Cloud computing security issues & challenges: A Review

[1]Avijit Mondal & [2]Subrata Paul
[1,2]Research Scholar, MAKAUT, INDIA
[1]Department of CSE, Techno International, Batanagar, INDIA
avijit.mondal@tib.edu.in
subratapaulcse@gmail.com

Radha Tamal Goswami
Department of CSE, Techno International New Town, INDIA
rtgoswami@tict.edu.in

Sayan Nath
Department of CSE, Techno International Batanagar, INDIA
sayan.nath@tib.edu.in

Abstract— **Cloud computing is the most latest developments in the IT industry also known as on-demand computing. This technology attracting different organization because of its advantages like throughput, scalability, easy access etc. Beside this it has a big challenge of security and privacy issues. In this paper, we review different security challenges in cloud computing like Trust, authenticity, confidentiality, encryption, key management, multitenancy, data splitting, virtual machine security and we also have discussed how to overcome these issues.**

Keywords- Cloud Computing, Security Issues, trust, confidentiality, authenticity, encryption, Multitenancy.

I. INTRODUCTION

In cloud computing data is distributed in different geographical locations as resources which are accessed remotely by different users across the cloud. Robustness and secured computing is very necessary in cloud infrastructure.The procedure followed is that any organization tries to store data either on host files or on the public cloud, the ability to have physical access is lost to the servers hosting its own information. Due to this potentially sensitive data becomes vulnerable to insider attacks. A recent report on Cloud Security Alliance says that insider attacks are the sixth biggest threat in cloud computing. To avoid such kind of threats a thorough background checks must be conducted for persons having physical access to the servers of data centres. Frequent monitoring required for data centres for any suspicious activities.

Cloud is mainly categorized as private cloud which can restrict, improve security or optimize the access between the user and network. Public cloud is a platform which provides individuals or organizations who want to access the service without absorbing the full cost of the infrastructure.Hybrid cloud is the mixture of two or more cloud models where data transfer occurs between them without affecting each other.

II. CLOUD ARCHITECTURE

Cloud computing models are divided into 3 categories.

A. Software as a Service:

Apps are hosted and distributed online via a web browser that provides traditional desktop apps such as Google Docs, Gmail, etc.

B. Platform as a Service:

For systems such as Google App Engine, cloud provides the software platform. The hardware and software are managed by a PaaS company on its own network. PaaS therefore enables users to install in-house hardware and software to build or run a new application.

C. Infrastructure as a Service

Here a number of virtualized services is stored in the cloud, such as space and processing power. Those consumers access resources and services through a wide area network, such as the internet, and can use the tools of the cloud provider to download the remainder of an application stack.

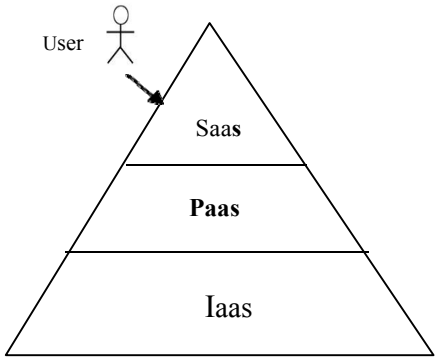
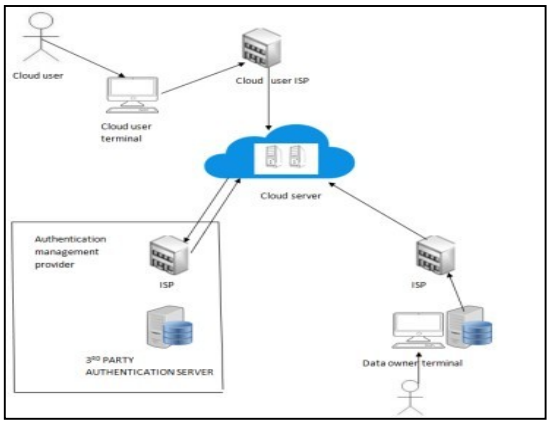


Fig 1: A Typical Cloud Model

978-1-7281-4514-3/20/$31.00©2020 IEEE

Fig 2: Authentication process in cloud computing



III. LITERATURE SURVEY

In cloud computing the main research issue is security and privacy. In the year 2008 Cloud Security Alliance [1] was formed and their main issue was to provide security in cloud environment. The Multi-Agency Cloud Computing Group has made great efforts to provide successful controls in the cloud environment to provide cyber security[2]. It is found that the main security problem with regard to cloud is trust, confidentiality, and encryption. Many security issues are discussed in [3] and [4]. A cloud computing framework and information asset classification model were proposed to help cloud users choosing different delivery services and models [2].

