Security Problems in Cloud Computing

https://doi.org/10.3991/ijes.v4i4.6538

Rola Motawie[1], Mahmoud M. El-Khouly[1], M. Samir Abou El-Seoud[2]
[1] Helwan University, Cairo, EGYPT
[2] The British University in Egypt (BUE), Cairo, EGYPT

***Abstract*—Cloud is a pool of computing resources which are distributed among cloud users. Cloud computing has many benefits like scalability, flexibility, cost savings, reliability, maintenance and mobile accessibility. Since cloud-computing technology is growing day by day, it comes with many security problems. Securing the data in the cloud environment is most critical challenges which act as a barrier when implementing the cloud. There are many new concepts that cloud introduces, such as resource sharing, multi-tenancy, and outsourcing, create new challenges for the security community. In this work, we provide a comparable study of cloud computing privacy and security concerns. We identify and classify known security threats, cloud vulnerabilities, and attacks**

***Index Terms*—cloud computing, data privacy, threats, vulnerabilities**

I. INTRODUCTION

The National Institute of Standards and Technology (NIST) [1] defined five essential characteristics of cloud computing, namely: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. Also, cloud computing is described as a dynamic and often easily extended platform to provide transparent virtualized resources to users through the Internet. Cloud computing architecture consists of three layers:

A. Software as a service (SaaS);
B. Platform as a service (PaaS)
C. Infrastructure as a service (IaaS)

The clouds are also viewed as five component architectures that comprise (clients, applications, platforms, infrastructure and servers). The current clouds are deployed in one of four deployment models:

A. public clouds in which the physical infrastructure is owned and managed by the service provider.
B. community clouds in which the physical infrastructure is owned and run by a consortium of organizations.
C. Private clouds in which the infrastructure is owned and administered by a particular organization. Moreover
D. Hybrid clouds that include combinations of the previous three models.

There are new concepts introduced by the clouds, such as resource sharing and centralized shared data, create new security challenges. The direct access or indirect usage of cloud infrastructure increase cloud vulnerabilities and threats. As clouds become more popular, security concerns grow bigger. Clouds are more sensitive to Distributed Denial of Service (DDoS) attacks due to the availability of resources and the elasticity of the architecture. Many researchers provide surveys that cover specific areas of cloud security concerns and proposed solutions. This study is categorized in threats, vulnerabilities, attacks, and other security and privacy issues that face the cloud [2][3]. Figure 1 shows cloud deployment models together (IaaS, PaaS, and SaaS).

I. CLOUD SECURITY CATEGORIES

We categorize cloud-computing security issues into three main categorize, as shown in Table 1 the different types of cloud security category, figure 2 show the various types of cloud security issues and classifications [34] figure 3 show Data security in cloud environment

A. Copy Data Category

Data Recovery, Data privacy, and data protection [6][7][8] have been labeled as important issues in different case studies that require data to be correctly transmitted, protected, encrypted, controlled and available in the time of need. In an on premise application deployment model, the critical data on each company proceeds to stay within its boundary and is subject to its logical, personnel, and physical security and access control policies. However, in the (SaaS) model, the company data is stored outside its boundary, at the (SaaS vendor) end. The SaaS vendor must use additional security controls to ensure data security and prevent violations due to security vulnerabilities in through hateful employees or the application. Involving the use of strong encryption techniques for data security and appropriates trained authorization to control access to data.

