RESEARCH ARTICLE OPEN ACCESS

Investigation on the Attribute Based Encryption for Secure Data Access in Cloud

Dr.K.Sai Manoj, Ms. K. Mrudula, Mrs K.Maanasa, K.Phani Srinivas
CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer,
Director, Innogeecks technologies,
Research Scholar, Acharya Nagarjuna University, Guntur Dist, Editor and Reviewer, Head R&D,
Associate Professor Amrita Sai Institute of Science and Technology
Vijayawada
AP – India

ABSTRACT

Cloud computing is a progressive computing worldview, which empowers adaptable, on request, and ease use of Information Technology assets. However, the information transmitted to some cloud servers, and various protection concerns are arising out of it. Different plans given the property-based encryption have been proposed to secure the Cloud Storage. In any case, most work spotlights on the information substance security and the get to control, while less consideration towards the benefit control and the character protection. In this paper, a semi-anonymous benefit control conspires AnonyControl to address the information protection, as well as the client character security in existing access control plans. AnonyControl decentralizes the central authority to restrain the character spillage and accordingly accomplishes semi-anonymity. Furthermore, it likewise sums up the document get to control to the benefit control, by which advantages of all operations on the cloud information managed in a fine-grained way. Along these lines, display the AnonyControl-F, which ultimately keeps the character spillage and accomplish the full secrecy. Our security assessment demonstrates that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie-Hellman presumption, and our execution assessment shows the attainability of our plans.

Keywords:-: Anonymity, multi-authority, attribute-based encryption**.**

I. INTRODUCTION

Cloud computing set up is a definite, advantageous, on request, arrange access to a Mutual pool of configurable computing assets which could be quickly arranged and discharged. With essential endeavors for administration or specialist organization association. Its primary Target is to convey quick, secure, helpful information stockpiling and net computing, Management, with all computing assets, imagine as administrations and conveyed over the Internet. Various computing ideas and advances could be used along with cloud computing to fulfill the computing needs of clients, it gives reasonable business applications online through Web programs, while their information and programming are kept away on the servers. It is an approach that could be used to boost the extension or venture up capacities vigorously without putting resources into the new system, sustenance modern workforce or Permitting new programming. It gives the enormous ability to information and quick computing To clients over the web. Information security is one of the parts of the cloud which helps clients From utilizing cloud administrations. There is dread between the information proprietor particularly in strong associations that their potential information abuses by the cloud supplier without their insight. Data security of the clients is possible by utilizing the idea of virtual private Systems, firewalls, and by upholding other security arrangements inside its boundaries. Security is an essential module in any cloud computing environment since it is crucial To guarantee that lone approved could be authorized, and ensured conduct acknowledged. Any Safe and protection contradiction is fundamental and can create pivotal outcomes. When the strict Directions and arrangements are against safety in the cloud, increasingly workforce will feel Spare to receive computing. A customer might be the person or a significant association; However, all are having the same concern, i.e., data security, so data security is the sad outcome. Data security at various levels is the crucial matter of this innovation, grouped into two Classifications: security at the external level and security at internal level. Security at external Level says that data are insecure contradicted to an outsider, cloud service provider or system Interloper. Security at internal level means that data is made available to approved clients or Representative of an association. A secure server gives an ensured establishment to facilitating web applications, and web Server setup assumes an essential part of web application's security. The gravely designed server Can prompt for unapproved

get. An overlooked share can give an advantageous indirect access, while an unused port is an assailant's front entryway. Ignored client records can allow an Aggressor to sneak past resistances unnoticed. Understanding dangers of the web server and Methods to recognize proper countermeasures grants to foresee many assaults and frustrate the Steadily developing quantities of assailants. This system gives bi-directional encryption of Correspondences between a customer and server, which ensures against listening in and messing With and additionally manufacturing the communication. Progressively, this provides a sensible Certification that one speaks with unequivocally

II. PROBLEM STATEMENT

Various layouts based on attribute based-encryption are proposed to secure the cloud storage, but most of the target on the data content privacy and the access control, while less attention given to the privilege control and the identity privacy. Data sharing in the cloud is very feeble to cyber-attacks since data stored on cloud servers, and multiple users access data from
Unknown servers, resulting in Data security and privacy as critical issues for remote data storage. This uncertainty of Data Privacy and User Integrity is the foundation of the study. Nature and Significance of the Problem A secure user enforced data access control mechanism is available to the cloud users to give them the flexibility to outsource sensitive data for cloud storage. With the need of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption
system with a fine-grained access control to encrypt outsourced data. In this paper, the proposed solution guarantees a secured data exchange between the client and target server which cannot be accessed by an unauthenticated user. Secure Server Plus application has twofold login security. That is, after signing into the application client gets a mystery key on his enrolled Gmail id. The key entered on the fly up box showed in the wake of signing into SSP Application. This application has two functions, Encryption, and Decryption. Encryption is the usefulness in which the record sent over Gmail and divided into four chunks of in byte arrangement and afterward encoded utilizing various encryption calculations. After Encryption, documents delivered to the beneficiary through Gmail. At the recipient end, At the recipient end, the user downloads the documents and uses SSP Application data in the records is scrambled and consolidated.

