International Journal on Emerging Technologies **11**(4): 216-224(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Security and Data Challenges in Cloud Environment

Deepika[1], Rajneesh Kumar[2] and Dalip[3]
[1]Assistant Professor, Department of Computer Science and Engineering, M. M. Engineering College, Maharishi Markandeshwar (Deemed to be University)(Mullana) Ambala, (Haryana), India.
[2]Professor, Department of Computer Science and Engineering, M. M. Engineering College, Maharishi Markandeshwar (Deemed to be University) (Mullana) Ambala, (Haryana), India.
[3]Assistant Professor, M.M. Institute of Computer Technology and Business Management, Maharishi Markandeshwar (Deemed to be University) (Mullana) Ambala, (Haryana), India.

(Corresponding author: Deepika)
(Received 18 May 2020, Revised 23 June 2020, Accepted 03 July 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In this current era the cloud computing plays a vital role in the field of IT. The various resources like applications, storage, servers and networks are provided to their users on the basis of their demand and then they pay accordingly. Companies like Amazon, Azure, Google and Microsoft provide these services. Some of the important security principles are data confidentiality, integrity, user privacy, authentication and availability are explained in this paper. This paper shows the collective comparative year wise study on different security issues, attacks, information and location based security parameters; are also depicted in the tables given below. Some of the important parameters like data security, privacy, integrity, encryption and decryption, compliance, virtualization, backup, recovery, data location, control, geographical location information and Google latitudes has also been discussed in this paper which will be helpful for the user to implement security in the system.

Keywords: Attacks, Principles, Information, Location, Security.

Abbreviations: GPS, global positioning system; TCSEC, trusted computer system evaluation criteria; IAAS, infrastructure as a service; PAAS, platform as a service; SAAS, software as a service; IS, information system; IoT, internet of things; QoS, quality of service; NFV, network function virtualization; SDN, software defined networking; CIA, confidentiality, integrity and availability; DL-BC, distributed ledger based blockchain; COP, common operating picture; BC, blockchain; LBS, location based service; MCC, mobile cloud computing..

I. INTRODUCTION

Cloud computing is merged with the different fields and industries which helps the researchers to work on upcoming technologies [33]. The various services and resources are provided to cloud users and then they can transfer their data to cloud servers. Nowadays where technologies are coming day by day there is the need of more security on information among other aspects. Security is considered as an essential part of human life [1]. The important information which requires to be secured are like companies, banks and the military intelligence systems etc. In distributed data system, the users need powerful tools to access that data. A latest technology is used to overcome this problem which is called as cloud computing. It facilitates its users to share data and resources at any time, place and through any system via internet. The important challenge faced by the researchers today is security. To protect their information in cloud the users, academias, researchers and organisations do not have sufficient tools.

Cloud Security and its Challenges [1]:

- **Insider Access:** Data is at risk if firewalls and other security mechanisms are not used. This type of threat comes from users who access resources within an organization.
- **Identity Management:** Information security is an important concern for an organizations [9]. The cloud users has the ability to access its resources in a control and secure manner are considered as an important part of identity management.
- **Accessibility:** "Extensible Access Control Marts resources markup Languages" can be used rather than server interface are used to user accessibility control to cloud services.
- **Data Protection:** The information used by its users is spread among several places in the distributed cloud area. For secure data access the users accounts has also been protected in the cloud
- Database in the cloud: A cloud database runs on public or private cloud computing platform. A unique database management system has been maintained by each users and facilitate its users as per their requirements.

Location based cryptography [1].

- **Location Based Identity:** The identity is considered as an important component of cryptography. For example the person_name, fingerprint scanning, person_address and official_address. The data is decrypted only by that person who has the private_key.
- Location Based Access Control: Access control is the location based cryptography.

The resources can only be accessed by those users who are physically present in some specified location. For example the person who is in room can use the printer but once out of the room is not able to use it.

• Principles of Geo-Encryption: The Geo-Encryption method added a new security layer on the encryption protocols by using the location information of its users. At a specific geographical point of time the user reads and decrypts the encrypted data. The specific point is one where the information is to be converted in a readable form.