B. Network category

Security engineers predict that clouds will be the focus of Hackers in future due to the concentration of valuable

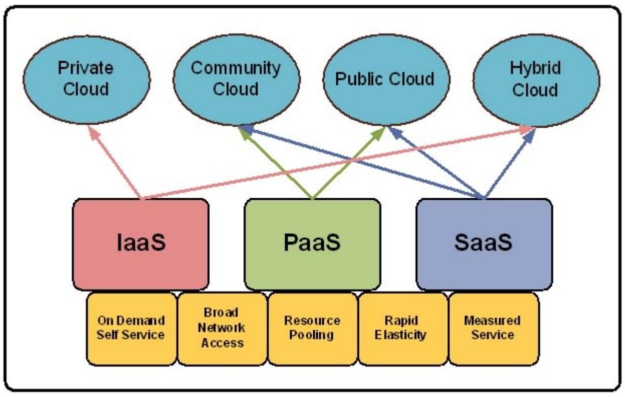

Figure 1. Cloud deployment models and infrastructure

TABLE I.
DIFFERENT TYPES OF CLOUD SECURITY CATEGORY

	Category	*Description*
1	Network	Includes network attacks such as Denial of Service DOS Connection Availability
2	Access Control	Authentication and access control, the privacy of user information and data storage
3	Data	Covers data related security issues including integrity, data migration.

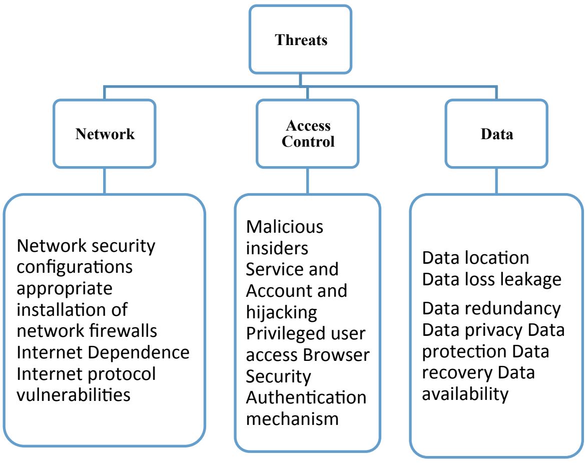
Threats
Network
Access Control
Data
Network security configurations appropriate installation of network firewalls Internet Dependence Internet protocol vulnerabilities
Malicious insiders Service and Account and hijacking Privileged user access Browser Security Authentication mechanism
Data location Data loss leakage Data redundancy Data privacy Data protection Data recovery Data availability

Figure 2. Cloud security issues and classifications [Rola, et.al., 2016][34]

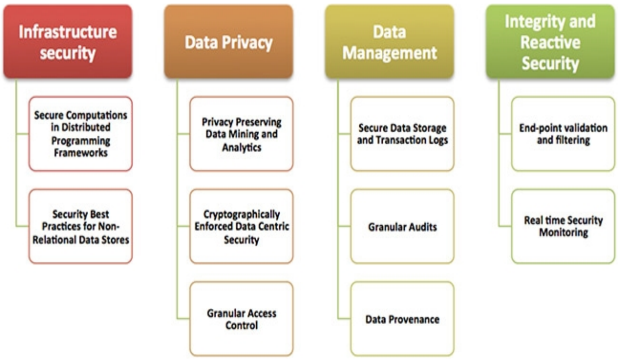
Infrastructure security
Secure Computations in Distributed Programming Frameworks
Security Best Practices for Non-Relational Data Stores
Data Privacy
Privacy Preserving Data Mining and Analytics
Cryptographically Enforced Data Centric Security
Granular Access Control
Data Management
Secure Data Storage and Transaction Logs
Granular Audits
Data Provenance
Integrity and Reactive Security
End-point validation and filtering
Real time Security Monitoring

Figure 3. Data Security issues in cloud environment

"assets" (data) within the clouds. The possible lack of proper installations of network firewalls and the overlooked security configurations within different clouds and on various networks, make it easier for intruders to access the cloud on behalf of authorized users. In a SaaS model, sensitive data is taken from the enterprises, prepared by the SaaS application and stored at the SaaS vendor at the end. All data flow over the network needs to be secured to prevent leakage of sensitive information. The use of (SSL) Secure Socket Layer and the Transport Layer Security (TLS) for security as network traffic encryption techniques. However, hackers can exploit weaknesses in the network to know the configuration to try to sniff network packets. The assessment tests made it is to validate the network security of the SaaS vendor. Network Penetration and packet analysis Session management weaknesses Insecure SSL trust configuration. Any vulnerability detected during these tests can be considered as exploited to hijack active sessions, gain access to user credentials and sensitive data [3].

