Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A LITERATURE SURVEY ON CLOUD COMPUTING SECURITY

Sachin Kumar Vishnoi[1], Dr. Ashish Saini[2], Kavita Paliwal[3]

[1]Research Scholar, Department of Computer Science, Quantum University, Roorkee
[2]Assist. Professor, Department of Computer Science, Quantum University, Roorkee
[3]Assist. Professor, Department of Electrical And Electronics Engineering, RIPM College, Haridwar

Abstract: Cloud computing is computing that give memory, databases, interacting medium, intelligence, software and coherent over the internet. Cloud computing means exposing resources over the internet to valid users and malicious attackers. A renter's assets can be accessed via web browsers, remote connections, APIs and so on. Cloud assistance is carrying out remotely and virtually every time from an off-premises data processing center. That's why there is a need to improve security risks to keep data secure from the theft and destruction. Cloud services control computing infrastructure efficiently. Certain work traces the overview for cloud safety matters, currently validate strategies, evidence depot methodologies. This paper also illustrates the comparison between the various cloud security schemes. In the end that work outlines future investigation area related to evidence safety and privations defense issues in cloud.

Keywords: Cloud computing, Authentication, Data Transparency, Data security

1. INTRODUCTION

According to the NIST **"**The data storage services, servers, network services are deliver over the Internet is known as Cloud computing". Cloud computing refers as delivery of different computing services over the internet. These services provided to the user into two form first service model and second demand model. The users only have to pay whenever he used it. Different both model enlisted below:

1.1 Service Model

- (SaaS): This service model provide the information with the help of service provider to the various consumer on the cloud by the Internet . Such as Google Docs, Email, Face book, etc .
- (PaaS): The services provided by this model in such a way that some specific operating system is preinstall by the cloud vendors to run the cloud services hence it is known as platform as a service for example Google apps, Amazon web services.
- (IaaS):It is one of the layers of cloud computing which provide the services as a infrastructure. Here user needs to pay for the pre-determined hardware configuration. The model of cloud computing is shown in fig.1.1 [3].

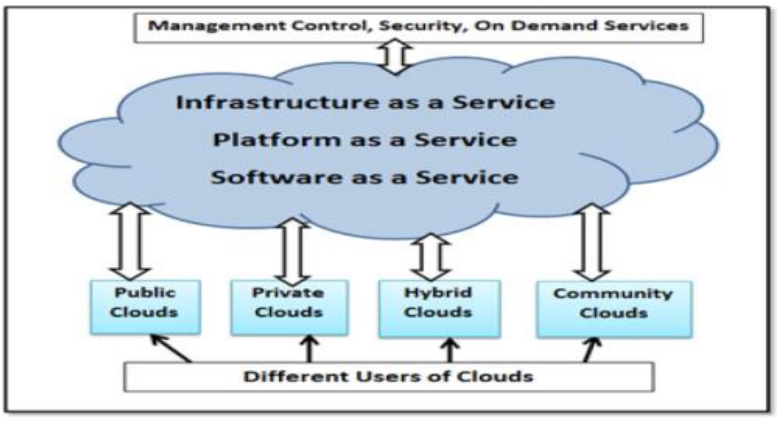


Fig .1.1 Model of cloud computing

1.2 Deployment model

According the NIST [4] different cloud deployment models are classified below:

- Private cloud: The cloud environment used by only single entities, hence it is called private cloud.
- Community cloud: The cloud architecture is utilized by numerous users, those have the identical purpose.
- Public cloud: The cloud model is utilized by all viewers.
- Hybrid cloud: The cloud structure is operate as privatized cloud, general cloud as well as community cloud.

This paper shows some comparison between the numerous security models and the rest of the paper is described as follows. Section 2 indicates the Cloud computing security threat. Section 3 describes various permission strategies for cloud security in cloud environment. Section 4 explains comparison between the different cloud security models. Section 5 presents the future direction.

2. CLOUD COMPUTING SECURITY THREAT

Threat	**Illustration**
1.Confidentiality	
Internal user risks: • Wicked cloud supplier buyer • Malicious cloud customer purchaser • Wicked unbiased observer	The risk of inners retrieving buyer info. belonging to inside the large network has superior to every of the supplier module.
External attacker threats: • Remote software exploit of cloud infrastructure and cloudapplication	The risks of outsider exploiters feasibly grasped to put in extra to general Internet cladding large network, but several kinds of cloud transmit prototypes be afflicted outsider exploiters, certainly into isolated large network where consumer last terminals are aim at.
Data leakage: • Defeat of protection approach in vast network environment	A risk for spilling the data beyond numerous challenger associations, using the same network provider feasible due to individual mistake that will cause to data embarrass.
2.Integrity	
User access: • Poor identity as well as retrieve managementprocedures	Execution of bad approach command strategy made several risks chances, can effect intended destruction to their source of evidence.
Evidence grade: • Initiation of malfunction request or configuration elements	The ultimatum of effect of evidence attribute is increased as big network providers host several consumers' information. The commencement of a defective or wrong configured element need by further cloud consumer would surely effect the integrity of information for alternate network customers Participating structure.
3.Availability	
Change management: • Buyer perforation checking impactingother vast network users • Structure switches depend on big	If network supplier is expanding liability to transpose administration inside each cloud delivery structure, Changes would surely generate bad effects, posing a risk. These would be due to changes in active micro services.

network supplier, buyer and unbiased observer organizations impacting large network buyers	
Substantial Interference: • Disturbance of cloud supplier IT servicesthrough physical access • Dislocation of TPA WAN facilities	The ultimatum of disturbance to cloud facility due to actual approach is inequality of large cloud facility suppliers and their consumers. There is a risk that large network buyer structure can be actually disturbed more quickly even by internal or outsider environment.
Exploiting weak recovery procedures: • Citation of deficient adversity recuperation or occupation constancy action	The risk of deficient adversity and event supervision process being launched is heightened when wide network buyers observe recuperation of their centralized organization.

