LHN Value
A	Authority
TH	HITS Trust
H	Hub

Tenants: Some organization provide machines as tenants in cloud having resource type {Bandwidth, Central Processing Unit, Memory}. Such individual machine is termed as tenantsin the cloud. Machine owner can charge cloud

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

as per its resource configuration and availability.

Virtual Cycle: Virtual packet movement is to perform for λ clock cycle. Tenants are unaware of this time period and routine of VC. In each cycle of virtual movement random source and destination tenants were select and packets were though in network. As centralized system knows about this movement to count successful and unsuccessful packet delivery. In this paper packet is a kind of task that a tenant needs to perform as per resource availability.

Resource Belief: Each tenant utilization was monitor for λ time to estimate its RB value. Tenant provide a limit of resource utilization before they submit machine to cloud. So, if resources are over utilized then cloud has to pay extra amount to the tenants. It is desiring that resource belief value should be below 1. This belief value may get higher than 1 if resources are over utilized. Over utilization is just a kind of alarm for the attack to the cloud. So, if T has r resources for cloud services and its maximum utilization limit is set up to T_M and during clock cycle duration tenant utilization is T_U, then Resource Belief value is estimate by Eq. 2.

$$R_{B,r} = \begin{cases} 1 \; T_U <= T_M \\ \frac{T_M}{T_U} \; T_U > T_M \end{cases} \quad ------> Eq1$$

$$------> Eq2$$

$$R_T = \frac{\sum_1^r R_{B,r}}{r}$$

Leicht Holme Newman: In order to estimate the trust of the proposed model as pe behavior of tenant in network Leicht Holme Newman algorithm was used. Direct trust value was estimate between nodes by Eq. 3 where successful task completion count was divided by total number of tasks between nodes. Ratio of minimum number of direct trust between nodes to the multiple of all direct value of between nodes is Leicht Holme Newman.

$$D_{i,j} = \frac{Ps_{i,j}}{Pt_{i,j}} ------> Eq3 \qquad \boldsymbol{L} = \frac{\boldsymbol{Min(D_{i,j})}}{\boldsymbol{D_i x D_j}} \text{ ---------- Eq. 4}$$

Leicht Holme Newman function value was estimate by eq. 4.

Adaptive Neural Fuzzy Interference System

In 1990 [15] ANFIS neural learning model was proposed. As this Uses concept of neural network and fuzzy logic so it terms as ANFIS. Learning of neural network was improved by use of logical operators IF Else, as this help in remembering rules in the dataset. This logical operator improves the neural learning for non-linear data as well.

Learning of malicious tenant behavior is done by Adaptive Neural Fuzzy Interference System. Features of each tenant collect to train this mode. Input training vector is set of {L, R, D). For training malicious tenants were identified by 0 and real tenants were identified by 1.

In this learning model five layers of neurons were present. In first layer membership function is identify as per the input value set. This is an fuzzification layer used in the work. As per the premise parameters membership function is select. Second neural layer used for the firing of neuron from the input, so this

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

second layer is named as rule layer. After this data is normalizeas some of values are dominating others, hence third layer was used for the normalization of model. This normalization distributes computing firing strength of neurons. Fourth layer takes normalize values and consequence parameters to defuzzied values and finally pass to the fifth and final layer [8].

Fuzzification layer in ANFIS model activation function is not a sigmoid nor a step but work apply some data processing methods to convert values into fuzzy format.