C. *Access category*

Account and service hijacking like fraud, software vulnerabilities, and phishing, where attackers steal credentials and gain unauthorized access to servers, [4] this unauthorized access is a threat to, confidentiality availability and integrity of data and services unauthorized access can be launched from inside or outside the organization. A single customer may access data and launch services from multiple cloud providers using a mobile application or a browser from anywhere. This kind of access brings risk, and this risk has been called privileged user access Most companies, if not all, are storing their employee information in some types of Lightweight Directory Access Protocol (LDAP) servers. In the case of small companies, a segment that has the highest SaaS adoption rate, Active Directory (AD) seems to be the most popular tool for managing users. With SaaS, the software is hosted outside the company, so user credentials are stored in the SaaS provider's databases and not as part of the corporate IT infrastructure. This means SaaS clients must remember to remove or disable accounts as employees leave the company and create/enable accounts as come onboard. In essence, having multiple SaaS products will increase IT management overhead. For example, SaaS providers can provide delegate the authentication the process to the customer's internal LDAP/AD server, so that organizations can retain control over the management of users. [5]

II. EFFECTS OF ATTACKS

A. *Denial of service (DOS)*

Most of the severe attacks in cloud computing come from denial of service (DoS), especially HTTP and XML. The cloud users start requests in XML, and then send requests over HTTP protocol and usually create their system interface through REST protocols such as those used in Amazon EC2 and Microsoft Azur. Due to some vulnerabilities in the system interface, DoS attacks are easier to implement and difficult for security experts to countermeasure. HTTP-based DDoS and XML-based distributed denial of service (DDoS) are more harmful than regular DDoS; these protocols are used in cloud computing with no powerful tools possible to avoid them. HTTP and XML are critical and essential elements of cloud computing, so security over these protocols becomes important to providing healthy development of a cloud platform. [7]

B. *Phishing Attacks*

Phishing is a try to access personal information from the single user through social engineering techniques. It is usually done by sending links to web pages in emails or through instant messages. These links appear to be correct, attending to a certain site such as bank account login or credit card information confirmation and verification, but they almost take users to fake locations.

Through this fraud, the attacker can collect sensitive information such as credit card information, passwords. Phishing attacks can be organized into two categories:

a) Abusive behaviour in which an attacker hosts a phishing attack site on the cloud by using one of the cloud services.

b) Hijack services and accounts in the cloud through traditional social engineering techniques [9].

CSA Cloud security alliances stated that cloud service providers do not maintain sufficient control over systems to avoid being hacked or spammed. To prevent such attacks, CSA proposed a few anticipation measurements such as strict registration process, secure identity check procedure, and enhanced monitoring skills. Privacy rules in cloud computing do not permit cloud service providers to look at what customers are doing, so if a hateful individual or organization is performing something wrong by using any cloud services, it cannot be detected until notified by some security software [10].

III. RECENT RESEARCH TRENDS

Many researchers (e.g., [11,12,13]) have addressed single attributes of cloud computing security such as data integrity, authentication vulnerabilities, auditing. Others (e.g., [14,15]) provide surveys that cover specific areas of cloud security concerns and proposed solutions. The authors in [22] discuss similar cloud security issues but with deeper investigations. In [23,24], the authors present surveys on cloud security requirements such as confidentiality, integrity, transparency, availability, accountability, and assurance. In [25], the authors present a study of the different security issues of the service delivery models of the clouds. In [26], the authors discuss the security challenges devoted to the public clouds. In [27], the authors discuss the security challenges of the public clouds. In [28], the authors classify the security issues in the cloud based on the SPI (SaaS, PaaS, IaaS) cloud infrastructure and services model.

