A REVIEW ON CLOUD SECURITY ISSUES AND USAGE OF ABE MECHANISM TO SAFEGUARD HEALTH CARE DATA IN THE CLOUD

P. Karthik[1] , Dr. D.Latha[2]

[1] Research Scholar, Department of Computer Science and Engineering, Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh, India.
[2] Assistant Professor, Department of Computer Science and Engineering, Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh, India.

Abstract:
The concept of providing computing services by means of the internet on a pay-per-use basis is known as cloud computing. Many sectors like health care, education, e-commerce, and social media are using cloud computing concepts in order to provide services to their users. Several organizations use Cloud Service Providers (CSP) to support the services they offer. Extensive usage of the cloud services has resulted in storage of large amounts of data in the cloud. The most common concern for cloud users and as well as cloud service providers is the security of the data residing in the cloud. Confidentiality, Integrity and Availability of the data in cloud are the major security issues to be addressed. In this paper, we have discussed the Opportunities, Security issues, and Challenges to be addressed in the adoption and usage of cloud computing services in any organization and also the possible solutions to provide security. We have also made a review of the applications of Attribute Based Encryption (ABE) one of the efficient techniques to encrypt data before storing it in the cloud.

Keywords: Cloud computing, Security issues, Challenges in cloud computing, Attribute Based Encryption.

1. INTRODUCTION

The term ‘cloud’ means a technology that is based on the internet where the organization and managing of data happen via remote servers. The data can be textual, audio, video, or images. Cloud Computing allows customers to rent computing services such as audio streaming, video streaming, data storage and data analysis by means of internet on pay- per-use basis. It provides facility for multi sharing, quick sharing of resources, and data backup and restoration. The origin of cloud computing is based on five technologies [36]. They are Distributed Systems, Virtualization, Web 2.0, Service Orientation, Utility Computing. Mainframe Computing, Cluster Computing, Grid Computing are variations of distributed computing, Cloud Computing is said to be the successor of grid computing technology. Cloud Computing technology is being used in many sectors and the health care sector is one among them. The purpose of using cloud services in the health care sector is to store the medical data in digital form in the cloud so that it can be accessed easily from anywhere via the internet. This will help doctors, patients, hospital management and also insurance companies to interact with each other in a better way. Even though access to data through the cloud has many advantages, it also has few concerns and one major concern among them is data security. Among the encryption techniques available to safeguard cloud data, Attribute Based Encryption (ABE) is one of the efficient techniques. The remaining part of this paper is organized in the following sections. Section 2 illustrates the various security issues in cloud computing. Attribute Based Encryption algorithm is discussed section 3. In section 4 a study of the application of ABE in different sectors is done. Finally, in section 5 concluding remarks.

2. SECURITY ISSUES IN CLOUD COMPUTING

Gurudat et al., 2012 [1] discussed how the usage of the concept of cloud computing at organizations level brings more challenges and issues to be addressed that are related to security of data residing in the cloud. This is because the data in the cloud will reside on remote servers which may be geographically located at any part of the globe and will be far away from the access control of the cloud service users. In such a scenario the organization providing cloud services must have proper knowledge related to working of cloud services and how they are offered to users.

According to Kui Ren et al., 2012 [2] Cloud computing services are most widely used in the Information Technology field but privacy and security of user data residing in the cloud are major concerns. Access control, Multi Tenancy security, security overhead etc., are some of the challenges to be addressed to ensure cloud security.

Chunming Ron et al., 2012 [3] provided an overview on cloud computing and its services which is one of the efficient ways of providing computing services via the internet but security concerns in the context of threats to data in the cloud is a concern. The author has highlighted both traditional security issues and challenges related to cloud computing. Service Level Agreements (SLA) are to be specified clearly for customers and it must include agreements related to cloud security also which might attract more users to use cloud services.

Cloud computing mechanism allows users to use computing services via the internet irrespective of the location and device of the users. This has increased demand for cloud but followed by challenges related to data security. Unauthorized access, Data recovery etc., are some of the vulnerabilities of cloud which needs to be addressed. Muhammad Roman et al., 2015 [4] suggests that the same level of security is not required for all cloud services. But providing security for only high level services is not advised. So, different levels of security can be offered by providers to different applications.