2.1 Cloud Challenges

The cloud challenges issues described in fig.1.2

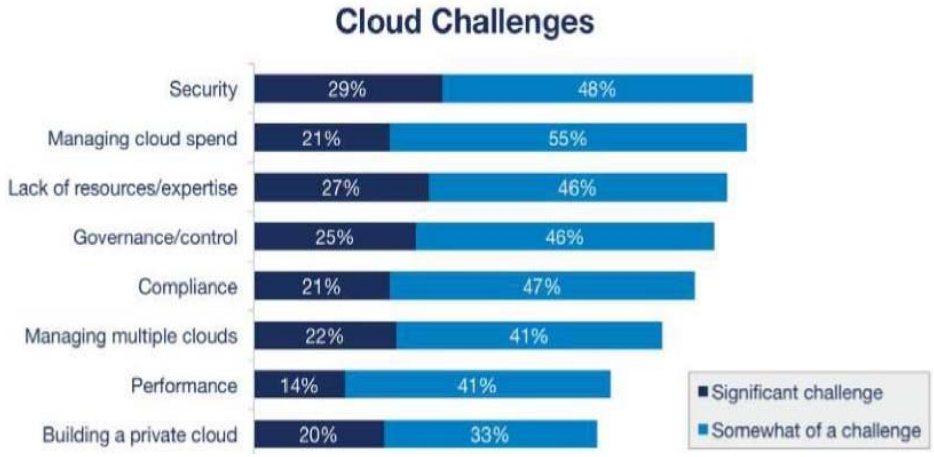


Fig.1.2 Cloud Challenges

According to the fig. cloud security is big task. The fig shows that for 77% of respondent, security a significant challenge [6].

3. AUTHORIZATION SCHEMES FOR CLOUD SECURITY

Amna Batool & Syed Muhammd Raza Abidi [1] gives a deep study on risks and provocation of cloud computing security.To minimize the problem of cloud security MLMI System is used by the authour . This model Output layer detects the security issues by determining various threats that occurs such as lack of visibility of data, theft of data, failure to control data. Syed Amma Sheik & Prabakar [2] conduct a survey on the issue of cloud security. Author also presented numerous schemes for authelications and data storage. Also comparison between the different security algorithms presented by the author. Shumailia Shahzadi & Bushra khaliq [3] presented security and risk protection method. An adaptive neural control fuzzy system, Sugeno control methods, Different membership functions and point-by-point examination approaches examine by the author. Sugeno membership function gives superior result and ensures the data accuracy and data computing efficiency. P. Mell and T. Grance [4] & M. Abadi, D.G. Andersen [5]provide a suitable definition of cloud computing , architecture, different service model, development model of cloud computing on the bases of experimental analysis .Also provide a baseline for new researcher in cloud computing. Stefania Loredana Nita [6] conducts a survey to compare various ANN approach in cloud security. On the bases of study conclude that ANN reduce the cloud security. X. Zhang, F. Chen, B. Chen, Z. Cao [7] purpose a neural network and learning algorithm. The purpose of using new approach is to disintegrate the vast put in equivalent parts and the entire is directed by two perceptions merge along a unusual 172P neuron. It is observe that DNA algo.is superior over S-BOX approach. Zhi Zhang et al. Zhi Zhang, Liwei Wang, Rulying Liu and Jinghang [8] presented an article which focus on

hardware and software platform of cloud computing. Their function is to minimize the data storage and high energy consumption problem of cloud. A. Amini, N. Jamil, A. R. Ahmad and H. Sulaiman [9] develop a conceptual risks identifying and prioritizes model according to the severity and prospects. This paper also present relationship between risk rate and trapezoidal fuzzy . Fuzzy logic based model is used to determine the risk rank in cloud computing. A. P. H. Gusmão [10] shows different cyber security obstacles model that made up of fault tree analysis and decision theory which purposed by the author to avoid the hacking of cyber security system. Tabassum, A. Ditta, T. Alyas, S. Abbas [11] shows a selection criteria based on QOS(Quality of servce) parameter in cloud. This help in improving the rank of cloud in hyper converged environment. Do ThiBac, Nguyen Hieu Minh [12] present new cloud computing technology which provides the security of cloud storage system. Jingyi Ma [13] proposes a meteorological prediction model to improve the accuracy and efficiency of cloud by using neural network as a tool. This technique used for large data analysis. B.Rajkumar , T.Gopikiran [14] proposed their approach in medical field .This approach collectively called UIMS cloud computing service in medical field. This technique helps in the treatment of cancer. Taher M. Ghazal, Muhammad Ubaidullah [15] explains the security issues and provoked. Also implements a issue detection model which help in find issue. Choe, Hebbian [16] purpose a model against overturn and majority overturn attack. This model provides the better security against the attacker because of lack of its knowledge of hidden units. Mazin Omar Khairo [17] Shows the relationship between cloud computing and neural network also illustrate the importance of neural network in cloud. Yuanyuan Chai, Limin Jia, Zundong Zhang [18] implements' a new techniques for data scaling, security. This technique uses a hydride algo. And used adaptive neural fuzzy system as a tool . Also explain the advantage of mamdani system. Jingyu Xing, Zheng Zhang [19] provides depth study of hierarchical network security. This techniques improves real time and effectiveness of network security posture by providing index to each individual process data. H. Fayyaz, Z. U. Rehman and S. Abbas [21], A. Fatima, S. Abbas and M. Asif [22]and L. Benedict Carvin , A Dalvin Vinoth Kumar , Dr. L. Arockiam [23]these shows enhancement of cloud techniques in different field such as medical, environment and disaster management. Rohan Jathanna , Dhanamma Jagli [24] provide study on different security issues, different security risk model. They provide deep knowledge of cloud computing issues and security.