A. *Identity-based Encryption with Outsourced Revocation in Cloud Computing [16]*

The researchers were trying to tackle the critical issue of identity revocation; they introduce outsourcing computation into Identity Base Encryption IBE for the first time and propose a revocable IBE scheme in the server-aided setting. They made a scheme offloads most of the key generation related operations during key-issuing and key update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally. This goal is achieved by utilizing a novel collusion-resistant technique: they employ a hybrid private key for each user, in which an AND gate is involved to connect and bond the identity and the time component. The researchers assume that PKG is honest, and it is a point of failure because if the PKG hacked all the keys will be known.

B. *Efficient key management for IOT owner in the cloud [19]*

The researchers present security model for IOT (internet of things) with minimal cost of IOT owner client without encryption, because IOT (internet of things) owners may not want their sensitive data to be public in the cloud, and the client operated by IOT owner need the process to be faster and lightweight. To remove this issue, they propose a novel solution to minimize the access control cost for IOT owner. First, they present a security model for IOT with minimal cost of IOT owner client without encryption, in which we transfer the encryption/decryption from the client to the cloud. Second, they propose an access control model to minimize the key management cost for IOT owner. Third, they provide an update authorization method to minimize the cost dynamically. First time all data sent in clear text to the server, this can be infected by the man in the middle attack.

C. *Secure Cloud Data Computing with Third Party Auditor Control [17]*

The researchers proposed methodology provided secure, centralized control and alert system. They use the same token with distributed verification of centralized data scheme. Their approach achieves the integration of storage correctness insurance and data error localization, such as the classification of misbehaving clients and it can be controlled by the servers. It can support data updating, deletion and visualization on demand with the restrictive tokenization. The system is only used for alert only there is no action taken after the intrusion has happened.

D. *Data Integrity Proof in Cloud Storage [18]*

The researchers present a scheme that gives a confidence of data integrity in the cloud storage in which the owner of the data can check the correctness of his data in the cloud. Both cloud and the client can verify this proof and could be joined in the service level agreement. This scheme ensures that the storage on the client side is minimal which will be useful for the thin-client and small scale company. This approach did not work on the changing data

E. *Survey on secure access and storage of data in cloud computing [21]*

The researchers separate the encryption and decryption process into two cloud service provider one to Encryption / Decryption and other for Storage without the decryption Key. There is no way for the Storage service to access the users Encrypted data. Within the service Encryption / Decryption, there is no stored user data, thus eliminating the possibility that user data might be improperly disclosed. The Core Concept is consistent with the division of management authority to reduce operational risk, thus avoiding the risk of wrongful disclosure of user data.

F. *Location Based Encryption [29]*

The authors give a new method by using location based encryption. By this a new security level is added to existing security there for particular geographical regions are maintained. They can limit the data access to the particular room located on a particular floor of a particular building and with specified time frame through this method.

G. *Cloud Computing Model based on Data Classification [30]*

The author presents a framework, which allows users to encrypt their data using their key which is not known to the provider. The database is encrypted Based on the degree of confidentiality. The proposed secure cloud storage model encrypts data based on its confidentiality degree through three levels: basic, confidential and highly confidential. The solution builds on the user has to specify the confidentiality level of data and manually classify it. Data with high confidentiality level will be stored on faster media whereas data with low confidentiality are stored on slower media. Another techniques of encryption are used such as Secure Hashing Algorithm (SHA), Advanced Encryption Standard (AES), and Transport Layer Security (TLS) are used based on the security level of the data.

H. Hidden Policy Attribute-based Access Control [33]

Given a paper proposed the multiple KDD structures for key distribution management. There are some hidden techniques for security like digital signature algorithm to hidden the attribute of the user from cloud and Query based approach to hidden the access policies associated with individual files from other users. For encrypting the outsourced data, Holomorphic encryption technique is used.