Proposed LHN-ANFIS Algorithm

Input: T // Number of Tenants

Output: ANFIS // Trained Neural Network

```
C ← Initial_Tenants(T)
Loop 1: CC
Loop 1: V
i ← Rand()
i ← Rand()
i ← Packet(i, j)
EndLoop
RB ← Resource _belief(CC)
Loop 1:T
 L[n] ← Leicht_Holme_Newman (RB)
 EndLoop
 Loop 1:n
 F[n] ← Input_Feature(L,D,RB)
 Do[n] ← Tenant_Class
 EndLoop
 NN ← Train_ANFIS(E, D)
```

Detail steps of the proposed algorithm shows that after each trust values were update and nodes which performed malicious activity in cloud are filtered and removed by trained ANFIS.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

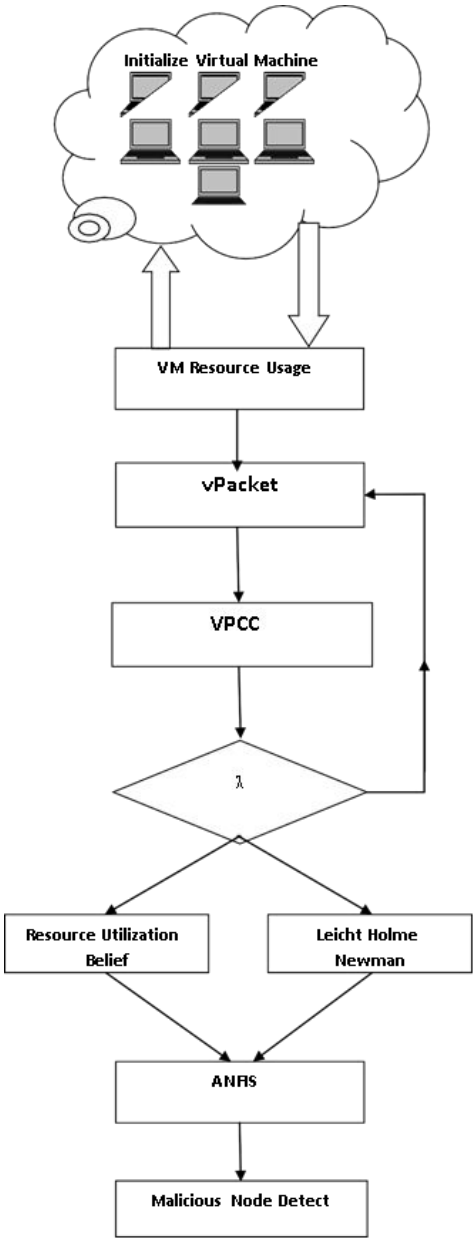

Fig.1Proposed malicious tenants' detection.

IV. EXPERIMENTS & RESULTS ANALYSIS

Implementation model was developed on MATLAB platform of 2016a version. Experimental values were compared on below parameters Eq. 5, 6, 7 and 8 [15, 16]. Under two environment first was no attack and other was DDoS attack.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

$$Precision = \frac{TP}{TP+FP}\text{-------Eq. 5}$$

$$Recall = \frac{TP}{TP+FN}\text{-------Eq. 6}$$

$$FMeasure = \frac{2*Precision*Recall}{Precision+Recall}\text{---------Eq. 7}$$

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}\text{-------Eq. 8}$$

	Compare Algorithm	
Actual	**T (Real)**	**F (Malicious)**
P (Real)	**TP**	**FP**
N (Malicious)	**TN**	**FN**

Results

In order to compare the values of proposed model SHCTM [17] with existing model TMM [18]. In this paper results are shown for different set of VM with number of malicious VM.

Table 2 Precision value-based comparison of DDoS malicious machine detection.

Experiment Setup (MachinexMalicious)	SHCTM	TMM	LHN-ANFIS
30x5	0.8667	0.5556	1
40x5	0.9	0.6364	1
40x8	0.875	0.25	1
50x10	0.8148	0.5294	1
50x0	1	1	1