Lohit Kapoor , Archana Pandita [25], Xiao Min ,Guo Mei , Zhu Weiping [26]and Mazin Omar Khairo [27]shows different security features of ANN and its various application. Using this methods author optimize the timing of accessing data and security risks.The study Ranganath Kothamasu, Samuel H. Huang [29]and Segismundo S. Izquierdoa , Luis R. Izquierdob [30] provide working of Mamdani inference system ,its role in cloud computing security .Author also provide the working and simulation model of this techniques. This model improves the security risks. Satendra Sonare, Ashish Mishra, Ashok Verma [31] introduced a client-server-cloud-computing model. This model immediately allows any businessmen application to other side of network to customers by providing single-point control. This technology is economical and assured. Saranya Eswaran and Dr.Sunitha Abburu [32] implements a new method called third-party-audit for data integrity. The aim of this method is to make certainity in the data and provide evidence to data is guarded. It also provides the coding to assure the data and it decreases the access time and cost of regain the file. Akhil bhel and Kanika bhel[33] focus on the various data privacy and security threats in cloud environment and provide a summary of available mechanisms for cloud security. Based on their research author recommend the cloud security solution related to following issues i.e. multi-tendency, elasticity, availability of evidence ,assure evidence supervise, evidence concerned to probity ,privacy and cloud assure federation. Md. Tanzim Khorshed, A.B.M. Shawkat Ali [34] focuses on cloud computing gaps and security concerns. Author presented a support vector machines technique .This model detect the attack and alert the data owner about the attack type. Wentao Liu [35] give a critical review on Traditional techniques which include encryption mechanisms, security authentication and control policy. It can preserve the user data and assured the cloud security and privacy. Deyan Chen, Hong Zhao [36]take a look cloud computing security risks and illustrate the security at every phase of data cycle.Paul de Hert, Vagelis Papakonstantinou, Irene Kamara [37] presented some ISO/IEC 27018 standard to address the drawback of cloud computing .This paper provide brief on data protection and provocation of security. This code also creates mechanisms for cloud customers. Marianthi Theoharidou, Nick Papanikolaou [38] inspects the privacy threats, vulnerabilities and remedies that customers should implements to achieve privacy conformance and accountability. It is examine the