Cloud Computing Service Models [2]:

• Infrastructure as a Service (IaaS): This model provides its users to those resources which are required by its users like virtual machines. The model which provide these services is also called to be an IaaS provider.

• Platform as a Service (PaaS): This model provides software related services to its users like software related applications and software development frameworks.

• Software as a Service (SaaS): The SaaS provides its users to those required applications that are used by the cloud users over the internet.

Cloud Deployment Models [2]:

• Private Cloud: This cloud is used by a single user or a small scale organization. It is also known as internal clouds.

• Community Cloud: A community is a cloud which is made up of more than one organizations. This model is used by limited number of users.

• Public Cloud: This model provide its services to their users publically.

• Hybrid cloud: The hybrid network is made up of more than two clouds (private, community, or public).It act as a bridge between the cloud used by one user and one cloud managed by the public user.

Cloud Computing Security [2]:

• Trust: In computer science engineering, trust is not a new concept but the parameters like accessibility, reliability and secure access to resources is one of the important aspect which is needed to be considered for research.

• Security identification of threats: It is necessary to address the various security threats and challenges to provide the security to information.

• Confidentiality and Privacy: The information is accessed by only those persons who have the permissions provided by the cloud owner. There are number of cloud users who have been sharing the resources that makes threats to the data.

• Integrity: The authorized users has the permissions to alter the data. Data integrity is achieved by preventing unauthorized access.

The authorization is crucial which ensures that only authorized users can use the data. Software Integrity means to protect software from unauthorized deletion, modification and fabrication.

This paper is divided into four sections. The section II explains about the existing work presented by several researchers and also finds various gaps and the third part elaborates the concept of security principles, security attacks, information security and location based security. The issues arises in security and its solutions are also presented. The section IV atlast defines the results.

Literature: Security Attacks and Countermeasures on Cloud Assisted IoT Applications: The paper Asma Alsaidi *et al.*, 2018 discussed the Internet of things (IoT) [4] is an upcoming field to make human life easier. An integrated framework is designed for telemedicine and urban cities. This paper also investigated various types of security threats and attacks in IoT nodes and cloud environment. Advantages: The IoT technology once integrated with cloud computing providing storage and processed huge amount of data in real life applications. It also determines various security threats and attacks because of illegal retrieval of information stored in IoT nodes. IoT also provides a framework which supports integrated devices which are connected to internet in order to get controlled access to these devices. There are several security attacks which reduce risk and improve IoT security. Securities and threats of Cloud Computing and Solutions: This paper by P. Gayatri *et al.*, 2018 discussed [5] that cloud is one of the upcoming area in IT industry. As data is stored on the remote host by the client and can be saved anywhere. There are several issues discussed in this paper such as security, reliability and availability of cloud computing with feasible solutions. Advantages: Cloud based computer is an on demand computing which provides cost effective application performance and sharing of pool of resources to their users. Cloud uses virtualization concept as to count all network resources; as collection of machines are stored on a single server so cloud only paid for those resources by their service provider who used it. At the point of time when data is switched to the cloud various security issues are need to be considered in prior as centralized access of information, data access at any place and security issues. Security and QoS Guarantee-based Resource Allocation within Cloud Computing Environment: The paper Mohamad Hamze *et al.*, 2018 discussed as [6] The suggested framework is evaluated for a cloud videoconferencing application. Broker architecture act as most economical to get efficient QoS and security requirements. Future Edge Cloud and Edge Computing for Internet of Things Applications: This paper discussed Jianli Pan , Member, IEEE *et al.*, 2018 that [7] internet connects multiple number of edge devices together and exchange a huge amount of data transfer between these devices. In old cloud architecture it faces difficulties like very large distance among the edge devices, networking in data centers, computation and storage problems etc. To solve this problem edge cloud and computing that provides resources closer. Classification of Data to Enhance Data Security in Cloud Computing: The given paper "Kumar Pal Singh *et al.*, 2018 explains that [8] the data is to be partitioned in cloud on the different characteristics of security. To protect information different encryption algorithms are needed to be implemented. The data encryption methods can be used in terms of optimality and cost effectiveness. Blockchain technology for security issues and challenges in IoT: The paper "Nallapaneni Manoj Kumar *et al.*, Blockchain technology for security issues and challenges in IoT [9] Blockchain (BC) technology is used in IoT and to avoid the concept of centralized server system. Blockchain technique is also used in several engineering field services. Blockchain provides flexible and ease use of data access. Towards Location-Aware Access Control and Data Privacy in Inter cloud communication: This