Cloud computing has revolutionized the on demand computing services availability but security issues like loss of secret data of users, leakage of data, disclosement of personal data of users are the critical challenges to be addressed. Nidal Hassan Hussein et al,2016.[5] proposed a 3-layer security model. In the first layer authentication techniques are used to identify the authorized user, second layer deals with data identification and encryption, third layer deals with cryptography for transmitting data in a secured way.

Muhammad Faheem Mushtaq et al., 2017 [6] presented about services offered by cloud computing as per demand without the need for organizations to have new infrastructure, software with license etc.,. This dynamic and scalable feature of cloud computing comes with security challenges. Most of the threats can be handled by combining cryptography specially, public key infrastructure (PKI), Single-sign on (SSO), and Lightweight directory access protocol (LDAP).

Esmaeil Mehraeen et al., 2017 [13] in their work focused mainly on the challenges of cloud security to be addressed in the health care sector. The sensitive data related to the medical history of patients cannot be made available to unauthorized users. But due to the increasing demand of cloud computing services even health care organizations are moving towards cloud services but their security challenges need to be carefully considered and understood. Articles that ensure the safety of health data in the cloud are reviewed in this work. Methods like Hybrid Execution Model, VCC-SSF, sHype Hypervisor Security Architecture, Identity Management, and Resource Isolation approaches are to be implemented in cloud to safeguard health data residing in it.

Cloud computing allows organizations to do savings in terms of operational expenditure. Nalini Subramanian et al., 2018 [8] focused on the security challenges faced by cloud service providers, owner of data and user of cloud services. Challenges related to network security level, VM level security, Data Security, and Hardware level are addressed.

Srijita Basu et al.,2018 [7] discussed the interconnection that is needed between various aspects related to cloud security and listed the issues prevailing in this area for more research. In their study authors have made comparisons between various cloud schemes related to data and virtualization confidentiality, data and virtualization integrity.
Cloud computing makes possible a centralized way of storing data in the cloud which gives more control on data to cloud service providers rather than hospitals and users. In such a scenario if a hacker accesses the data from the cloud it would be dangerous for all the parties

involved in storing health data in the cloud. Yazan Al-Issa et al, 2019 [14] discussed some state-of-the-art solutions to these issues but more extensive research is needed to overcome this problem. Some existing solutions related to health data security in the cloud are following the predefined security standards like HIPAA, HITECH, ISO series. Most of the solutions offered in this paper are solve only part of the problem and are unable to provide a solution which will balance all requirements of security.

Cloud computing offers a wide variety of computing services through the internet which results in efficient and simple IT infrastructure usage, remote access from any point around the globe. Work done by Hamed Tabrizchi et al.,2020 [9] provide a new categorization of the security challenges related to cloud.

Isma Zulifqar et al., 2021 [10] have given attention to security issues of the cloud that are related to data and also discussed that encryption is a better security solution for safeguarding data in the cloud. Different types of cloud security were discussed.

Manoj Kumar Sasubilli et al.,2021 [11] in their work highlight the fire attacks that can happen on cloud data and possible solutions for it. Counter measures like DevSecOps processes, Automated application deployment and management tools, Unified security with centralized management across all services and providers etc., were suggested by the authors to overcome security issues for cloud data.

Table 1 gives a summary description of the security issues in the cloud identified and discussed by the authors mentioned above.

Authors	Security Issues
Gurudatt Kulkarni et al.	Malware injection attack problem, Flooding attack problem, Accountability check problem, Browser security, Service provider security issues.
Kui Ren et al.	Security of computation outsourcing, Access control, Trustworthy service metering, Privacy leaks in Multi Tenancy, Security Overhead.
Chunming Rong et al.	Resource location, Multi Tenancy issues, Authentication and trust of required information, System monitoring and logs, Cloud standards.
Muhammada Roman et al.	Weak authentication, Injection attacks, Storage security risks, securing communication, Weak credential reset procedure, Denial of account and Denial of services.
NidalHassan Hussein et al.	Denial of service, Networks and Internet connectivity attacks, Data confidentiality, Availability, Data breaches.
Muhammad Faheem Mushtaq et al.	Tag forgery attack, Data deletion attack, Replace attack, Pollution attack, Data leak attack.
Srijita Basu et al.	Cross scripting attacks, Metadata spoofing attack, Wrapping attack, VM elope, VM hopping.
Nalini Subramanian et al.	Communication level challenges, Computation level challenges, SLA level challenges, VM level security challenges, Hypervisor level security challenges, hardware level challenges, Data security challenges.
Hamed Tabrizchi et al.	Network related issues, Application related issues, Data storage issues, User-oriented security issues, Security policy related issues.
Isma Zulifqar et al.	Interoperability issues, Vendor Lock in, Integrity, Availability
Manoj Kumar et al.	SQL Injection Attack, Net Sniffers, Hijacking Session, Man in the Middle Attack,Flooding Attacks, Privacy Breach
Ning Zhang et al.	Data Confidentiality, Data Remanence, Data Integrity, Data Breach, Availability, Account/Service Hijacking