numerous privacy threats. Jungwoo Ryoo , Syed Rizvi[39] explored unique cloud certainty provocations related to specific cloud computing authority sucha as banking, medical and government sectors and also introducing the actual resources to the IT security examiners faced with cloud security. A. Kassahun [40] emerge new technology that will amendment the accomplishment of buyer- tech- occupation required for flesh drive sequence limpid organization .Also provide brief idea based on EPCIS as well as limpid organization activated by large network depend utility. Xu Yanga,, Xinyi Huang, Joseph K. Liu[41] show a number of authentication point of view and proposed a verticular handover authentication scheme which work on key pre-distribution phase and handover authentication phase. Also present the performance consideration inclined in distinct handover convention. Prassanna.J,Punitha.K, Neelanarayanan. V [42]examine the process for data liability and cloud costomer data in distribute cloud which provide the better data transparency, data intigirity and data accountability. Yinghui Zhang , Xiaofeng Chen[43] proposed a MATCH-THEN-DECRYPT methodology and ABE module to improve the privacy and decryption efficiency of outsourced data in cloud computing by implementing first match the phase process then introduced decryption phase . Yousra Abdul Alsahib S.Aldeen, 1Mazleena Salleh[44] show a ananymization methodology that control the performance of overhead and improve the privacy data. HuiYina , Zheng Qin[45] focus on a query privacy enhanced and secure keyword query scheme to provide protection over encrypted cloud data. Sravani Challa, Ashok Kumar Das[46] show a secure authentication key sentiment scheme for cloud which help smart grid and also describe performance consideration based on interval communication ,computation cost and functionality features. Christos Stergiou, Kostas E. PsannisSecurity[47] present a new methodology to improve the security and privacy issues by using IoT integrated architecture. Qamas Gul Khan SaÞ , Senlin Luo[48] presented cloud based security for communication information environment. Also presented identity based signature to warrant the privacy of carrier node in cloud system. Vinod Kumar, Musheer Ahmad [49] Show elliptic curve cryptography based authentication for cloud security and also show simulation loop “AVISP” to achieve the goal of secure communication to accompany with anonymous. Rabah Attia, Maryline Laurent[50] presented a PAbAC technology that depend on characteristic based coding technology to ensure the certainity of outsource data in cloud server. Saurabh Dey, Qiang Ye, Srinivas Sampalli[51] show a machine based interposition observation scheme. This scheme used a OS and situation data as the outline of a client to protect the cloud data from the malicious attack. B.D. Deebak, Leonardo Mostarda [52] proposed a secure unidentified scheme to provide routing control overhead. Masoumeh Safkhani, Carmen Camar [53] improve the work of [49] by introduced a advanced RSEAP 2 scheme to improve security RSEAP scheme .It is more efficient method. B.D. Deebak, Fadi AL-Turjman[54] have emerged a lightweight smart card depends secure authentication [LS-BSA] scheme to enhance the performance efficiency in term of calculation . K. Mohana Prabha, Abdelhakim Zeroual[55][56] emerge multifactor authentication scheme to improve the performance of single factor authentication scheme by effectively checking the consumer who need the cloud data service with minimal time. Meijia Xu , Ding Wang[57] presented reason of failure of authentication scheme. Heng Zhou, Chunjie Yang [58] introduced a multi-objective optimization depends on deep learning methodology to determine blast furnace making process. S. Navin Prasad, C.Rekha [59] suggests an IAS convention to ensure the validation and reliability of information transmission in cloud accretion.This model permit for deconcentrated key supervision for retrieval and cancellation. To examine the productiveness of this process author proposed model is simulated on cloud environment. This method show better performance in term of energy consumption. Nishant Doshi, Payal Chaudhari[60] offer an IoT based identification mechanisms using sensor and it assert to secure the cloud averse to various attack. Miguel Landry Foko Sindjoung,Mthulisi Velempini [61] give a deep study on hybride computerized encoding system that uses regular and irregular computerized coding to improve information security. Zainulabedin Hasan Mohammed [62] explores block chain method to erect a definitive localized certification system. This model provides the true authentication and the trace of end activity by improving the lustiness of numerous checks on evidence.