paper discussed "Naseer Abwnawar *et al.*, 2017 proposed the [10] data privacy issues in hybrid cloud act as inter-cloud data transferred among various locations, networks and domains. The data is transferred among various physical and logical network locations on the basis of different security levels. The sensitive data is exchanged among several domains with different security levels and mechanisms so there is a requirement to adopt flexible access control approach. This paper deals with data privacy issues among heterogeneous cloud environment. The concept of location awareness and policy transition provides flexible access control among active location of both users and data. Advantages: The current and physical location of both the subject and object can be used to decide which rule has been used. Various policies can be applied as location changes. The concept of policy transition provides a flexible and fine approach to define location awareness policies in heterogeneous environment. Secure integration of IoT and Cloud Computing: This paper "Christos Stergiou *et al.*, 2016 [11] explained that there is another upcoming technology named as IoT in which wireless telecommunications can be used. The integration of these two technologies is to provide the interaction between the things and objects among wireless networks and act as a single entity. Advantages: The security issues in these two technologies are examined in order to find the common characteristics and determmine the usefullness of their integration. This paper presents that how cloud computing improve the functionality of IoT technology. The RSA and AES encryption algorithm used in integrated cloud computing and IoT technologies are used to find the security challenges by using the proposed algorithm model. Secure Framework for Data access Using Location Based Service in Mobile Cloud Computing: Location Based Service (LBS) [12] described by "Deepanshu Goyal *et al.*, 2015 which is used in authentication process. A user becomes an authorized user if its location is valid within an organization otherwise it will be unauthorized. This paper proposed a secure architecture for information accessing using the location based service (LBS) in MCC (mobile cloud computing) for authorized and registered user within the organization. The user is authentic if its identity is valid within the organization. The mobile devices are resources controlled on the basis of computation, storage and bandwidth.

Gaps: Security can be enhanced by extending sensor attributes and extends the functionality of MCC application. Only survey is presented for Cloud security attacks. No secure model is designed for cloud security. No provision for accessing secure information from cloud. Only Security and threats of cloud computing is analysis and their solutions is presented here. No cloud based security model is implemented. DDoS attacks should be implemented practically for cloud security. No provision for location based authentication for cloud users. Not a reliable framework for data and information security in cloud environment. Less provision for information security in cloud environment. The information security system can be implemented which can be optimal and cost effective. No latest techniques such as location, IoT and Block chain based secure framework are implemented for cloud security. No provision for location based authentication. The proposed approach extends the existing access control policy which supports location awareness and implements hybrid cloud where multiple networks and domains are involved. To enhance security a Location and Block Chain based secure framework can be implemented.

Table 1: Different Attacks and Methods in Cloud Environment.

Security Services	Different Methods and Security Attacks	Solutions
Data Confidentiality	• Packet sniffing • Wiretapping • Phishing • Information Gathering	By using advanced encryption and keys generation algorithms which are used to translate senders original data into a form which is not understandable by a human being at the time of data transmission.
Data Integrity	• Masquerade • Replay • Sequence Prediction • IP Spoofing • Alteration • Man-in-the-Middle Attacks • Message suppression / Fabrication /	Data integrity means to protect data from unnecessary modifications or alterations.
User Privacy	• Inference Attack • Phishing attack • Spam attacks • Malware Attacks	Cryptographic algorithms are implemented for system privacy and security.
Authentication	• Password Attacks • Dictionary attacks • Tunneling • Authentication bypass attacks • Session hijacking • Brute force Attack • Message Tampering	To maintain the authenticity of the user different authentication algorithms are used ; so that user becomes the legitimate user of the system such as RSA based digital signature and digital certificates.
Access Control	• Denial of Service Attack • Spoofing • Hardware hacking • SQL Injection	Different methods are used to control data access such as MAC (Mandatory Access Control), RBAC (Role Based Access Control) and DAC (Discretionary Access Control) .