3. ATTRIBUTE BASED ENCRYPTION

Attribute Base Encryption (ABE) is a type of public key-based authentication scheme. It allows encryption based on attributes. The decryption of the ciphertext can be carried out only when the set the attributes of the user key matches the attributes of the ciphertext. It facilitates secure data sharing among multiple users achieving privacy and access control.

Say, we have 2 users X and Y. X wants to communicate with Y. Both X and Y has some attributes.Say Y has the following attributes:- 1. a - India (Country) 2. b - 31 (Age) 3. c

- Female (Gender) 4. d - 22/09/1992 (Date of Birth). Now to perform ABE the steps to be followed are:

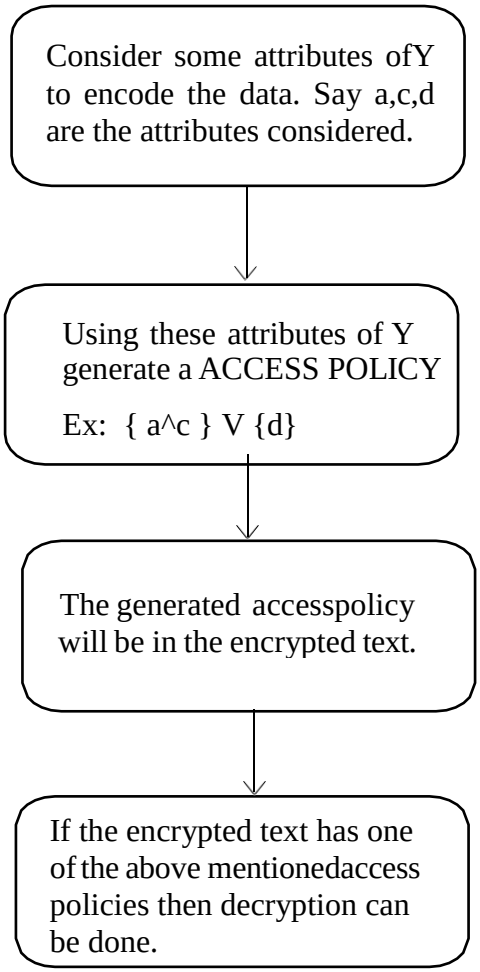

Figure-1 Attribute Based Encryption

4. AREAS OF APPLICATIONS OF ATTRIBUTE BASED ENCRYPTION

Yinghui Zhang et al., 2020 [33] have provided a review of ABE and its taxonomy has been provided. Different categories of ABE that are KP-ABE, CP-ABE have been reviewed. To analyze benefits and drawbacks of ABE schemes comparisons were made based on proposed criteria for assessment related to performance and security.

The advancements happening in the fields of network, communication technologies, computing methods, wireless medical sensors etc., have given scope for the rise of the modern medical system. In this system electronic health records (EHRs) are outsourced to third parties called cloud service providers (CSP) to store and organize them. But these CSPs are not completely trust worthy as they have security issues related to data access in the cloud. To prevent unauthorized data access this work proposes a scheme based on decentralized hierarchical ABE. In this scheme proposed Xueyan Liu et al., 2020 [32], Multiple attribute authority (AA) ABE is used to avoid bottleneck and achieve fine grained access control, also

hierarchical access tree is used to perform encryption on multiple files in single operation which saves storage and calculation load. The Global Identifier (GID) of a user is used to overcome collusion attacks of users.To ensure integrity of EHRs users can perform double verification based on convergent key and verification tag. In order to provide better decentralized properties, block chain technology can be combined with the above proposed scheme in future.