I. Secure and Search data using Ranked Manner [31]

The authors suggest a technique where the trust from the service provider is not required but the security of data will be control by the data owner. It contains a tool that allows the owner of the data to decide about the access rights of his/her data, notification, and revocation if any security breaches are in place. Conventional searching techniques will improve by allowing the user to search in their files in the encrypted database with ranked keyword search.

J. Security in cloud computing [20]

The researchers separate the encryption and decryption process into two cloud service provider one to Encryption / Decryption and other for Storage i.e. Without the decryption Key, So there is no way to the Storage service to access the users Encrypted data. Within the Encryption / Decryption Service System there is no stored user data, thus eliminating the possibility that user data might be improperly disclosed. The Core Concept is consistent with the division of management authority to reduce operational risk, thus avoiding the risk of wrongful disclosure of user data.

K. Trust Management Approach for Secure and Privacy Data Access [32]

Given a method uses a BASE64 algorithm, which encodes the JAR file to secure data from attackers. The proposed work gives benefits of log files, and these log files send to data owner periodically, so he can invalidate the user and forbidden them from further access to data. The CIA framework approach provides accountability in a highly distributed fashion; usage monitoring and validation combines aspects of entry restriction for users.

IV. CONCLUSION

Security of data is a critical component in cloud computing. This paper presents the survey of different existing security measures in cloud computing and compares various parameters of security. One of the significant issue in the cloud is to provide security of data, which take back the clients to store their data in the cloud environment. In the cloud computing, there are various security challenges, but this paper discuss some of them and the techniques to prevent them which can be used to maintain the secure communication and remove the security problems. This survey is primarily done to study some problems like attacks, data loss and unauthenticated access to data as shown in table 2 and the methods to eliminate those problems.

TABLE II.
SHOWS THE COMPARATIVE STUDY OF ABOVE MENTION RESEARCH

Title	Publication/year	Strengths	Limitation
Identity-based Encryption with Outsourced Revocation in Cloud Computing	IEEE 2013	offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally	Assumption of the KU-CSPs to be honest
Secure Cloud Data Computing with Third Party Auditor Control	Springer International Publishing Switzerland 2015	provides secure centralized control and alert system by the same token with distributed verification of the centralized data scheme	Alert system in the case of unauthorized access,
Data Integrity Proof in Cloud Storage	International Journal of Emerging Technology and Advanced Engineering April 2014	Assurance of data integrity in the cloud storage in which the owner of the data can check the correctness of his data in the cloud. This proof can be agreeing upon by both cloud and the client and can be incorporated in the service level agreement.	Works only on static data not in dynamic storage
Efficient key management for IOT owner in the cloud	IEEE 2015	First, security model for IOT with minimal cost of IOT owner client without encryption Second, access control model to minimize the key management cost for IOT owner. Third, an update authorization method to minimize the cost dynamically.	Sending the client data owner first time in clear text
Security in cloud computing	International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 13 Issue 3 –MARCH 2015	Independent Encryption/Decryption Services “in cloud computing environments, users of cloud computing services will use the services of at least two cloud computing service providers, one service provider to Encryption / Decryption and other Service Provider for Storage	Study the customer database Not working in all operation in database
Survey on secure access and storage of data in cloud computing	International journal of engineering September 2015	Make comparative study between 12 paper which talk about data access and storage security in cloud computing	

REFERENCES

[1] National Institute of Standards and Technology's web site, last seen 28/12/2015.http://www.nist.gov/itl/cloud,

[2] B. Rex Cyril1, DR. S. Britto Ramesh Kumar2, July-2015Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey, International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 04 |

[3] Ruchi U. Samudre, Prof. Vaishali R. Patel, Special Issue September 2015Department of Information Technology SVM Institute of Technology Bharuch 392-001, Gujarat, India, A Survey on Secure Access and Storage of Data in Cloud Computing, International

Journal of Engineering Technology Science and Research IJETS R www.ijetsr.com ISSN 2394 – 3386 Volume 2,