II. MATERIALS AND METHODS

The given Table 2 depicts study of twenty nine papers for different security principles. A total eight security principles are taken for survey. Out of eight security principles six security principles such as Data Confidentiality (DC), Data Integration (DI), Authentication (AU), Access Control (AC), Data Privacy (DP) and Data Availability (DA) are widely used for survey in most of the research papers. Two security principles Client Server Security (CSS) and User Privacy (UP) are not commonly analyzed. This comparative study of all these security papers corresponding to all security principles shows useful contribution in cloud environment. In our research work, this study gives us an idea to further improve the information and location security of the users.

III. RESULTS AND DISCUSSION

A yearwise comparison of different security attacks, information and location security attributes are shown in the Table 3 given below. From this comparative analysis it has been quite clear that location security attribute and more secured information attributes are not frequently discussed in the existing studies and this will motivates the researchers to do their research on location and information based attributes in cloud environment. Atlast this paper discussed few important enhanced security attributes and performance evaluation metrics which has not been frequently used in the studies.

Table 2: Yearwise Comparison of Security Principles in Cloud Environment.

S. No.	Survey Papers	Years	Discussion on Security and Data Challenges	Security Principles							
				DC	DP	DA	DI	UP	AU	CSS	AC
1.	Kresimir Popovic *et al.*, [13]	2010	• Security issues, requirements and challenges are discussed.		y			y			y
2.	S. Subashini *et al.,* [14]	2011	• Various issues in challenges of security and securely storing of data is discussed.			y	y		y		
3.	Pardeep Sharma *et al.,* [15]	2011	• This paper describes different security issues and comparison of different service models.	y	y	y	y		y		
4.	Zaigham Mahmood [16]	2011	• Issues related to consumers data security,storage location,cost,availability and security	y	y	y	y				
5.	Yu-Jia *et al.,* [17]	2011	• Location data security problem in LBS and IJS algorithm for data encryption is discussed.		y	y			y		
6.	Dimitrios Zissis *et al.,* [2]	2012	• Cryptography, PKI operating in concert with SSO and LDAP and Generic principle are discussed to prevent threat among data security.	y	y		y	y	y		y
7.	Meer Soheil Abolghasemi *et al.,* [1]	2013	• Different issues in security, its challenges, geo-encryption and location based security is discussed.		y				y		y
8.	Lipi Akte *et al.,* [18]	2013	• Information security, Data storage, infrastructure and privacy among information during the transfer of data among users.	y	y	y	y		y		
9.	Lien *et al.,* [19]	2013	• To provide protection to LBS model and private circular query protocol(PCQP) which provides security was presented in this paper.					y			
10.	Ni Zhang *et al.*, [20]	2013	• Different technical solutions are discussed to provide data security like virtualization and IDM.								y
11	T V Sathyanarayana *et al.,* 21]	2013	• To analyze the information security on basic principles of confidentiality, availability and integrity.	y	y	y	y		y		
12.	Keiko Hashizume *et*	2013	• Virtualization, data storage and different security issues and their			y					y