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

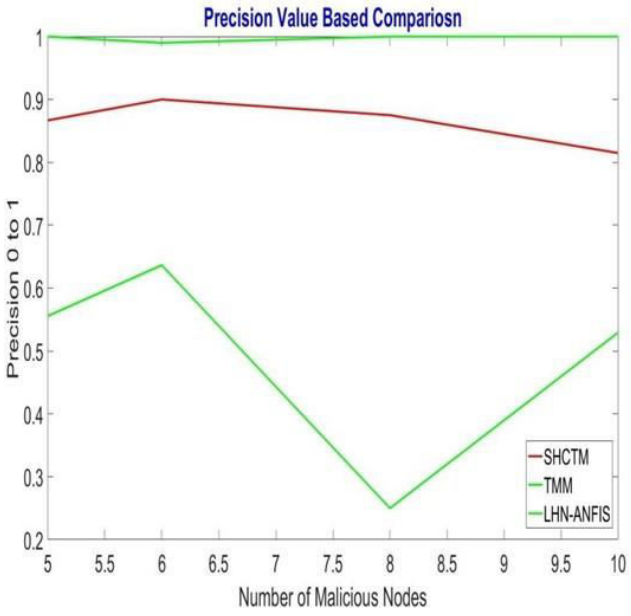

Fig. 2 Precision value-based comparison.

Table 2 and fig. 2 shows that LHN-ANFIS proposed model has drastically improved the precision value of normal node detection accuracy to 1. This improvement was achieved by learning of ANFIS model by fuzzy concepts of internal layers of the neural network. Further LHN-ANFIS improved average precision value by 10.46% as compared to SHCTM model and 40.5% as compared to TMM [18] model.

Table 3 Recall value-based comparison of DDoS malicious machine detection.

Experiment Setup (MachinexMalicious)	SHCTM	TMM	LHN-ANFIS
30x5	0.8125	0.8333	0.8333
40x5	0.875	0.875	0.875
40x8	0.7368	0.6667	0.825
50x10	0.8148	0.8182	0.8
50x0	1	1	1

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

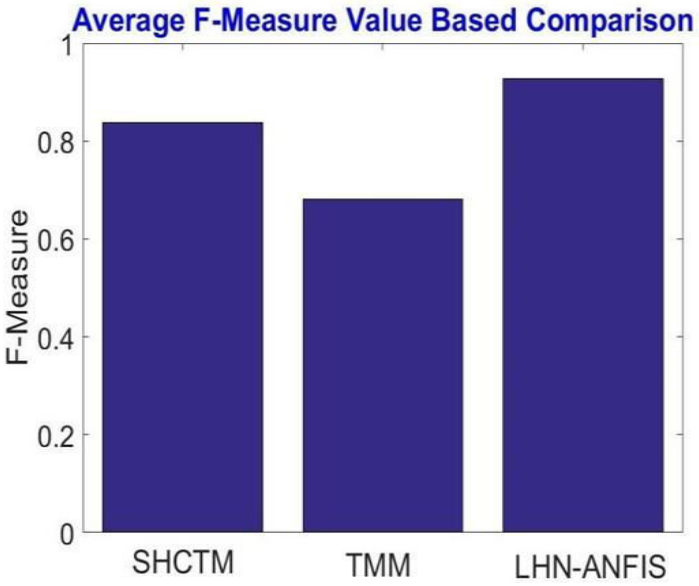

Fig. 3 Average F-measure value-based comparison.

Table 4 F-measure value-based comparison of DDoS malicious machine detection.

Experiment Setup (MachinexMalicious)	SHCTM	TMM	LHN-ANFIS
30x5	0.8387	0.667	0.9091
40x5	0.7368	0.7368	0.9333
40x8	0.8	0.3636	0.9041
50x10	0.8148	0.6429	0.889
50x0	1	1	1

Table 3, 4 and fig. 4 shows recall, F-measure parameters. It was obtained that proposed model has increases the recall value by 2.17% as compared to SHCTM and 3.23% as compared to TMM model. Similarly, f-measure by 9.6% as compared to SHCTM. Use of social trust and ANFIS model for detection of malicious node increases the work performance.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