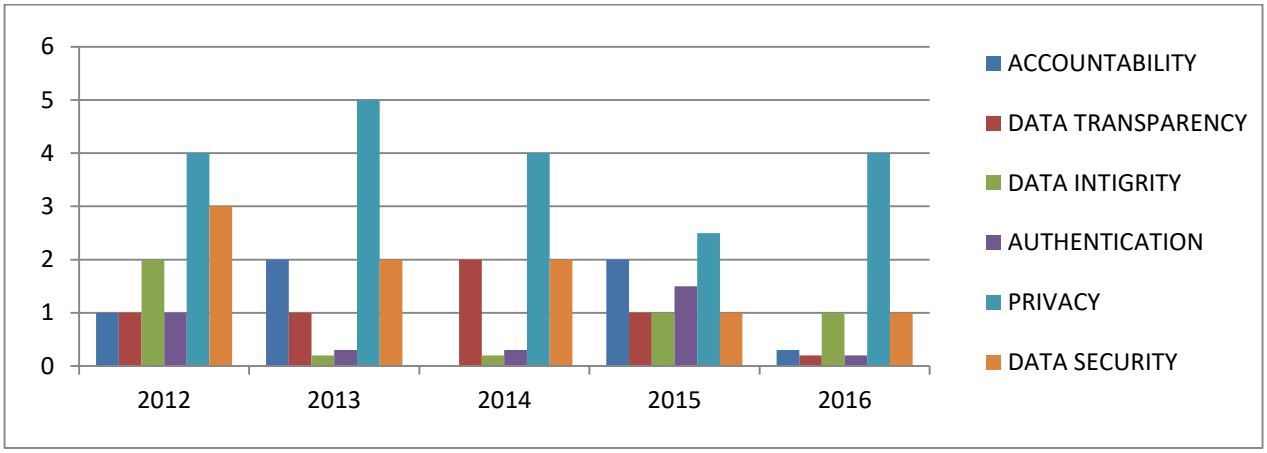
4. COMPARISON BETWEEN THE DIFFERENT CLOUD SECURITY SCHEMES

COMPARISON OF SECURITY SCHEME								
S. NO	**PAPER**	**METHODOLOGY**	**ACCOUNTABILITY**	**DATA TRANSPARENCY**	**DATA INTIGRITY**	**AUTHENTICATION**	**PRIVACY**	**DATA SECURITY**
1	Satendara sonare[31](2012)	CLIESNT SERVER CLOUD COMPUTING	YES	NO	NO	NO	NO	NO
2	Saranya Eswaran[32](2012)	TPA	NO	NO	YES	NO	NO	YES
3	akhil bhel[33](2012)	MULTI-LAYER SECURITY SOLUTION	NO	NO	YES	NO	YES	NO
4	Deyan Chen[36](2012)	DIFC(decentralized information flow control)	NO	NO	No	NO	YES	YES
5	Md. Tanzim Khorshed[34](2012)	Support Vector Machine technique	NO	YES	No	NO	YES	NO
6	Wentao Liu[35] (2012)	Encryption mechanism	NO	NO	No	YES	YES	YES
7	Paul de Hert[37] (2013)	standard ISO/IEC 27018	YES	YES	NO	NO	NO	YES
8	Marianthi Theoharidou[38] (2013)	CSPs	YES	NO	NO	NO	YES	YES
9	Jungwoo Ryoo[39](2014)	ISMS,Service Level Agreements,	NO	YES	NO	YES	NO	YES
10	A. Kassahuna[40](2014)	3p TSP TRANSPARENCY SYSTEM BASED ON EPCIS	NO	YES	NO	NO	NO	NO
11	Xu Yang[41](2015)	Vertical handover authentication scheme	NO	NO	NO	YES	YES	YES
12	Prassanna.J[42] (2015)	data accountability mechanism	YES	YES	YES	NO	NO	NO
13	Yinghui Zhang[43](2016)	match-then-decrypt and cp-ABE construction	NO	NO	NO	NO	YES	YES
14	Yousra Abdul Alsahib S.Aldeen[44](2016)	Innovative Privacy Preserving Technique	NO	NO	YES	NO	YES	NO
15	A. Amini[9](2017)	Fuzzy Logic Based	NO	NO	NO	NO	NO	YES
16	Mazin Omar Khairo[17](2017)	neural networks	NO	NO	YES	NO	NO	YES
17	L. Benedict Carvin[23](2017)	ENNEGCC	NO	NO	NO	NO	NO	NO
18	Hui Yin[45](2017)	a query privacy-enhanced and secure keyword query scheme	NO	YES	NO	NO	YES	YES

19	Sravani Chall[46](2018)	Cyber-Physical System	NO	NO	NO	YES	NO	YES
20	Christos Stergiou[47](2018)	Big Data & IoT	NO	NO	NO	NO	YES	YES
21	Qamas Gul Khan Saf[48](2018)	(IBS)	NO	NO	NO	NO	YES	YES
22	Vinod Kuma[49](2019)	elliptic curve cryptography (ECC) based authentication Mechanism	NO	NO	NO	YES	NO	YES
23	Rabah Attia e [50] (2019)	PAbAC i	YES	NO	NO	YES	NO	NO
24	Saurabh Dey[51](2019)	Machine Learning Based Intrusion Detection	NO	YES	YES	NO	NO	NO
25	B.D. Deebak[52](2020)	seamless secure anonymous authentication scheme (S-SAAS)	NO	NO	NO	YES	YES	YES
26	Masoumeh Safkhani[53](2020)	RSEAP2	NO	NO	NO	YES	NO	YES
27	B D Deebak[54](2020)	LS-BSA approach	NO	NO	NO	YES	NO	YES
28	K. Mohana Prabha[55](2020)	SKMA-SC technique	NO	NO	NO	YES	NO	YES
29	Abdelhakim Zeroual [56] (2021)	DeepCNN and LTP (Hybrid approach)	NO	NO	NO	YES	YES	NO
30	Meijia Xu[57](2021)	multifactor authentication schemes based on passwords	NO	NO	NO	YES	YES	YES
31	Heng Zhou[58]](2021)	multi-objective optimization model b	YES	NO	NO	NO	NO	NO
32	D. Prabhu[1](2022)	(PPS-BAS)	NO	NO	NO	yes	YES	YES
33	Amna Batool[2](2022)	CSID-MLMFIS	NO	YES	NO	NO	NO	YES
34	Do -Thibac[12](2022)	AES	NO	NO	YES	NO	YES	NO
35	Taher M. Ghazal[15](2022)	FUZZY LOGIC	NO	YES	YES	NO	NO	NO
36	S. Navin Prasad[59](2023)	BLOCK CHAIN BASED IAS METHOD	NO	NO	NO	YES	YES	YES
37	Nishant Doshi[60](2023)	Lee et al scheme(IOT,sensor)	NO	NO	NO	YES	NO	NO
38	Miguel Landry Foko Sindjoung[61](2023)	Mobile Edge Computing-based network	NO	NO	NO	YES	YES	YES
39	Zainulabedin Hasan Mohammed[62] (2023)	Blockchain-enabled bioacoustics	NO	NO	NO	YES	YES	YES

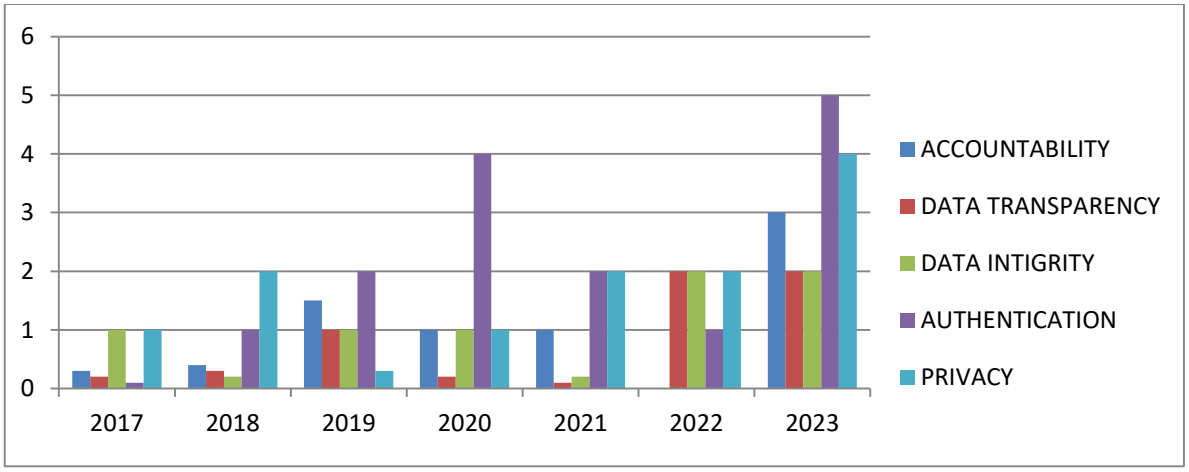
40	Qing Yang[63](2023)	BAN logic analysis	NO	NO	NO	YES	YES	YES