	al., [22]		solutions are presented in this paper.								
13.	Dinadayalan *et al.,* [24]	2014	• Various latest technologies are discussed that are used to provide resources to cloud users like network, storage etc are discussed in this paper.	y		y	y	y	y	y	
14.	Shweta *et al.,* [25]	2014	• Data Security, Network Security, Virtualization.		y	y	y		y		y
15.	Shankarwar and Pawar [26]	2015	• This paper explains several methods that are used to solve the security issues and privacy.	y	y	y					y
16.	Mojtaba Alizadeh *et al.,* [27]	2016	• To provide security in the system authentication mechanisms are there to provide it.	y	y	y		y	y	y	y
17.	Minhaj Ahmad Khan *et al.,* [28]	2016	• This paper presents the data security and its solutions on cloud platform.	y	y	y	y		y	y	y
18.	Subash Chandra Pandey *et al.,* [29]	2016	• This paper describes that the different cloud users can remotely access their data so that they can achieve high quality applications and services.	y	y	y	y		y		
19.	Ahmed Albugmi *et al.,* [30]	2016	• This paper discussed about the efficient encrypting technique that provide security to its data.	y		y	y		y		
20.	Yaxing *et al.,* [31]	2016	• To identify privacy and security issues and PDP protocol which is used to determine geographic location attribute for urban areas.	y	y		y	y			
21.	Ashish Singh *et al.,* [33]	2017	• This paper explains the different security attacks, threats and its solutions and also explain how different cloud users access its resources from different locations.	y	Y	y	y	y	y		y
22.	Muhammad Baqer Mollah *et al.,* [34]	2017	• Security solutions(Proposed schemes) and security features • Challenges faced by MCC	y	y		y		y		y
23.	Rajakumar S *et al.,* [3]	2017	• This paper discussed secure cloud framework to provide security in the system from unauthorized users.	y			y	y	y		y
24.	Tejashri A. Patil *et al.,* [35]	2017	• This paper explains the identity of the user who is going to access the data remotely.	y	y	y	y		y		y
25.	Tarek Radwan *et al.,* [36]	2017	• This paper discussed cloud computing security issues, challenges, risks, deployment and delivery models. • Overcome virtualization and multi-tenancy problem. • Develop new cryptographic method for cloud computing.	y	y	y	y	y	y		y
26.	Gururaj Ramachandra *et al.,* [37]	2017	• This paper explains the security layer which is to be implemented in every layer of cloud.		y	y					y
27.	E.Kesavulu Reddy [38]	2017	• To identify privacy and security issues. • Security challenges			y				y	
28.	Jayachander [39] Surbiryala *et al.,*	2017	• Proposed a framework using homomorphic encrption for solving data security problems in cloud environment	y		y	y				y
29.	Aruna Guruvaya Mogarala *et al.,* [40]	2018	• Secure NoSQL technique is used in the data encryption.				y				y

*** Security Principals Attributes:** DC: Data Confidentiality DI: Data Integrity AU: Authentication AC: Access Control **UP: User Privacy** DP: Data Privacy DA: Data Availability **CSS: Client Server Security.**

Table 3: Yearwise Comparison of Security Attacks, Information Security, Location Security and Performance Evaluation in Cloud Environment.

Survey Papers	Years	Security Attacks Attributes					Information Security Attributes															Location Security Attributes							Performance Evaluation	
		ZA	LG	LT	DLL	DT	VM	IS	NS	DL	LB	DEKM	BR	DRCC	TM	NS	IAM	DS	DA	DLRL	PA	MT	DLP	DLC	GL	GLI	PA	LT	LCD	CO	CC
Ramgovind *et al.* [41]	2010													y			y							y							
Kresimir Popovic *et al.* [13]	2010		y				y							y			y		y					y							
Subashini *et al.* [14]	2011											y																			
Pardeep Sharma *et al.* [15]	2011						y				y				y	y	y		y												
Zaigham Mahmood *et al.* [16]	2011		y															y	y	y			y	y						y	
Yu-Jia Chen *et al.* [17]	2011											y													y		y	y			
Dimitrios Zissis *et al.* [2]	2012	y										y			y											y					
Meer Soheil Abolghasemi *et al.* [1]	2013																y							y		y					
Lipi Akte *et al.* [18]	2013								y			y						y													
Lien *et al.*, [19]	2013											y													y						
Ni Zhang *et al.* [20]	2013	y			y	y	y					y					y														
T V Sathyanarayana *et al.* [21]	2013						y			y	y	y	y	y	y		y					y									
Keiko Hashizume *et al.* [22]	2013						y					y										y									
Chetan Jaiswal *et al.* [23]	2014																								y	y	y	y			
Dinadayalan *et al.* [24]	2014				y							y	y	y	y	y		y	y	y											y
Singh *et al.* [25]	2014		y	y	y		y		y			y					y	y	y				y	y							
Shankarwar and Pawar [26]	2015				y	y				y		y			y				y		y	y									
Mojtaba Alizadeh *et al.* [27]	2016	y		y	y		y	y			y	y			y	y	y		y	y										y	
Minhaj Ahmad Khan *et al.* [28]	201	y					y		y			y			y	y	y		y											y	