IoT data that is stored in the cloud must be provided with efficient security and authorized access mechanisms. In this paper the Jiguo Li et al.,2020 [31] have proposed a ciphertext policy attribute-based encryption (CP-ABE) which will enable fine grained access control of encrypted IoT data on cloud. A white box traceable CP-ABE scheme was proposed to address authorization center key abuse and user key abuse.

To ensure proper and efficient security for the data the cloud service providers must come with feasible mechanisms which provide an encryption method that is reliable. To realize this idea Huang et al., 2016 [34] has proposed a data collaboration scheme. In this paper the author has indicated the weakness that exists in the data collaboration scheme with hierarchical ABE that was proposed by Huang et al., 2016 [34]. This paper has shown that data confidentiality was not achieved as claimed by Huang[34].In [34] an hierarchical attribute based encryption scheme was proposed to achieve data collaboration in cloud computing. But the vulnerability that exists in this mechanism is, the cloud service provider who is a semi trusted entity will get access to users data after any unauthorized access happens on that data. But the requirement is that cloud service providers must never get to know what exactly is present in user data. According to Wei-Liang Tai et al.,2020

[30] this the confidentiality ensured in [34] is not fully achieved and also secure data collaboration scheme in cloud is still a very urgent requirement.

Storage and retrieval of data from files is performed in a secured and robust manner using the technology of cloud computing. Many researchers have proposed and developed several encryption schemes using

ABE, but most of them suffer from complexity related to communication and computation. Most of the existing techniques were encrypting the file based on a keyword, whereas with this protocol the set of patient records will be encrypted using a common attribute. In this paper the N. Deepa et al., 2020 [29] have proposed an Efficient recovery of files by using ABE mechanism from cloud. In this protocol there are 4 working mechanisms. They are:-

1. Patient key computation
2. Doctor index building computation
3. Cloud working mechanism
4. Patient report decryption This scheme will provide security against attacks like masquerade, eavesdropping etc.,,

Most of the companies have been outsourcing their data since the rapid development of cloud computing concept in providing computing services. ABE is one of the better techniques to provide security for data in the cloud. Mohammad Ali et al., 2020 [28] introduced the concept of Fully

Distributed Revocable Ciphertext Policy Hierarchical ABE (FDR-CP-HABE) scheme. This

scheme offers a high level of scalability and flexibility in user revocation and key delegation mechanisms. This scheme enables owners of data to specify access control policies of a set of attributes.This scheme was also proved to be secure based on the assumption of hardness in decisional bilinear Diffie-hellman (DBDH) problem. This scheme also achieved fine grained access control over the cipher texts that are outsourced and also against collusion attacks that are made by unauthorized users.

Cloud computing has been one of the trending technologies to store and organize large amounts of data. Various industries are using cloud services. Among them, the healthcare industry is an industry which is widely using cloud computing services. This extensive usage of cloud data leads to security issues too. J. Priyanka et al., 2020 [27] provides an analysis of various schemes under ABE which is one of the prominent techniques to provide security for cloud data.

Collaborative e-health which allows the collection and sharing of medical data related to patients and doctors is overcoming the geographical and accessibility barriers. The rapid advancements that are being made in the field of healthcare data using cloud is enabling the access of user data from anywhere in the world. ABE is one of the efficient techniques to safeguard data in the cloud. In this paper Kennedy Edemacu et al., 2019 [26] different ABE schemes that are used to safeguard health data have been surveyed.
Amit Pandey et al., 2019 [25] have proposed a Deduplication technique along with ABE in order to overcome the brute force attacks that can happen on data residing in the cloud.
In areas like Health care, military, IT etc.,.There will be a multi-level hierarchy for the data that is stored in the cloud. The CP-ABE encryption algorithm does not investigate the hierarchy that is present in the data and multi-access control is not investigated. In this paper Praveen S. Challagidad et al.,2019 [24] Multi-authority access control using ABE in the cloud.This paper contains an algorithm called RHA (Role Hierarchy Algorithm) and Hierarchy Access Structure (HAS) to protect privacy of user's data. RHA divides users of cloud into groups based on their attributes and HAS defines an access structure for multi- authority access control of the resources of cloud.