4.1 GRAPHICAL REPRESENTATION OF FIVE YEAR CLOUD SECURITY SCHEME FROM 2012 T0 20216



(a) Chart from 2012-2016

4.2 GRAPHICAL REPRESENTATION OF LAST SIX YEAR CLOUD SECURITY SCHEME FROM 2017 TO 2023



(b) Chart from 2017-2023.

5. CONCLUSION AND FUTURE DIRECTIVES

In this work, we present the various cloud computing security scheme used in cloud environment. Last 10 year cloud security work is described here by using tabulation and graphical representation. Our future aspect is that this paper will provide the better understating to the researcher in different cloud security scheme which will help in their further future work.

REFERENCE

[1] Amna Batool ,Syed Muhammad Raza Abidi, Mushtaq Hussain,‘‘Intelligent Cloud Security Issues Detection Using Mamdani Fuzzy Logic, ‘‘International Journal of Computer Intelligence System,vol.1, I 3,pp 33-51 (July-Sep 2022)

[2] Syed Amma Sheik, Amutha Prabakar Muniyandi ,‘‘Secure authentication schemes in cloud computing with glimpse of artificial neural networks”,2023

[3] Shumaila Shahzadi, Bushra Khaliq, Muhammad Rizwan, ‘‘Security Of Cloud Computing Using Adaptive Neural Fuzzy Inference System’’Security And Communication Networks vol 2020, Article ID 5352108, 15 pages.

[4] P. Mell and T. Grance, “The NIST definition of cloud computing,” in National Institute of Standards and Technology, vol. 53(6), pp. 50, 2009.

[5] M. Abadi, D.G. Andersen, Learning to protect communications with adversarial neural cryptography,ar Xivpreprint arXiv:1610.06918 (2016).
[6] Stefania Loredana Nita , Marius Iulian Mihailescu, ‘‘On Artifical Neural Network used in Cloud Computing Security-A Survey,’’ International Conference-10th edition (2018) IEEE
[7] X. Zhang, F. Chen, B. Chen, Z. Cao, ‘‘A new scheme for implementing s-boX based on neural network, in: Computational Science and Computational Intelligence (CSCI), 2015 International Conference on, IEEE, 2015, pp. 571–576.
[8] Zhi Zhang ,Liwei Wang, Rulying Liu and Jinghang , ‘‘Development of Cloud Computing Platform Based on Neural Network,’’vol.2022, Article ID 1513081,9 pages.
[9] A. Amini, N. Jamil, A. R. Ahmad and H. Sulaiman, "A Fuzzy Logic Based Risk Assessment Approach for Evaluating and Prioritizing Risks in Cloud Computing Environment," Recent Trends in Information and Communication Technology. IRICT 2017. Lecture Notes on Data Engineering and Communications Technologies, vol. 5, p. 650–659, 2017.
[10] A. P. H. de Gusmão, M. M. Silva, T. Poleto, L. C. e Silva and A. P. C. Seixas Costa, "Cyber security risk analysis model using fault tree analysis and fuzzy decision theory," International Journal of Information Management, vol. 43, pp. 248-260, 2018.
[11] Tabassum, A. Ditta, T. Alyas, S. Abbas, H. Alquhayz, N. A. Main and M. A. Khan, "Prediction of Cloud Ranking in a Hyperconverged Cloud Ecosystem Using Machine Learning," Computers, Materials and Continua, vol. 67, no. 3, p. 3129–3141, 2021.
[12] Do ThiBac, Nguyen Hieu Minh, ‘‘Design of network security storage system based on under cloud computing technology’’Thai Nguyen University, Vietnam,2022.
[13] Jingyi Ma,‘‘Research On Meteorological Cloud Computing Platform Based On BP Neural Network,’’ International Conference on Computer Information and Big Data Application,2020.
[14] B.Rajkumar , T.Gopikiran ,‘‘ Neural Network Design in CloudComputing’’ ,International Journal of Computer Trends and Technology- volume4Issue2- 2013
[15] Taher M. Ghazal, Shahan Yamin Siddiqui, Muhammad Ubaidullah, Hafiz Muhammad Usama, Ali Younas, Atif Ali , ‘‘Cloud Security Issues Detection Using Fuzzy Logic,’’ The 8th International Conference on Next Generation Computing 2022
[16] Choe, Hebbian learning, in: Encyclopedia of Computational Neuroscience, Springer, 2015, pp. 1305–1309.
[17] Mazin Omar Khairo, ‘‘The Use of Neural Networks in the Cloud Computing Environment’’, Journal of Information Engineering and Applications , Vol.7, No.2, 2017.
[18] Yuanyuan Chai, Limin Jia, Zundong Zhang, ‘‘Mamdani Model based Adaptive Neural Fuzzy Inference System and its Application,’’ International Journal of Computational Intelligence,2009.
[19] Jingyu Xing, Zheng Zhang , ‘‘Hierarchical Network Security Measurement and Optimal Proactive Defense in Cloud Computing Environments’’ Security and Communication Networks, Volume 2023, Article ID 9808414, 1 page.
[20] Vladimir Stantchev, Ricardo Colomo-Palacios, Michael Niedermayer, ‘‘Cloud Computing Based Systems for Healthcare,’’ The Scientific World Journal, Volume 2014, Article ID 692619, 2 pages.
[21] H. Fayyaz, Z. U. Rehman and S. Abbas, "An IoT Enabled Framework for Smart Buildings Empowered with Cloud & Fog Infrastructures," 2019 International Conference on Innovative Computing (ICIC), pp. 1-8, 2019.
[22] A. Fatima, S. Abbas and M. Asif, "Cloud Based Intelligent Decision Support System for Disaster Management Using Fuzzy Logic," Lahore Garrison University Research Journal of Computer Science and Information Technology, vol. 2, no. 3, 2018.
[23] L. Benedict Carvin , A Dalvin Vinoth Kumar , Dr. L. Arockiam, ‘‘ENNEGCC-3D Energy Efficient scheduling algorithm using 3-D Neural Network Predictor for Green Cloud Computing Environment’’ International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT),2017.
[24] Rohan Jathanna , Dhanamma Jagli , ‘‘Cloud Computing And Security Issues’’ International Journal of Engineering Research and Applications -June 2017.
[25] Lohit Kapoor , Archana Pandita , “Neural Network Based Optimal Placement Strategy for Service Components in Cloud Computing’’ International Conference on Electrical and Computing Technologies and Applications,2017