	6																													
Subhash Chandra Pandey *et al.* [29]	2016									y		y	y			y			y											
Ahmed Albugmi *et al.* [30]	2016		y				y					y						y				y								
Yaxing Zha *et al.* [31]	2016									y		y			y											y			y	y
Vincent C. Emeakaroha *et al.* [32]	2017										y		y		y								y							
Muhammad Baqer Mollah *et al.* [34]	2017						y			y	y			y			y	y	y				y							
Rajakumar.S *et al.* [3]	2017																													y
Patil *et al.* [35]	2017			y	y					y		y						y	y		y	y						y		
Singh *et al.* [33]	2017	y	y	y	y		y					y			y	y	y		y			y								
Tarek Radwan *et. al.* [36]	2017				y		y		y	y			y		y				y			y		y						
Gururaj Ramachandra *et al.* [37]	2017		y				y					y	y											y						
Reddy *et al.* [38]	2017											y	y	y	y	y	y	y	y									y		
Asma Alsaidi et al. [4]	2018	y																												
Aruna Guruvaya Mogarala *et al.* [40]	2018	y					y					y	y						y											y
Christos Stergiou *et al.* [11]	2018			y	y				y		y	y						y	y			y		y						

***Security Attacks Attributes** ZA: Zombie Attack (DoS/DDoS attack) LG: Loss of Governance LT: Loss of Trust DLL: Data Loss and Leakage DT: Data Transmission.
***Information Security Attributes** VM: Virtualization IS: Internet & Service NS: Network Security DL: Data Loss LB: Load Balancing DEKM: Data Encryption and Key Management BR: Backup & Recovery DRCC: Data Recovery in Cloud Computing TM: Trust Management NS: Network Security IAM: Identity & Access Management DS: Data Security DA: Data Availability DLRL: Data Location and Relocation PA: Phishing Attack MT: Multi-Tenancy.
***Location Security Attributes** DLP: Data Location Policy DLC: Data Location GLI: Geographic Location Information GL: Google Latitudes PA: Phishing Attack LT: Location Tracking LCD: Location & Control of Data.
***Performance Evaluation Attributes** CO: Computational Overhead CO: Computational Cost.

IV. CONCLUSION

This paper explains the different security issues occurred in the cloud environment. The section 2 elaborates the contribution of several research papers and finds various gaps and section 3 shows a tabular representation of different security principles, security attacks, information security and location based security attributes. The above comparison shows that most of the parameters are commonly used by the researcher for their study but few parameters was less utilized. So this survey will help us to enhance the security in the wide manner. After completing the survey of all these security papers it has been quite cleared that less work done on information and location security attributes. This will encourage the researchers to do their research in the domain of location and information security based attributes in cloud environment.

V. FUTURE SCOPE

In future, some more security concepts are there for further research and as seen from the above tabular representation different security attacks, issues, challenges and location attributes are there which helps the researchers in their work. With the help of latest technologies like Internet of things and Blockchaining; more enhanced security can be implemented.

REFERENCES

[1]. Meer Soheil Abolghasemi, Mahdi Mokarrami Sefidab and Reza Ebrahimi Atani (2013). Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing. *International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE*, 261-265.

[2]. Dimitrios Zissis and Dimitrios Lekkas (2012). Addressing Cloud Computing Security Issues. *Future Generation Computer System*, *28*: 583-592.

[3]. Rajakumar, Anakath, Naresh and Senthilkumar (2017). A detailed study on Security Services in Cloud Environment. *Second International Conference on Recent Trends and Challenges in Computational Models, IEEE*.

[4]. Asma Alsaidi and Firdous Kausar (2018). Security Attacks and Countermeasures on Cloud Assisted IoT Applications. *IEEE International Conference on Smart Cloud*, 213-217.