(PHR) Personal Health Records has been built as a platform for trading data related to health care. But delegation of PHR data across the cloud needs to address its security issues. In this paper Azath Mubarakali et al., 2019[23] have proposed (AHRP) Attribute Based Health Record Protection algorithm which controls secrecy, confidentiality and credibility of cloud data. Author has also shown that encryption and decryption time in case of text, document and pdf records are being reduced to certain extent.

Cloud services are provided from a remote location via the internet. But storage of data in a cloud server which we do not know anything about leads to security concerns. Encryption of cloud data is one possible solution. But traditional symmetric and asymmetric encryptions are not much suitable for this job. This is because of lack of flexibility and lack of fine grained access control. ABE is one of the better encryption techniques to provide fine grained access control and privacy for data in the cloud. In this paper the P.Praveen Kumara et al., 2018 [22]

have provided a survey on various existing ABE methods. More exploration is done on cipher text-based ABE. Author also provided a comparison of ABE schemes. According to this comparison CP-ABE scheme performs better than KP-ABE scheme as it gives full control on data to its owner.

Healthcare organizations generally face the challenge of getting adapted to the cloud environment to store and access health data due to risk of facing data breaches and data loss due to unauthorized access. Traditional EHR management systems follow a patient centric approach where data access is the responsibility of patients. This causes trouble to patients as they have to control every activity related to access of their data.

A novel ABE based authorization mechanism has been proposed by Maithilee Joshi et al., 2018 [21] which will easily delegate the service management overhead from patients to medical organizations. An attribute based field level document encryption model has been proposed by authors to restrict data access and provide security for EHRs residing on cloud.

The state-of-the-art research which is related to cloud computing has been discussed in this paper by Omar Ali et al.,2018 [20]. Review has mainly classified cloud related concepts into opportunities, applications and issues. Real time implementation of cloud computing in healthcare sector has been discussed.
Introduction of the IOT concept has provided many uses to people in their daily lives. Health care sector is also one of those sectors which benefited from IOT applications. Tasks like electronic medical billing, devices related to health monitoring etc., are made available in an efficient way in health organizations.To use IOT devices in a better way they are combined with cloud computing mechanisms so that all these services can be provided as on demand services. But privacy of the data residing in the cloud is a major challenge to be addressed. A review has been provided in this paper by Afsheen Ahmed et al., 2018 [19] which highlights the top threats that may cause danger to IOT and cloud data.

Maithilee Joshi et al., 2018 [18] have proposed a novel attribute based authorization mechanism where secured access for electronic health records residing in the cloud is delegated properly between medical organizations and patients.The system proposed was organized in 4 levels namely cloud service provider, ABE and Key management module, access broker.To automate access policies a knowledge graph has been developed that will specify roles and attributes of different stakeholders of the health care organization.

Knowledge sharing and resource sharing via the internet are 2 major issues faced by users due to the presence of malicious intruders and hackers. In this paper a secure access control has been proposed by Suyel Namasudra et al., 2017 [17] using ABE, DHT, IDTRE. Data is encrypted first using user attributes and IDTRE algorithm will encrypt the decryption key and embedded with cipher text and this cipher text will be uploaded into DHT and stored in cloud servers.

Qinlong Huang et al., 2016 [16] have proposed a collaboration scheme for writing encrypted

data in the cloud using ABE and ABS. To prevent the burden of key management on attribute authority a full delegation mechanism has been proposed which is based on HABE.

To safeguard the data, encrypting it before storing in the cloud is the possible solution. Out of these encrypting techniques, a searchable CP-ABE technique with attribute revocation has been suggested by Jiguo Li et al., 2015 [15]. Here access structures are partially hidden so that users at the receiving end cannot retrieve the sensitive information residing in cipher text. Based on DBDH assumption and DL assumption, security of this scheme has been proved.

The following table gives the summary of applications of ABE schemes in different sectors.

Table - 2: Summary of Application of ABE mechanism in different sectors

SN O	Reference	Technique	Area/Sector Where ABE was used	Remarks
1	Xueyan Liu et al.,[32]	Decentralized HABE	Health care	The confidentiality of shared EHRs is improved by a hidden access policy. The Key escrow attack of dishonest attribute authority is avoided.
2	JiguoLi et al.,[31]	CP-ABE	Cloud IoT	A ciphertext policy hiding ABE scheme was proposed. This scheme is secure against the chosen plaintext attack.
3	Wei-Liang Tai et al.,[30]	HABE	Analysis on Data Collaboration Scheme proposed by Huang et al.,2017 [34]	Data collaboration scheme is still an important cloud security issue that is to be addressed.
4	N.Deepa et al.,[29]	ERFC	Health care	ERFC takes less computation time and also a semi trusted cloud segment was developed to increase security for retrieving encrypted files from the access tree.