III. OBJECTIVE OF THIS RESEARCH PAPER

This project aims to set up a secure layer for storing, retrieving and transfer of data across multiple users with Data Privacy, Content Privacy and User Identity intact. Proposed secrecy Control to let cloud servers to control clients' get to help without knowing their character data. The advocated plans can secure client's protection against every single expert. Halfway datarevealed in secrecy Control and no evidence showed in secrecy Control-F. The proposed plans are tolerant against specialist bargain, and trading off up to (N −2) experts do not cut the entire system down. Given formal investigation of security and execution to show attainability of the plan obscurity Control and obscurity Control-F. Initially, actualized the whole toolbox of a multi-specialist based encryption conspire secrecy Control and namelessness Control-F.

IV. LIMITATION OF THIS RESEARCH PAPER

The research has some limitation as follows: Difficult to user revocation. Whenever an owner wants to change the access right of the user, it is not possible to do efficiently. Decryption keys only support user attributes which are organized logically as a single set, so users can just use all possible combinations of characteristics in a unique set issued in their keys to satisfy the Policies.

V. DEFINITION OF TERMS

ABE. Attribute-Based Encryption: It is a Public Key encryption. Here the secret key of the user and cipher text depend upon the attributes, i.e., on the address of the user or the kind of subscription attributes unique to the user. The two flavors of ABE are(KP-ABE)–Key Policy ABE: Here the Cipher Text along with the set of attributes and private key along with monotonic access structure like a tree, which describes the user's identity (e.g., IIT And Ph.D. or Masters). A user can decrypt the cipher text if and only if the access tree in his private key satisfies the attributes of the cipher text. The main drawback of KP-ABE is every time the user encrypts data the system must reissue the private keys to gain access to the file. (CP-ABE)–Cipher text ABE: Here Cipher Text created with an access structure, which specifies the encryption policy and private keys generated according to user's attributes. A user can decrypt the cipher text if and only if attributes in the user's private key satisfy the

access tree specified in the cipher text. Here the private keys are not re-issued every time**.**

VI. BACKGROUND RELATED TO THE PROBLEM

Introducing bi-linear maps, give formal definitions for access structures and relevant background on Linear Secret Sharing Schemes (LSSS). Then the algorithms and security definitions of Cipher text-Policy Attribute-Based Encryption with identity-based user revocation.

VII. LITERATURE RELATED TO THE PROBLEM

According to Park (2011), the Computing service provider cannot be trusted entirely because of data security reasons, the danger of data safety and infringement of protection variables are considered. Particularly, ensuring data classification required to take care of these issues, Yu, Wang, Ren, and Lou (2010) proposed to conspire which guarantees data classification and fine-grained get to control. Be that as it may, data secrecy which was damaged by intrigue assault of repudiated client and cloud server. To take care of this issue, ensured data secrecy by putting away and separating data document into header and body. What's more, the strategy for an assignment about the entire or fractional message as indicated by delegates' consistent quality towards delegate utilizing sort based re-encryption is determined. According to Yang and Ziaohua (2014), Cipher text-Policy Attribute-based Encryption (CP-ABE) is a promising strategy for getting to control of scrambled data, which requires a trusted expert to deal with every one of the characteristics and disseminates enters in the system. In multi-specialist computing storage systems, the clients' qualities originated from various spaces each of which is overseen by another expert. In any case, existing CP-ABE plans cannot be connected explicitly to data get to control for multi-specialist computing storage systems, because of the wastefulness of scrambling and repudiation. In this part, the proposed DACMACS (Data Access Control for Multi-Authority Cloud Storage), a robust and secure data get to control conspire with effective scrambling and disavowal. According to Yu et al. (2010), Cloud computing is an arising computing model in which resources of the computing infrastructure is offered as services over the Internet. As promising as it is, this change also brings with it many new challenges for data security and access control when users outsource delicate information for sharing on cloud servers, which are not found within the same trusted domain as data owners. While trying to keep this sensitive, user data confidential from entrusted and prying servers, already existing solutions usually apply cryptographic methods by revealing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for the primary distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-granularity, scalability, and data confidentiality of access control remains unresolved. This paper addresses this challenging open issue by, on the one hand, defining and enforcing access policies based on data attributes, and, on the contrary, allowing the data owner to delegate most of the computation tasks involved in fine-grained facts to access control to entrusted cloud servers without disclosing the underlying data contents. This goal is achieved by putting in place the usage of techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has main properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed system is highly efficient and provably secure under existing security models. According to Le, Yu, Zheng, Ren, and Lou (2013), Personal health record (PHR) is a rising patient-centric model of health information exchange, which is often outsourced to kept at a third-party, such as cloud providers. However, there have been grave privacy concerns as personal health information could be exposed to those third-party servers and unauthorized parties. To assure the patients' control access over to their PHRs, it is a promising method to encrypt the PHRs before outsourcing. Problems which includes risks of privacy exposure, scalability in the central management, flexible access, and efficient user revocation, have remained an essential challenge toward attaining fine-grained, cryptographically enforced data access control. In this paper, a novel patient-centric framework and group of mechanisms for facts access manipulate to PHRs saved in semi-relied on servers. To attain fine-grained and Scalable data access control for PHRs, applications attribute-based encryption (ABE) strategies to encrypt every patient's PHR file. Different from preceding works in secure data outsourcing, the focus is on the multiple data owner situations and divides the users in the PHR system into numerous security domains that substantially reduces the key management complexity for owners and users. A high degree of patient privacy guaranteed simultaneously by exploiting multi-authority ABE. Our scheme additionally enables dynamic change of