A. Security challenges in Cloud Computing andprobable Solutions:

1. Trust Problem: Trust between serving end and receiving end is the main issue for all. Person at receiving end is never sure whether the serving end is providing trustful data so the servicing ends are bound by Service Level Agreement(SLA) document. SLA document includes duties of the service provider and their future plan activities [5]. SLA framework [6] is used as a trust management model for security in cloud environment.

2. Confidentiality Problem: It prevents disclosure of any private information. If we design a secure storage service is public cloud infrastructure and apply cryptographic analysis, privacy of data and confidentiality can be achieved. A new approach [8] P2P reputation system is used now days to prevent privacy. It gives virtualized defence [9], describes attribute-based cryptography, so that user can share data in a flexible and dynamic manner.

3. Authenticity Problem: Integrity is the method which checks if there is any improper modification of information. Cloud should be very secure. A cloud user has to be an authentic user.

Authentication problem generally solved using digital signature approach. An access control mechanism proposed [10] is a robust and decentralized control mechanism where cloud verifies the identity of cloud user without knowing the user information and stores the information of the user. Stored information can be decrypted by the authentic users.

4. Encryption Problem: Most widely data securing mechanism is encryption in cloud computing. But the main drawback of encryption is, it needs high computational power. It also reduces overall database performance because every time when query is run, decryption required for the encryption. A proposed methodology [12] suggests that using cryptographic algorithms in combination instead of only one algorithm, one can efficiently accelerate the throughput. The cloud tables are maintained such a way that data are encrypted using these methods. Here requested query is executed against the stored data, and the result is decoded by the user. This increases overall performance. Another method called end-to-end mechanism based encryption [13] works differently for the cryptographic processes. Another approach called fully Holomorphic encryption [14] which can calculate results of encrypted data processing instead of the raw data, which might increase potential data confidentiality.

5. Key Management Problem: Managing the efficient use of key is abig security problem in cloud which includes the proper management of encryption/decryption and keys. Cloud stores the encrypted key which is a very complex technique. A small database should be maintained to accommodate keys protectively.To accomplish this, additional hardware and

data are scattered everywhere, so access control mechanism

978-1-7281-4514-3/20/$31.00©2020 IEEE

software resources are required and costing increases to implement. A two-level encryption solution is given to this problem [15].

6. Data Splitting Problem: It is an alternative of encryption process and works faster than encryption. Data splitting is a process to split data to more than one host at a time when they cannot communicate individually. So when users want his or her data back, the user must have to access all of the service allocators to recollect the original data. It also has some security problems.If multiple clouds are being used, then ensuring integrity should be checked after splitting process can be done using Multi-Cloud Database Model [5]. As data are stored in different cloud and replication should be done, security also is in higher priority. Because the attacker will get less chance to access multiple clouds at a time. Secret Sharing algorithm [16] and TMR Technique [17] is used to share data.

7. Multitenancy problem: Confidentiality issue might arise due to scattered resources in different geographical area of cloud environment. Isolation of applications and system should be done for proper confidentiality, if not done may lead to insecurity issues[18].If data are stored virtually, then virtual machine hosting a malicious program may affect the overall

978-1-7281-4514-3/20/$31.00©2020 IEEE

performance of their machines. Cloud service provider should use IDS for the security of their customers. Architecture to deploy IDS is defined in [19]. Virtual machine security can be provided by using Trusted Cloud Computing Platform (TCCP) [20].