5	Mohammad Ali et al.,[28]	FDR-CP-HABE	Data outsourcing into cloud servers	The proposed scheme provides high flexibility levels and scalability in user revocation mechanism and key delegation. Also this scheme enables the data owners to impose access control policies on a set of attributes.
6	Praveen.S.C halla gidad et al.,[24]	ABE	Cloud Storage	RHA and Hierarchy Access Structure was proposed to achieve privacy, protection,multi-authority and fine grained access
				control on user's data in cloud.
7	Azath Mubara kali et al.,[23]	AHRP Algorithm	Health care Services	AHRP algorithm was proposed to provide confidentiality,credibility and secrecy for the information access in the cloud.
8	Maithilee Joshi et al.,[21]	ABE	Secure Access to EHR Systems	An Attribute based, field level document encryption was developed to manage secured data access of EHRs in the cloud.
9	Maithilee Joshi et al.,[18]	Delegated Authorization Framework using ABE	Health care	The mechanism proposed in this work allows access to patient records in a delegated manner based on policies of organization and also service management overhead is transferred from patient to medical organization.
10	Amit Pandey et al.,[25]	Deduplication wit h ABE	E-Health care systems	This scheme overcomes the problem of repeated data in the database environment.

5. CONCLUSION & FUTURE WORK

Cloud Computing became enormously popular in the provision of computing services through the internet. Various sectors are using these services and the healthcare sector is one of them.

The concept of storing and organizing Electronic Health Records(EHRs) in the cloud has many advantages that includes quick and anytime anywhere interaction between doctors and patients. Along with this there is also an issue of privacy and security for data residing in the cloud. Unauthorized access of the EHRs will be dangerous to all sets of people who are involved in it. To avoid this and provide security for data residing in cloud (ABE) Attribute Based Encryption is one of the efficient techniques. Here user data is encrypted before it is stored in the cloud. In this paper, we have reviewed research papers that covered various security issues involved in the organization of data in the cloud, the importance of digitizing health care data and different algorithms of ABE which are used for encrypting data. In future work we will come up with a better version of the existing ABE algorithms that will encrypt the data in a more efficient way before storing it in the cloud.

6. REFERENCES

[1] Gurudatt Kulkarni1, Nikita Chavan, Ruchira Chandorkar, Rajnikant Palwe, Cloud Security Challenges, ,2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA)

[2] Kui Ren, Cong Wang, and Qian Wang • Illinois Institute of Technology, Security Challenges for the Public Cloud, , JANUARY/FEBRUARY 2012 1089- 7801/12/$31.00 © 2012 IEEE ,Published by the IEEE Computer Society

[3] Chunming Rong a , Son T. Nguyen a, Martin Gilje Jaatun b,Computers and Electrical Engineering, Beyond lightning: A survey on security challenges in cloud computing , 2012 Elsevier Ltd. All rights reserved. http://dx.doi.org/10.1016/j.compeleceng.2012.04.015

[4] Roman, M. & Khan, S. (2015). Cloud Computing Security: A Survey, Global Journal on Technology [Online]. 08, pp 15-28. Available from: http://awer- center.org/gjt/

[5] Nidal Hassan Hussein Ahmed Khalid, A survey of Cloud Computing Security challenges and solutions, ,International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016, https://sites.google.com/site/ijcsis/
ISSN 1947-5500

[6] Faheem Mushtaq1 , Urooj Akram1 , Irfan Khan2, Sundas Naqeeb Khan1 , Asim Shahzad1 , Arif Ullah1, Cloud Computing Environment and Security Challenges: A Review Muhammad , (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 10, 2017

[7] Srijita Basu, Arjun Bardhan, Koyal Gupta,Payel Saha, Mahasweta Pal,Manjima Bose, Kaushik Basu,Saunak Chaudhury, Pritika Sarkar,Cloud Computing Security Challenges & Solutions-A Survey, , 978-1-5386-4649-6/18/$31.00 ©2018 IEEE