access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency eventualities. Significant analytical and experimental results are represented which show the security, scalability, and efficiency of our proposed scheme. According to Li, Yu, Ren, and Lou (2010), online personal health record (PHR) enables patients to manage their medical records in a centralized way, which greatly facilitates the storage, access, and sharing of personal health data. With the uprising of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, to enjoy the elastic resources and cut the effective cost. However, by storing PHRs in the cloud, the patients lose physical control to their health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Under encryption, it is challenging to do fine-grained access control to PHR data in a scalable and efficient way. For each patient, the PHR data should be encrypted so that it is expandable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is essential to cut the critical distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios. According to Park (2011),Cloud computing service provider cannot be trusted due to data security reasons, the risk of data safety and violation of privacy factors accounted. Especially, guaranteeing data confidentiality needed. To solve these problems, Yu et al. (2010) Proposed scheme which ensures data confidentiality and fine-grained access control. However, data confidentiality violated by collision attack of revoked user and cloud server. To solve this problem, guaranteed data confidentiality by storing and dividing data file into header and body. Also, the method of selective delegation about the or partial message according to delegator's reliability towards delegate using type-based re-encryption was specified.As it is clear from the risks associated with cloud storage, it is paramount to direct central focus on strategic information security for cloud-stored data. Most multinational technology company, set to have many security challenges especially those emanating from cyber-attacks. Therefore, the corporations should adopt workable strategic information security by controlling the risks. These strategies involve taking adequate protection mechanisms for an information system, address the issue of the relationship between people and safety, the legal and ethical matters about security as well as employing efficient security principle that will help in control, mitigation and recovering from security threats.

VIII. CONCLUSION

This paper presents a semi-mysterious property based benefit control plot AnonyControl, and an entirely anonymous characteristic based benefit control conspires AnonyControl-F address the client protection issue in a computing storage server. By utilizing the many experts in the computing system, our proposed plans do not just fine-grained benefit control additionally character obscurity while controlling benefit control given clients' character data. More vitally, our system can acknowledge up to N-22 expert bargain, which is exceedingly ideal particularly in Internet-based computing condition. Likewise, immediate point-by-point security and execution investigation which demonstrates that AnonyControl both proficient and secure for cloud capacity system. One of the up and coming future works is to present the proficient client denial instrument on top of our mysterious ABE. Supporting client renouncement is an essential issue in the original application, and this is an impressive test the application of ABE plans (Yu et al., 2010). Making our plans versatile with existing ABE plans bolster proficient client denial is one of our future works.

REFERENCES

[1]. A Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli,International Journal of Computer Science and Mobile Computing - Vol.6 Issue.11, November- 2017, pg. 7-11

[2]. Cloud Security Risk Factors and Security Issues in current trends research paper by Dr.K.Sai Manoj accepted and Presented in Scopus Based 2nd International Conference on Materials, Applied physics and Engineering (ICMAE 2018) at Indore. Proceedings of the 2018 First international conference on Materials, Applied physics and Engineering. After Clear scientific check this Paper was already Promoted to Science Publication Corporation.

[3]. Literature survey on the destruction of attaches with MH HOP to HOP to HOP-AODV Routing Protocol in Vehicular Ad-hoc Network, Dr.K.Sai Manoj, Mrudula Kudaravalli , © December 2017 | IJIRT | Volume 4 Issue 7 | ISSN: 2349-6002

[4]. I. Hedenfalk, D. Duggan, Y. Chen, M. Radmacher, M. Bittner, R. Simon, P. Meltzer, B. Gusterson, M. Esteller, O. P. Kallioniemi, B. Wilfond, A. Borg, and J. Trent, "Gene Expression profiles in hereditary breast cancer," N Engl J Med, vol. 344, no. 8, February 2001, pp. :539–548.