IV. A SHORT REVIEW ON RECENT WORKS ACCOMPLISHED IN SECURITY ISSUES OF CLOUD COMPUTING

TABLE I. SHORT REVIEW ON DIFFERENT TYPE OF PAPER IN SECURITY ISSUES OF CLOUD COMPUTING

Sl. No	Year of Publication	Paper Title	Authors	Short Description
1	2019	Large-scale Optimized Searching for Cruise Itinerary Scheduling on the Cloud	TessemaMengistu, Abdulrahman Alahmadi, Abdullah Albuali	Taking into consideration the Cruise Itinerary Schedule Design (CISD) issue, a cruise itinerary needs to be identified to improve a cruise company's payoff. A strategy optimization approach based on a heuristic taboo search strategy that measures and tests the cruise schedule and a genetic algorithm optimizing the heuristic search parameters. The suggested performance approach and the scalability / cost efficiency of the Amazon Web Services cloud infrastructure were given.
2	2019	A new Security Mechanism for Vehicular Cloud Computing Using Fog Computing System	MhidiBousselham, Nabil Benamar, Adnane Addaim	Vehicle Cloud Computing (VCC) has recently become an appealing approach that meets demands for vehicles to compute and store service. Traditional cryptographic algorithms needs to ensure safety after compromising their keys. To ensure a stable vehicle network, using a fog computing architecture, a new DT decoy technology and user behavior profiling (UBP) has been implemented as an alternative solution to address data security, confidentiality and confidence in vehicle cloud serversIn the scenario of malicious actions, a high productivity is achieved by supplying decoy files in such a way that the attacker can not distinguish between both the original and decoy files.
3	2019	Green Cloud Framework for Reducing Carbon Dioxide Emissions in Cloud Infrastructure	Mustafa Ibrahim Khaleel, Awder Mohammed Ahmed	The rising installation of data centers and cloud services worldwide, with higher electricity rates, increased energy costs, the cost of cooling and connectivity, and the emission of carbon dioxide. Dynamic Voltage and Frequency Scaling (DVFS) method has been applied to minimize cloud server power consumption by measuring the best near-optimal frequency. The goals were achieved without reducing the quality of service (QoS) set out in the Agreement on Service Level (SLA). Cloud Sim has been simulated and compared with algorithms such as the Rank and EARES-D showing better results than heuristic methods.
4	2018	One Quantifiable Security Evaluation Model for Cloud Computing Platform	Aobing Sun, GuohongGao, TongkaiJi, Xuping Tu.	In a cloud, users lack effective, quantifiable security evaluation methods to capture their own information infrastructure's security situation. A quantifiable security assessment system has been introduced for various clouds that can be accessed through a consistent API. The grading system includes the engine for security inspection, the engine for security recovery, the design for safety analysis, the visual display module, etc. The program adopts "one vote vetoed" mechanism to count one field's score and add the summary as the overall score, and to establish one view of safety.
5	2018	Trust Model for Computing Security of Cloud	Snehal R Rathi Vikas KKolekar	Through creating a confidence model for the computing power of a cloud service, researchers have tried to overcome security challenges. In this case, the trust value is created using the implemented trust model to provide various security aspects such as authorisation and authentication. The article tends to focus on different parameters such as data security, authorization, authentication, and virtualization to provide cloud security. The system enacted here could be used by cloud users to evaluate different cloud services.
6	2018	Research on key technology of network security situation awareness of private cloud in enterprises	Liu Qing Zhu, Boyu Wan Jinhua, Li Qinqian	This article considers as its point of entry the basic network network security security situation, big data protection, private cloud network security situation, analyzes the related evaluation indexes and sets up the evaluation system model and other key technologies, elaborates on the security situation of private cloud networks in companies
7	2017	A "No Data Center" Solution to Cloud Computing	TessemaMengistu, Abdulrahman Alahmadi, , YousefAlsenani, DunrenChe	The enormous unused processing and storage capacities of underused PCs can be combined as complementary cloud fabrics to provide large cloud services, mainly as a network infrastructure. They had already implemented a "no data center" approach that complements the cloud provision model based on the data center. Their opportunistic cloud computing system, known as cucloud, operates on underutilized PC assets within an organization / community.
8	2016	A Remote Engine Health Manage	JianXiong ; Hong Gu	ECU (Electronic Control Unit) of the engine can not only control the engine, but also can monitor the working condition, diagnostic the faults of engine, generate and save

978-1-7281-4514-3/20/$31.00©2020 IEEE

		ment System Based on Mobile Cloud Computing		fault code with DSM (Diagnostic System Management) module. This article adds a centralized DSM and mobile cloud-based engine health management capable of gathering the engine's real-time working conditions and fault codes to the Big Data Cloud platform. By analyzing and processing these Big Data, it can help customers to know about the condition of the engine health in a timely manner, can give precaution to the faults, can improve the engine's availability. In the meantime, it can help manufacturers boost new product performance and quality.