[8] Nalini Subramanian, Andrews Jeyaraj, Recent security challenges in cloud computing , Computers and Electrical Engineering 71 (2018) 28–420045-7906/ © 2018 Elsevier Ltd. All rights reserved. https://doi.org/10.1016/j.compeleceng.2018.06.006

[9] Hamed Tabrizchi , Marjan Kuchaki Rafsanjani, A survey on security challenges in cloud computing: issues, threats, and solutions © Springer Science+Business Media, LLC, part of Springer Nature 2020.The Journal of Supercomputing https://doi.org/10.1007/s11227-020-03213-1

[10] Isma Zulifqar, Sadia Anayat, Imtiaz Khara, A Review of Data Security Challenges and their Solutions in Cloud Computing, I.J. Information Engineering and Electronic Business,

2021, 3, 30-38 Published Online June 2021 in MECS (http://www.mecs- press.org/) DOI: 10.5815/ijieeb.2021.03.04

[11] Manoj Kumar Sasubilli, Venkateswarlu R, Cloud Computing Security Challenges, Threats and Vulnerabilities, , Proceedings of the Sixth International Conference on Inventive Computation Technologies [ICICT 2021] IEEE Xplore Part Number: CFP21F70-ART; ISBN: 978-1-7281-8501-9

[12] Ning Zhang, An Overview of Advantages and Security Challenges of Cloud Computing, International Journal of Computer Science and Mobile Computing, A Monthly Journal of Computer Science and Information Technology, IJCSMC, Vol. 10, Issue. 1, January 2021

[13] Esmaeil Mehraeen , Marjan Ghazisaeedi, Jebraeil Farzi & Saghar Mirshekari, Security Challenges in Healthcare Cloud Computing: A Systematic Review, Global Journal of Health Science; Vol. 9, No. 3; 2017 ISSN 1916-9736 E-ISSN 1916-9744 Published by Canadian Center of Science and Education. doi:10.5539/gjhs.v9n3p157 URL: http://dx.doi.org/10.5539/gjhs.v9n3p157

[14] Yazan Al-Issa, Mohammad Ashraf Ottom , and Ahmed Tamrawi, eHealth Cloud Security Challenges: A Survey, , Hindawi Journal of Healthcare Engineering Volume 2019, Article ID 7516035, 15 pages https://doi.org/10.1155/2019/7516035

[15] Jiguo Li, Yuerong Shi and Yichen Zhang,Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage,, INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS Int. J. Commun. Syst. (2015) Published onlinein Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2942.

[16] Qinlong Huang, Yixian Yang,Mansuo Shen, Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing http://dx.doi.org/10.1016/j.future.2016.09.021 0167-739X/© 2016 Elsevier B.V. All rights reserved.Future Generation Computer Systems journal homepage: www.elsevier.com/locate/fgcs

[17] Suyel Namasudra, An improved attribute-based encryption technique towards the data security in cloud computing Concurrency Computat: Pract Exper. 2017;e4364. https://doi.org/10.1002/cpe.4364, wileyonlinelibrary.com/journal/cpe Copyright © 2017 John Wiley & Sons, Ltd.

[18] Maithilee Joshi, Karuna P. Joshi and Tim Finin, Delegated Authorization Framework for EHR Services using Attribute Based Encryption, Citation information: DOI 10.1109/TSC.2019.2917438, IEEE Transactions on Services Computing IEEE

TRANSACTIONS ON SERVICES COMPUTING, 2018

[19] Afsheen Ahmed & Rabia Latif & Seemab Latif & Haider Abbas & Farrukh Aslam Khan, Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment: A Systematic Literature Review,# Springer Science+Business Media, LLC, part of Springer Nature 2018, https://doi.org/10.1007/s11042-017-5540-x

[20] Omar Ali , Anup Shresthaa,∗ , Jeffrey Soara , Samuel Fosso Wambab, , Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review,International Journal of Information Management 43 (2018) 146–1580268- 4012/ Crown Copyright © 2018 Published by Elsevier Ltd. All rights reserved. https://doi.org/10.1016/j.ijinfomgt.2018.07.009

[21] Maithilee Joshi, Karuna P. Joshi and Tim Finin, Attribute Based Encryption for Secure Access to Cloud Based EHR Systems, 2018 IEEE 11th International Conference on Cloud Computing, 2159-6190/18/$31.00 ©2018 IEEE DOI 10.1109/CLOUD.2018.00139

[22] Kumar, P.P., Kumar, P.S., Alphonse, P.J.A., Attribute based encryption in cloud computing: A survey, gap analysis, and future directions, Journal of Network and Computer Applications (2018), doi: 10.1016/j.jnca.2018.02.009.