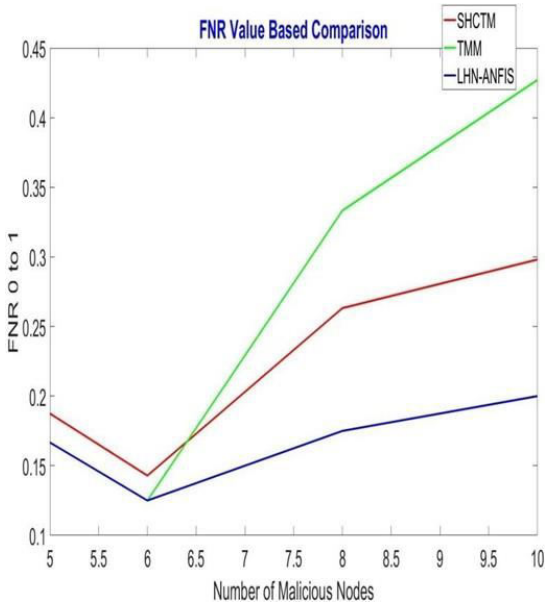

Fig. 4 FNR value-based comparison.

Table 5 FNR value-based comparison of DDoS malicious machine detection.

Experiment Setup (MachinexMalicious)	SHCTM	TMM	LHN-ANFIS
30x5	0.1875	0.1667	0.1667
40x5	0.1429	0.125	0.125
40x8	0.2632	0.3333	0.175
50x10	0.2981	0.4271	0.2
50x0	0	0	0

Table 5 and fig. 4 shows that LHN-ANFIS proposed model has drastically reduced the FNR value of malicious node detection. Use of Leicht Holme Newman function has increased the trust value efficiency that gradually increase or decrease the value as per activity of nodes. Further LHN- ANFIS reduced the average FNR value by 33.74% as compared to SHCTM model and 57.8% as compared to TMM [18] model

V. CONCLUSION

Multi-tenant cloud architecture needs two inner and outer side security. This paper has proposed a security model for inner security by use of trust evaluation technique. Leicht Holme Newman social trust method was used in the work that collectively evaluate trust of nodes as per activity they perform in a monitoring clock cycle. This trust value was used in the learning ofANFIS model. Trained ANFIs model predict the class of node (Normal/Malicious). Use of Leicht Holme Newman ANFIS for malicious node detection in the work has improved the work performance. Experiment was done on different situation of network by varying nodes normal and malicious. Result shows that proposed LHN-ANFIS has improved the recall value by 2.17% as compared to SHCTM and 3.23% as compared to TMM model. Further it was obtained that FNR of the model was also reduced by 33.74% as compared to SHCTM model. In future

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

scholar can introduce some technique that can alarmed outer attack activities.