[5]. Li, M., Schucheng, Y., Ren, K., & Lou W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings.International Conference on Security and Privacy in Communication Systems. Heidelberg, Germany: Springer Publications.

[6]. Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In International Conference on Security and Privacy in Communication Systems (pp. 89

[7]. Berlin, Germany: Springer Verlag. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems, 24(1), 131-143.

[8]. Mishra, D. P., Mishra, R., & Tripathy, A. (2011). A privacy preserving repository for securing data across the cloud. In Proceedings of the third International Conference on Electronic Computer Technology (pp. 6-10). Avizienis A, Laprie J C, Randell B and Landwehr C 2004

[9]. Yang, K., & Ziaohua, J. (2014). DAC-MACS: Effective data access control for multi-authority cloud storage systems. Security for Cloud Storage Systems, 59-83. New York, NY: Springer Publications.

AUTHORS' CONTRIBUTIONS

The other of the paper do all the work, the environment for research work are done by my best of my knowledge and supporting my family members.

ACKNOWLEDGEMENTS

This paper heartily dedicated to beloved Honorable Secretary and Correspondent Sri. K.Ram Mohan Garu, & Smt.K.Bhavani Devi Garu Amrita Sai Institute of science and technology. Also to all the respected Amrita Sai Management members. Our special thanks to the Innogeecks technologies, Vijayawada for their technical support in all the aspects.

Dr. SAI MANOJ KUDARAVALLI, is a Founder and CEO in Innogeecks™ Technologies, Vijayawada and also Worked as Professor Amrita Sai Institute of Science and Technology since 2014, and he played vital key role in Fidelity Investments as a Senior Business Analyst for 4.4 years in Business Analytics & Research and worked as Project Engineer in Wipro Technologies for 1.5 years, He got more than 10 years of experiences in financial services, IT services and education domain.

He was completed Bachelor of Technology in Mechanical Engineering from Amritha University, Coimatore.He is completed Master of Technology in Information Technology from IIIT- Bangalore. He holds Doctor of Philosophy (Ph.D) in Cloud computing arena from Kanpur University, India.
He was certified in Microsoft Certified Technology Specialist (MCTS) from Microsoft Corporation, and Certified Ethical Hacker v9 (CEH), and "Paul Harris Fellow" recognition by Rotary International. He is Published more than 10 research papers in various reputed International and national research journals/conferences/ Magazines. He attended 4 national level workshops and participated 3 international workshops; He is also a charted Engineer (Computer Science) from IEI. He is active member of IEEE, ACM, IEI, SHRM, NEN – Bangalore Chapter, HR Sangham – Chennai, CCICI (Cloud Computing), Rotary International Services.He is acting as a reviewer for the High Standard Journals such as Springer,IE,Scopus etc.

Ms. K.Mrudula working with an Assistant Professor in CSE Dept from Amrita Sai Institute of Science and Technology. She was completed M.Tech from IIIT-Hyderabad .She got more than 6 years of experience in Teaching. She published more than 5 research papers in various International and national research journals. She attended 2 FDP, and 1 workshop.

Mrs.K.Maanasa worked as HR manager in Jaya lakshmi Powercorp Ltd for a Period of 6 years after completing her M.B.A from RVR&JC college of Engineering. She is currently Pursuing her doctorate (Ph.d) in Development of Framework for Tourism Promotion in AP and ICT Integration from Nagarjuna University.

K.PHANI SRINIVAS working as an Associate Professor and Head of Research and Development and He Had Five Years of Industrial Experience as a team Leader in the research areas of Embedded Systems and Tele-Communications and also He is Having 12 Years of Experience in Academics, Research and

Administrative reports. He received several research awards like Best Engineer Award, Best Teacher Award and Best Research Paper Award. Also He is acting as an Editor/Reviewer for so many top international Journals.

The Focus of His research work is Design of Patch antennas which are Suitable for Defense and Space Based Applications. He received appreciation award in various National and International Conferences. He received Best Coordinator Certificates from IUCEE,IIT ROORKEE,IIT Bhubneswar, NCAT,ELAT and INTEL. He attended WIPRO training Program. He completed one Joint research Program with IIT Kharagpur.He Organized various student level Competitions, workshops, Faculty Development Programs, Guest lectures, Orientation Programs, Subject Based Seminars with scientists and Academicians. He is doing research work under the valuable Directions of Eminent Scientists. He had done technical Discussions with experts at Space Station, Antenna Research Lab, Radar station. He Published research articles in Various Scopus International Journals.He is an active Editor/Reviewer for so many reputed international journals.