[23] Azath Mubarakali & M. Ashwin & Dinesh Mavaluru & A. Dinesh Kumar ,Design an attribute based health record protection algorithm for healthcare services in cloud Environment, Springer Science+Business Media, LLC, part of Springer Nature 2019, https://doi.org/10.1007/s11042-019-7494-7

[24] Praveen S. Challagidada , Mahantesh N. Birje, Efficient Multi-authority Access Control using Attribute-based Encryption in Cloud Storage, 1877-0509 © 2020 The Authors. Published by Elsevier B.V. International Conference on Computational Intelligence and Data Science (ICCIDS 2019).10.1016/j.procs.2020.03.423

[25] Amit Pandey , Gyan Prakash, Deduplication with Attribute Based Encryption in E-Health Care Systems, International Journal of MC Square Scientific Research Vol.11, No.4,2019

[26] KENNEDY EDEMACU, HUNG KOOK PARK, BEAKCHEOL JANG , AND JONG WOOK KIM, Privacy Provision in Collaborative Ehealth With Attribute- Based Encryption: Survey, Challenges and Future Directions, IEEE Access, Digital Object Identifier 10.1109/ACCESS.2019.2925390

[27] J. Priyanka, M. Ramakrishnan, Performance Analysis of Attribute based Encryption and Cloud Health data Security,, Proceedings of the International Conference on Intelligent

Computing and Control Systems (ICICCS 2020) IEEE Xplore Part Number:CFP20K74-ART; ISBN: 978-1-7281-4876-2

[28] Mohammad Ali , Javad Mohajeri , Mohammad-Reza Sadeghi , Ximeng Liuc, A fully distributed hierarchical attribute-based encryption scheme,0304-3975/© 2020 Published by Elsevier B.V. , https://doi.org/10.1016/j.tcs.2020.02.030

[29] N. Deepa·,P. Pandiaraja, E healthcare data privacy preserving efficient file retrieval from the cloud service provider using attribute based file encryption, Journal of Ambient Intelligence and Humanized Computing, https://doi.org/10.1007/s12652- 020-01911-5

[30] Wei-Liang Tai, Ya-Fen Chang, and Wen-Hsin Huang, (Corresponding author: Ya-Fen Chang), Security Analyses of a Data Collaboration Scheme with Hierarchical Attribute-based Encryption in Cloud Computing, International Journal of Network Security, Vol.22, No.2, PP.212-217, Mar. 2020 (DOI: 10.6633/IJNS.202003 22(2).04)

[31] Yichen Zhang, Jianting Ning, Xinyi Huang, Geong Sen Poh, and Debang Wang, Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT,Jiguo Li, IEEE Transactions on Cloud Computing,2168-7161 (c) 2019 IEEE.
DOI 10.1109/TCC.2020.2975184

[32] XUEYAN LIU , XIAOTAO YANG, YUKUN LUO, LI WANG1, AND QIANG ZHANG, Anonymous Electronic Health Record Sharing Scheme Based on Decentralized Hierarchical Attribute-Based Encryption in Cloud Environment, IEEE Access Digital Object Identifier 10.1109/ACCESS.2020.3035468

[33] YINGHUI ZHANG, ROBERT H. DENG, SHENGMIN XU, and JIANFEI SUN,QI LI, DONG ZHENG, Attribute-based Encryption for Cloud Computing Access Control: A Survey, © 2020 Association for Computing Machinery. 0360 0300/2020/08-ART83 $15.00, ACM Computing Surveys, Vol. 53, No. 4, Article 83. Publication date: August 2020. https://doi.org/10.1145/3398036

[34] Qinlong Huang , Yixian Yang, Mansuo Shen, Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing http://dx.doi.org/10.1016/j.future.2016.09.021 0167-739X/© 2016 Elsevier B.V. All rights reserved.