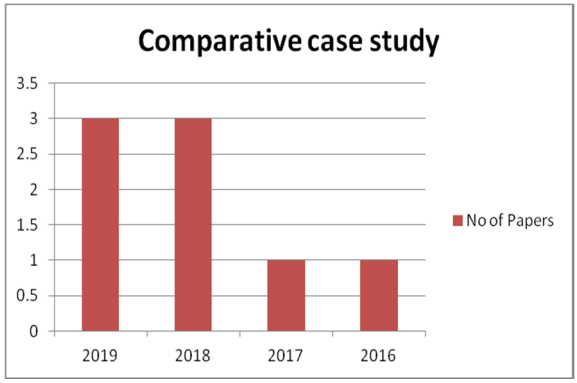


Fig 3: Comparative case study yearwise

V. CONCLUSION

In this Review Paper, the major points discussed are the security issues along with privacy. The convenient available solutions are also discussed in this paper. Moreover one major issue is sharing the resources. So, we may conclude that to enhance the service of Cloud Computing, the security issues has to be minimized as well as we have to enhance the Encryption method.

VI. FUTURE WORK

Sharing of resources is the biggest security problem in cloud computing. In cloud computing, data can be access by any person. So we have to put some encryption and decryption part in cloud computing. In the future we will put username and password in the cloud computing which will be used for specific user only. Research in cloud computing is not end here, so much work can be done in future .But still many problem are unknown and unseen so the door of the future research is always open.

REFERENCES

[1] Messmer, Ellen (March 31, 2009). "Cloud Security Alliance formed to promote best practices". Computerworld.Retrieved May 02, 2014.

[2] Onwubiko, Cyril. "Security issues to cloud computing." Cloud Computing. Springer London, 2010. 271-288.

[3] Ko, Ryan KL, et al. "TrustCloud: A framework for accountability and trust in cloud computing." Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011.

[4] Pearson, Siani, and AzzedineBenameur. "Privacy, security and trust issues arising from cloud computing." Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on.IEEE, 2010.

[5] AlZain, M., Soh, B., & Pardede, E. (2012). A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. IEEE.

[6] M. Alhamad, "Conceptual SLA Framework for Cloud Computing", Accepted for IEEE DEST 2010 on 15 March 2010 2010.

[7] Alhamad, Mohammed, Tharam Dillon, and Elizabeth Chang. "Sla-based trust model for cloud computing." Network-Based Information Systems (NBiS), 2010 13th International Conference on.IEEE, 2010.

[8] Hwang, Kai, Sameer Kulkareni, and Yue Hu. "Cloud security with virtualized defense and reputation-based trust mangement." Dependable, Autonomic and Secure Computing, 2009.DASC'09.Eighth IEEE International Conference on.IEEE, 2009.

[9] Narayan, Shivaramakrishnan, Martin Gagné, and Reihaneh Safavi-Naini. "Privacy preserving EHR system using attribute-based infrastructure." Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010.

[10] Yu, Shucheng, et al. "Achieving secure, scalable, and fine-grained data access control in cloud computing." INFOCOM, 2010 Proceedings IEEE. Ieee, 2010.

[11] Yassin, Ali A., et al. "Efficient Password-based Two Factors Authentication in Cloud Computing." International Journal of Security & Its Applications 6.2 (2012).

[12] Purushothama. B., & Amberker, B. (2013). Efficient Query Processing on Outsourced Encrypted Data in Cloud with Privacy Preservation.

[13] Pearson, Siani, et al. "End-to-end policy-based encryption and management of data in the cloud." Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on. IEEE, 2011.

[14] Tebaa, Maha, Saïd El Hajji, and Abdellatif El Ghazi. "Homomorphic encryption applied to the cloud computing security." Proceedings of the World Congress on Engineering. Vol. 1. 2012.

[15] Wang, Guojun, Qin Liu, and Jie Wu. "Achieving fine□grained access control for secure data sharing on cloud servers." Concurrency and Computation: Practice and Experience 23.12 (2011): 1443-1464.

[16] Shamir, Adi. "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

[17] Lyons, Robert E., and Wouter Vanderkulk. "The use of triple-modular redundancy to improve computer reliability." IBM Journal of Research and Development 6.2 (1962): 200-209.

[18] Behl, A., & Behl, K. (2012). An Analysis of Cloud Computing Security Issues. IEEE, 109-114.

[19] Roschke, Sebastian, Feng Cheng, and Christoph Meinel. "Intrusion detection in the cloud." Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on. IEEE, 2009.

[20] Santos, Nuno, Krishna P. Gummadi, and Rodrigo Rodrigues. "Towards trusted cloud computing." Proceedings of the 2009 conference on Hot topics in cloud computing. 2009.

[21] Alexey Lesovsky. Getting Started with oVirt 3.3. ISBN 9781783280070.

[22] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4

978-1-7281-4514-3/20/$31.00©2020 IEEE