REFERENCES

1. Xu M, Buyya R. "Brownout approach for adaptive Management of Resources and Applications in cloud computing systems". ACM Comput Surve 52(1), 2019.
2. Zhu Y, Zhang W, Chen Y, Gao H. "A novel approach to workload prediction using attention-based LSTM encoder-decoder network in cloud environment". EURASIP J Wirel Commun Net 2019.
3. K. Hwang and D. Li. "Trusted Cloud Computing with Secure Resources and Data Coloring." IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, Sept– Oct. 2010.
4. S. Horvat and R. Agrawal, "Trust in cloud computing," in SoutheastCon2015, 2015, F. Corradini, F. Angelis, F. Ippoliti and F. Marcantoni. "A Survey of Trust Management Models for Cloud Computing," in 5th International Conference on Cloud Computing and Services Science, 2015.
5. G. Atoosa, A. Mostafa A trust model based on quality of service in cloud computing environment Int. J. Database Theory Appl., 8 (5), 2015.
6. K. Gokulnath, U. Rhymend 2015 Scientific World Journal, Hindawi Publishing Corporation, Game theory-based trust model for cloud environment 2015.
7. S. Udaykumar, T. Latha Trusted computing model with attestation to assure security for software services in a cloud environment Int. J. Intell. Eng. Syst., 10, 2017
8. E. Christian, M. Ficco, F. Palmieri, A. Castiglione Smart cloud storage service selection based on fuzzy logic theory of evidence and game theory IEEE Trans. Comput., 65 (2016)
9. D. E. Kouicem, Y. Imine, A. Bouabdallah and H. Lakhlef, "A Decentralized Blockchain-Based Trust Management Protocol for the Internet of Things," in IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2020.
10. J. Jiang, X. Zhu, G. Han, M. Guizani and L. Shu, "A Dynamic Trust Evaluation and Update Mechanism Based on C4.5 Decision Tree in Underwater Wireless Sensor Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 9031-9040, Aug. 2020.
11. P. Huang, K. Fan, H. Yang, K. Zhang, H. Li and Y. Yang, "A Collaborative Auditing Blockchain for Trustworthy Data Integrity in Cloud Storage System," in IEEE Access, vol. 8, 2020.
12. E. A. Leicht, P. Holme, and M. Newman. Vertex similarity in networks. Phys. Rev. E, 73,2006.
13. Jang, Jyh-Shing R (1991). Fuzzy Modeling Using Generalized Neural Networks and Kalman Filter Algorithm (PDF). Proceedings of the 9th National Conference on Artificial Intelligence, Anaheim, CA, USA, July 14–19. 2. pp. 762–767.
14. Jang, J.-S.R. (1993). "ANFIS: adaptive-network- based fuzzy inference system". IEEE Transactions on Systems, Man and Cybernetics. 23 (3): 665–685.
15. S.Kannadhasan and R.Nagarajan, Development of an H-Shaped Antenna with FR4 for 1-10GHz Wireless Communications, Textile Research Journal, DOI: 10.1177/00405175211003167 journals.sagepub.com/home/trj, March 21, 2021, Volume 91, Issue 15-16, August 2021
16. Abraham, A. (2005), "Adaptation of Fuzzy Inference System Using Neural Learning", inNedjah, Nadia; de Macedo Mourelle, Luiza (eds.), Fuzzy Systems Engineering: Theory and Practice, Studies in Fuzziness and Soft Computing, 181, Germany: Springer Verlag.
17. Embedded is the research paper on "Multi-Tenant Cloud Environment Trust Management by Sorensen and HITS Algorithm", which got published in the following Scopus journal.
18. Omar Abdel Wahab, Jamal Bentahar, Hadi Otrok, and Azzam Mourad. "Optimal Load Distribution for the Detection of VM-based DDoS Attacks in the Cloud". IEEE Transaction, Services Computing Nov. 2020

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

BIOGRAPHY

Mr. Surendranath Singh B G has vast work experience in software industry and has worked in companies like IBM, Mindtree Limited and UST Global on different technologies. He is pursuing PhD. in Department of CSE, LNCT University, Bhopal Madhya Pradesh, India.

Papers published by the author:

1. Embedded is the research paper on "Multi-Tenant Cloud Environment Trust Management by Sorensen and HITS Algorithm", which got published in the following Scopus journal.

http://www.thedesignengineering.com/index.php/DE/artic le/view/2853

2853-Article Text-5028-1-10-2021

2. Embedded is the survey paper on "Detail Study of Cloud Infrastructure Attacks and Security Techniques", which got published in the following International journal (Issue-->Archive--> Volume-9, Issue-2, March-2021).

https://www.ijircst.org/download_certicate.php

Detail Study of Cloud Infrastructure

Certificate of Publishing_Detail St

Embedded is the survey paper on "SORENSEN BASED MULTI-TENANT CLOUD MANAGEMENT BY TRAINED ANFIS MODEL", which got published in the following International journal.
http://www.viirj.org/specialissues/2021/SP2110/Part%2015.pdf

http://www.viirj.org/specialissues/2021/SP2110/SP2110.html

- Part 15 (Download)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007091 |

Vidyabharati International Interdisciplinary Research Journal (Special Issue) | ISSN 2319-4979

SORENSEN BASED MULTI-TENANT CLO

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details