[26] Xiao Min ,Guo Mei , Zhu Weiping, " Reseach and Impementation of Network Security Deployment Based On Private Cloud Security Platform" International Conference on Intelligent ,Interactive System and Applications, 2022
[27] Mazin Omar Khairo, "The Use of Neural Networks in the Cloud Computing Environment" Management of Information Technology Department, Journal of Information Engineering and Applications, Vol.7, No.2, 2017.
[28] Muder Almiani, Alia Abughazleh, Yaser Jararweh, "Resilient Back Propagation Neural Network Security Model for Containerized Cloud Computing" Department of computer Engineering and Telecommunication International IT University, Almaty, Kazakhstan,2022
[29] Ranganath Kothamasu, Samuel H. Huang, "Adaptive Mamdani fuzzy model for condition-based maintenance" Intelligent Systems Laboratory, Department of Mechanical, Industrial, and Nuclear Engineering, University of Cincinnati, 2007
[30] Segismundo S. Izquierdoa , Luis R. Izquierdob, " Mamdani fuzzy systems for modelling and simulation: A critical assessment" University spain, 2022
[31] Satendra Sonare1, Ashish Mishra, Ashok Verma, "An authentication mechanism based on Client-Server architecture for accessing Cloud Computing" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 7, July 2012.
[32] Saranya Eswaran1 and Dr.Sunitha Abburu , "IJCSI International Journal of Computer Science Issues," Vol. 9, Issue 2, No 1, March 2012.
[33] Akhil bhel and Kanika bhel , "An analysis of cloud computing security" ICDCIT 2012, LNCS 7154, pp. 212–230, IEEE 2012.
[34] Md. Tanzim Khorshed, A.B.M. Shawkat Ali , "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing" School of Information and Communication Technology, CQ University 2012
[35] Wentao Liu , "Research on Cloud Computing Security Problem and Strategy" Department of Computer and Information Engineering, Wuhan Polytechnic University, Wuhan Hubei Province 430023, China 2012
[36] Deyan Chen, Hong Zhao , "Data Security and Privacy Protection Issues in Cloud Computing" College of Information Science and Engineering Northeastern University1 Shenyang,ICCSEE.2012.193 2012
[37] Paul de Hert, Vagelis Papakonstantinou, Irene Kamara, "The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection" Free University of Brussels[2013]
[38] Marianthi Theoharidou, Nick Papanikolaou "Privacy Risk, Security, Accountability in the Cloud", Information Security & Critical Infrastructure Protection Research Laboratory Department of Informatics, International Conference on Cloud Computing Technology and Science IEEE 2013.
[39] Jungwoo Ryoo , Syed Rizvi , "Cloud Security Auditing :Challenges and Emerging Approaches" article 2014 IEEE
[40] A. Kassahun, R.J.M. Hartog , T. Sadowski , "Enabling chain-wide transparency in meat supply chains based on the EPCIS global standard and cloud-based services" Information Technology Group, Wageningen University, Hollandseweg 1, 6706 KN, Wageningen, The Netherlands,2015.
[41] Xu Yanga,, Xinyi Huang, Joseph K. Liu , "Efficient Handover Authentication with User Anonymity and Untraceability for Mobile Cloud Computing" Faculty of Information Technology, Monash University, Australia 2015.
[42] Prassanna.J, Punitha.K, Neelanarayanan.V , "Towards an analysis of data accountability and auditing for secure cloud data storage" School of Computing Science & Engineering, VIT University, Chennai 2015.
[43] Yinghui Zhang , Xiaofeng Chen , " Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing" National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, china 2016.
[44] Yousra Abdul Alsahib S.Aldeen, 1Mazleena Salleh, "An Innovative Privacy Preserving Technique for Incremental Datasets on Cloud Computing" Faculty of Computing, Universiti Teknologi Malaysia, 2016.
[45] HuiYina , Zheng Qin, " A query privacy-enhanced and secure search scheme over encrypted data in cloud computing" Journal of Computer and System Sciences 2017.
[46] Sravani Challa, Ashok Kumar Das , "Design and analysis of authenticated key agreement schemein cloud-assisted cyber-physical systems" Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 2018