[5]. P. Gayatri, M. Venunath, V. Subhashini and Syed Umar (2018). Securities and threats of Cloud Computing and Solutions. *Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018),*1162-1166.

[6]. Mohamad Hamze, Hassan Harb, Oussama Zahwe and Mohamad Abou Taam (2018). Security and QoS Guarantee-based Resource Allocation within Cloud Computing Environment. *IEEE Middle East and North Africa Communications Conference (MENACOMM)*.

[7]. Jianli Pan, Member, IEEE, and James McElhannon (2018). Future Edge Cloud and Edge Computing for Internet of Things Applications. *IEEE Internet Of Things Journal, 5*(1), 439-449.

[8]. Kumar Pal Singh, Dr. Vinay Rishiwal and Prof. (Dr.) Pramod Kumar (2018). Classification of Data to Enhance Data Security in Cloud Computing, *IEEE*.

[9]. Nallapaneni Manoj Kumar, Pradeep Kumar and Mallick (2018). Blockchain technology for security issues and challenges in IoT. *International Conference on Computational Intelligence and Data Science (ICCIDS 2018), Elsevier Ltd*, *132*: 1815-1823.

[10 Naseer Abwnawar, Halgie Janicke and Richard smith (2017). Towards Location-Aware Access Control and Data Privacy in Inter cloud communication. *IEEE EUROCON*, *5*(1), 739-744.

[11]. Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim and Brij Gupta. Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems, Elsevier B.V*, *78*: 964–975.

[12]. Deepanshu Goyal and M. Bala Krishna (2015). Secure Framework for Data access Using Location Based Service in Mobile Cloud Computing. *IEEE INDICON*, 1-6.

[13]. Kresimir Popovic and Zeljko Hocenski (2010). Cloud computing security issues and challenges. *The 33rd International Convention MIPRO, published by IEEE,* 344-349.

[14]. S. Subashani and V. Kavitha (2011). A survey on security issues in service delivery models of Cloud Computing. *Journal of Network and Computer Applications, Elsevier, 34*: 1-11.

[15] Pardeep Sharma, Sandeep K. Sood and Sumeet Kaur (2011). Security Issues in Cloud Computing. *International Conference on High Performance Architecture and Grid Computing HPAGC 2011, CCIS*, *169*: 36-45.

[16]. Zaigham Mahmood (2011). Data Location and Security Issues in Cloud Computing. *International Conference on Emerging Intelligent Data and Web Technologies, published by IEEE computer society*, 49-54.

[17]. Yu-Jia Chen and Li-Chun Wang (2011). A Security Framework of Group Location-Based Mobile Applications in Cloud Computing. *40th International Conference on Parallel Processing Workshops, IEEE computer society,* 184-190.

[18]. Lipi Akter, Prof. Dr. S M Monzurur Rahman and Md. Hasan (2013). Information Security in Cloud Computing. *International Journal of Information Technology Convergence and Services (IJITCS), 3*(4), 13-22.

[19]. Lien, I. T., Lin, Y. H., Shieh, J. R., & Wu, J. L. (2013). A novel privacy preserving location-based service protocol with secret circular shift for k-nn search. *IEEE Transactions on Information Forensics and Security*, *8*(6), 863-873.

[20]. Ni Zhang, Di Liu and Yun-Yong Zhang (2013). A Research on Cloud Computing Security. *International Conference on Information Technology and Applications, published by IEEE*, 370-373.

[21]. Sathyanarayana, T. V., & Sheela, L. M. I. (2013, December). Data security in cloud computing. In *2013 international conference on green computing, communication and conservation of energy (icgce)* (pp. 822-827). IEEE.

[22]. Keiko Hashizume, David G Rosado, Eduardo Fernandez-Meedina and Eduardo B Fernandez (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications 4, 5, published by a Springer Open Journal*.

[23]. Chetan Jaiswal, Mahesh Nath and Vijay Kumar (2014). Location-Based Security Framework for Cloud Perimeters, *IEEE Cloud Computing published by the IEEE Computer Society*, 56-64.