[4] Gonzalez, N.; Miers, C.; Redigolo, F.; Carvalho, T.; Simplicio, M.; Naslund, M.; Pourzandi, M. 1989.A quantitative analysis of current security concerns and solutions for cloud computing. In Proceedings of the 2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), Athens, Greece, 29 November–1 December 2011; pp. 231–238.Science,

[5] Tripathi, A.; Mishra, A. Cloud computing security considerations. In Proceedings of the 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, China, 14–16 September 2011; pp. 1–5 https://doi.org/10.1109/ICSPCC.2011.6061557

[6] Jain, P.; Rane, D.; Patidar, S. 2011A survey, and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment. In Proceedings of the World Congress on Information and Communication Technologies (WICT), Mumbai, India, 11–14 December 2011; pp. 456–461.

[7] Lv, H.; Hu, Y. 20–21 August 2011Analysis and research about cloud computing security protect policy. In Proceedings of the 2011 International Conference on Intelligence Science and Information Engineering (ISIE), Wuhan, China,; pp. 214–216. https://doi.org/10.1109/ISIE.2011.16

[8] Bhardwaj, A.; Kumar, V. 22–24 December 2011Cloud security assessment and identity management. In Proceedings of the 2011 14th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh,; pp. 387–392., https://doi.org/10.1109/iccitechn.2011.6164819

[9] Mahmood, Z. 7–9 September 2011Data location and security issues in cloud computing. In Proceedings of the 2011 International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), Tirana, Albania,; pp. 49–54. https://doi.org/10.1109/EIDWT.2011.16

[10] Karnwal, T.; Sivakumar, T.; Aghila, G. 1–2 March 2012A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In Proceedings of the 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India,; pp. 1–5.

[11] Tripathi, A.; Mishra, 14–16 September 2011A. Cloud computing security considerations. In Proceedings of the 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, China; pp. 1–5. https://doi.org/10.1109/ICSPCC.2011.6061557

[12] Sengupta, S.; Kaulgud, V.; Sharma, V.S. USA, 4–9 July 2011Cloud computing security—Trends and research directions. In Proceedings of the 2011 IEEE World Congress on Services (SERVICES), Washington, DC; pp. 524–531. https://doi.org/10.1109/SERVICES.2011.20

[13] Chen, Z.; Yoon, J5–10 July 2010. IT auditing to assure a secure cloud computing. In Proceedings of the 2010 6th World Congress on Services (SERVICES-1), Miami, FL, USA,; pp. 253–259.

[14] Popovic, O.; Jovanovic, Z.; Jovanovic, N.; Popovic, R. 5–8 October 2011;A comparison and security analysis of the cloud computing software platforms. In Proceedings of the 2011 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), Nis, Serbia, Volume 2, pp. 632–634. https://doi.org/10.1109/telsks.2011.6143192

[15] Holloway, I.; Todres, L. 2003The status of method: Flexibility, consistency and coherence. Qual. Res., 3, 345–357. https://doi.org/10.1177/1468794103033004

[16] Top Threats to Cloud Computing V1.0; Cloud Security Alliance: March 2010.

[17] Grosse, E.; Howie, J.; Ransome, J.; Reavis, J.; Schmidt, S. 2010Cloud computing roundtable. IEEE Secur. Priv., 8, 17–23. https://doi.org/10.1109/MSP.2010.173

[18] Bishop, M. Computer Security: Art and Science; Addison-Wesley, 2002, MA,USA,.

[19] Leandro, M.A.P.; Nascimento, T.J.; dos Santos, D.R.; Westphall, C.M.; Westphall, C.B2012. Multitenancy authorization system with federated identity for cloud-based environments using shibboleth. In Proceedings of the Eleventh International Conference on Networks,; pp. 88–93.