[47] Christos Stergiou, Kostas E. PsannisSecurity, “Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT” Department of Applied Informatics, School of Information Sciences, University of Macedonia,2018.
[48] Qamas Gul Khan SaÞ , Senlin Luo , Chao Wei , Limin Pan ,Guanglu Yan , “Cloud-based security and privacy-aware information dissemination over ubiquitous VANETs” Information System & Security and Countermeasures Experiments Center, School of Information and Electronics,Beijing Institute of Technology,2018.
[49] VinodKumar, MusheerAhmad, “ RSEAP:RFID based secure and efficient authentication protocol for vehicular cloud computing” Department of Applied Sciences and Humanities, Jamia Millia Islamia,, India 2019
[50] Rabah Attia, Maryline Laurent, “Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds” SERCom Lab, Ecole Polytechnique de Tunisie, Université de Carthage, Tunisie, SAMOVAR, CNRS, Télécom SudParis, Institut Polytechnique de Paris, France. Journal of Parallel and Distributed Computing 135 (2020) 1–20
[51] Saurabh Dey, Qiang Ye, Srinivas Sampalli, “A Machine Learning Based Intrusion Detection Scheme for Data Fusion in Mobile Clouds Involving Heterogeneous Client Networks” Faculty of Computer Science, Dalhousie University, Canada 2019.
[52] B.D. Deebak , Leonardo Mostarda, “ Seamless secure anonymous authentication for cloud-based mobile edge computing” School of Computer Science and Engineering, Vellore Institute of Technology, Computer Science department, Camerino University, Italy 2020.
[53] MasoumehSafkhani,, Carmen Camar, “ An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing” aComputer Engineering Department, Shahid Rajaee Teacher Training University, Tehran 16788-15811, Iran ,Computer Science Department, Carlos III University of Madrid, Madrid 28911, Spain 2020.
[54] B.D. Deebak, Fadi AL-Turjman, “Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing” School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India 2020.
[55] K. Mohana Prabha., Vidhya Saraswathi, “Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography for privacy preserved data access in cloud computing” Department of Computer Applications, Kalasalingam Academy Of Research And Education, Anand Nagar, Krishnankoil 626126, Tamil Nadu, India, Department of Computer Science and Information Technology, Kalasalingam Academy Of Research And Education, Anand Nagar, Krishnankoil 626126, Tamil Nadu, 2020
[56] Abdelhakim Zeroual , Mohamed Amroune, “ Lightweight deep learning model to secure authentication in Mobile Cloud Computing” Journal of King Saud University – Computer and Information Sciences 34 (2022) 6938–6948
[57] Meijia Xu , Ding Wang, “Understanding security failures of anonymous authentication schemes for cloud environments” Journal of Systems Architecture 118 (2021).
[58] Heng Zhou, Chunjie Yang, Youxian Sun, “Intelligent Ironmaking Optimization Service on a Cloud Computing Platform by a Digital Twin” The State Key Laboratory of Industrial Control Technology & College of Control Science and Engineering, Zhejiang University, Hangzhou,china 2021.
[59] S. Navin Prasad, C. Rekha, “ Block chain based IAS protocol to enhance security and privacy in cloud computing” Dept. of Data Science, The American College, Madurai, Tamilnadu, India , Department of Computer Science, Government Arts College, Melur, Tamilnadu,2023.
[60] Nishant Doshi, Payal Chaudhari, “ Cryptanalysis of Authentication Protocol for Cloud Assisted IoT Environment” Pandit deendayal Energy Unviersity, Gandhinagar, Gujarat, India.2023
[61] Miguel Landry Foko Sindjoung , Mthulisi Velempini, “A data security and privacy scheme for user quality of experience in a Mobile Edge Computing-based network” Department of Computer Science, University of Limpopo, Mankweng, South Africa, 2023.
[62] Zainulabedin Hasan Mohammed , “ Blockchain-enabled bioacoustics signal authentication for cloud-based electronic medical records” Department of Information Technology, Jazan University, Saudi Arabia,2023.
[63] Qing Yang , Xiaoqian Zhu, “A novel authentication and key agreement scheme for Internet of Vehicles” School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, China ,

School of Information and Communication Engineering, Guangzhou Maritime University, Guangzhou, China
2023