[24]. Dinadayalan, P., Jegadeeswari, S., & Gnanambigai, D. (2014, February). Data security issues in cloud environment and solutions. In *2014 World Congress on Computing and Communication Technologies* (pp. 88-91). IEEE.

[25]. Shweta Singh (2014). Security in Cloud Computing. *International Journal of Computer Applications Technology and Research, 3*(8), 488-493.

[26]. Shankarwar, M. U. and Pawar A. V. (2015). Security and Privacy in Cloud computing: A Survey. *Proc. of the 3rd Int. Conf. on Front. of Intell. Compt. (FICTA), Springer International publishing Switzerland,* 2.

[27]. Mojtaba Alizadeh, Saeid Abolfazli, Mazdak Zamani , Sabariah Baharun and Kouichi Sakurai (2016). Authentication in mobile cloud computing: A survey. *Journal of Network and Computer Applications, Elsevier*, *61*: 59-80.

[28]. Minhaj Ahmad Khan (2016). A survey of security issues for Cloud Computing. *Journal of Network and Computer Applications, Elsevier*, *71*: 11-29.
[29]. Subash Chandra Pandey (2016). An Efficient Security Solutions for Cloud Environment. International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES*), IEEE*, 950-959.
[30]. Ahmed Albugmi, Madini O. Alassafi, Robert Walters and Gary Wills (2016). Data Security in Cloud Computing. *Fifth International Conference on Future Generation Communication Technologies (FGCT 2016), IEEE*, 55-59.
[31]. Yaxing Zha, Shoushan Luo, Jianchao Bian and Wei Li (2016). A Novel Provable Data Possession Scheme Based on Geographic Location Attribute. China Communications, *published by IEEE*, *13*(9): 139-150.
[32]. Vincent C. Emeakaroha, Kaniz Fatema, Lisa van der Werff, Philip Healy, Theo Lynn and John P (2017). A Trust Label System for Communicating Trust in Cloud Services. IEEE Transactions on Services Computing, *10*(5): 689-700.
[33]. Ashish Singh and Kakali Chatterjee (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications, Elsevier*, *79*: 88-115.
[34]. Muhammad Baqer Mollah, Md. Abul Kalam Azad and Athanasios Vasilakos (2017). Security and Privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of network and Computer Applications*, *84*: 38-54.
[35]. Patil, T. A., Pandey, S., & Bhole, A. T. (2017, October). A review on contemporary security issues of cloud computing. In *2017 1st International Conference on Intelligent Systems and Information Management (ICISIM)* (pp. 179-184). IEEE.
[36]**.** Tarek Radwan, Marianne A. Azer and Nashwa Abdelbaki (2017). Cloud computing security: challenges and future trends. *Int. J. Computer Applications in Technology. Inderscience Enterprises Ltd.*, *55*(2): 158-172.
[37]. Gururaj Ramachandra, Mohsin Iftikhar and Farrukh Aslam Khan (2017). A Comprehensive Survey on Security in Cloud Computing, *The 3rd International Workshop on Cyber Security and Digital Investigation(CSDI 2017). Procedia computer Science 110, published by Elsevier B.V.,* 465-472.
[38]. Reddy, E. K., Prasad, K. S., & Ramakrishna, S. (2014). Information Security in Cloud Computing. *International Journal of Computer Applications Technology and Research*, *3*(8), 510-514.
[39]. Jayachander Surbiryala, Chunlei Li and Chunming Rong (2017). *2nd IEEE international Conference on Cloud Computing and Big Data Analysis,* 260-264.
[40]. Aruna Guruvaya Mogarala and Dr. Mohan K.G (2018). Security and privacy designs based data encryption in cloud storage and challenges: A review. *International Conference on Computing and Networking Technology (ICCNT), IEEE*- 43488.
[41]. Ramgovind S., Eloff MM and Smith E (2010). The Management of security in Cloud Computing. Conference: Information Security for South Africa (ISSA), *published by IEEE.*

How to cite this article: Deepika, Kumar, R. and Dalip (2020). Security and Data Challenges in Cloud Environment. *International Journal on Emerging Technologies*, *11*(4): 216–224.