[20] Sanchez, R.; Almenares, F.; Arias, P.; Diaz-Sanchez, D.; Marin, 2012A. Enhancing privacy and dynamic federation in IdM for consumer cloud computing. IEEE Trans. Consum. Electron., 58, 95–103 https://doi.org/10.1109/TCE.2012.6170060

[21] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia and Wenjing Lou, 2013 Identity-based Encryption with Outsourced Revocation in Cloud Computing, IEEE

[22] Gul, I.; ur Rehman, A.; Islam, M.H. Cloud computing security auditing. In Proceedings of 2011 The 2nd International Conference on Next Generation Information Technology (ICNIT), Gyeongju, Korea, 21–23 June 2011; pp. 143–148.

[23] Kandukuri, B.R.; Paturi, V.R.; Rakshit, 21–25 September 2009A. Cloud security issues. In Proceedings of the IEEE International Conference on Services Computing, 2009 (SCC '09), Bangalore, India,; pp. 517–520.

[24] Apoorva Rathi and Nilesh Parmar, 2014Secure Cloud Data Computing with Third Party Auditor Control, Springer International Publishing Switzerland 2015 S.C. Satapathy et al. (eds.), Proc. of the 3rd Int. Conf. on Front. of Intell. Comput. (FICTA),Vol. 2, Advances in Intelligent Systems and Computing 328, https://doi.org/10.1007/978-3-319-12012-6_17

[25] Thombare Kishor V1, Suryawanshi Nilesh D2, Patil Ganesh S3, April 2014Data Integrity Proof in Cloud Storage, International Journal of Emerging Technology and Advanced Engineering 2008 Certified Journal, Volume 4, Issue 4,),

[26] Zongmin Cui, Haitao Lv, Chao Yin, Guangyong Gao, Caixue Zhou 2015School of Information Science and Technology, Efficient key management for IOT owner in the cloud, IEEE Fifth International Conference on Big Data and Cloud Computing

[27] Shweta Mahajan#1 and Sachin Mahajan, MARCH 2015, Security in cloud computing, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 13 Issue 3.

[28] Ruchi U. Samudre1, Prof. Vaishali R. Patel2, September 2013,A Survey on Secure Access and Storage of Data in Cloud Computing, International Journal of Engineering Technology Science and Research IJETSRwww.ijetsr.com ISSN 2394 – 3386 Volume 2, Special Issue

[29] Meer Soheil Abolghasemi, Mahdi Mokarrami Sefidab, Reza Ebrahimi Atani, 2013. "Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing", IEEE conference on Advances in Computing, Communications and Informatics,

[30] Lo'aiTawalbeh,Nour S. Darwazeh, Raad S. AlQassas and Fahd AlDosari, 2015, "A Secure Cloud Computing Model based on Data Classification", ELSEVIER.

[31] Sarika Gupta Sangita Rani Satapathy Piyush Mehta Anupam Tripathy, 2012, "A Secure and Searchable Data Storage in Cloud Computing", IEEE on International Advance Computing Conference,.

[32] Mythili.K, Anandakumar.H, 2013, "Trust Management Approach for Secure and Privacy Data Access in Cloud Computing", IEEE conference on Green Computing, Communication and Conservation of Energy,

[33] M. Sowmiya, M. Adimoolam, 2013 ,"Secure Cloud Storage Model with Hidden Policy Attribute based Access Control", IEEE conference on Recent Trends in Information Technolo

[34] Rola Motawie, Mahmoud M. El Kholy, Maged Heussien, Addressing security issue in cloud computing. European Journal of Scientific Research, Volume 138 Issue 2

AUTHORS

Rola Motawie Faculty of Computers & Information, Helwan University, Cairo, EGYPT

Mahmoud M. El-Khouly., Faculty of Computers & Information, Helwan University, Cairo, EGYPT

M. Samir Abou El-Seoud The British University in Egypt (BUE), Cairo, EGYPT

Submitted 14 November 2016. Published as resubmitted by the authors on 17 December 2016.