International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

A Survey on Efficacious Data Transit System for Mobile Cloud Computing

Mr. V. Balamurugan[1], K. Abinaya[2], P. Inba Devi[3], C. Nivedita[4]
[1 ,2, 3, 4]*Computer Science and Engineering, S.A. Engineering College*

Abstract: ***In mobile cloud computing the data to be shared from the mobile devices to the cloud contains only the data confidentiality, authentication has been provided to the data which is being shared from the mobile. Thus for the security of the data the algorithms which are used is CP-ABE which is Cipher Text Attribute Based Encryption. The LDSS light weight data sharing scheme which uses the CP-ABE. And also the pseudo random permutation based system is also being used to give the security to the data which is being stored in the cloud. And also the light weight identity based authenticated data sharing protocols are used to resist chosen cipher text attack.***
Keywords: cloud computing, CP-ABE, LDSS, TPA, accessibility.

I. INTRODUCTION

Cloud computing is the computing that relies on shared computing resources instead of having a local servers or personal devices to handle or manage the applications. The services are delivered and used over internet and paid by cloud customer as needed or pay per use business model. Cloud computing can be defined accordingly to its five main characteristic: on demand self services, broad-based network access, resource pooling, rapid elasticity and measured services.

The cloud has become more popular among several business due to its numerous benefits. Business can outsource their data to cloud service providers this can be cost effective since it gives high storage capacity and high data processing speed. Cloud computing is important fot information technology applications and though it has some issues to be solved for the user. Data security is one of the most important barriers to the usage of cloud and it also accompany issues like compliance, privacy, trust, legal matters. Thus goal of the cloud computing is to provide a security, integrity, confidentiality of data stored in the cloud. Data confidentiality is also the important from user ‘s view because user store private data in the cloud. Data confidentiality should be maintained by the cloud reliability and trustworthiness. Data authentication and access control methods are to be used to ensure data confidentiality.

Android is a mobile operating system developed by the Google and basically it is based on the modified version of Linux Kernel and other open source software. And the android has been used in the touch screen mobile phones. Now a days the android has been used in the television , android auto for cars, wrist watches, tablets, cameras.

The features of android are interface, application, memory management. Interface which is a user interface and it is a direct manipulation by using a touching inputs to the system like tapping, swiping. Application extends the functionality of devices are written using the android software development kit which is also known as (SDK). The SDK includes a set of development tools, debugger, a handset emulator. Memory management is managed by androids for application.

II. RELATED WORKS

To achieve a complete information the techniques which has been[1] used is information capacities with link quality indication (LQI), packet receive radios (PRR) with this we can extract useful information to ensure network integrity. And the feedback mechanism for computing also being used under PRR. A novel secure information management architecture based on emerging attribute based encryption (ABE) primitives. [2]A policy which needs the complex policies so the HIPAA compliant distributed file system and social network. Though this is approach is solution for securely managing information in large. Due to the dynamic changes in the run time in the cloud thus to provide a runtime data protection mechanism combining all the existing approaches to protect data and extending them to run time.[3] And thus also delivering an end to end architecture to protect data at runtime. E2E not only support the infrastructure level also it covers the application level by supporting data controller. Sharing aggregations of cloud data is been executed without revealing the any extra information to any of other services involved. [4]For that privacy preserving query execution model to execute multi source queries managed by different clouds. Goal of the project is to enable the services involved answering a query to apply their privacy policies while at that time keeping possible to link the data subjects. For

data integrity in order to reduce the burden of generating meta data at client side. [5]Stateless verification , unbounded use of queries , public verification, support dynamic operation, batch auditing these are the techniques used for checking scheme. Extensive security and performance analysis is highly efficient and provably secure. User identified by attributes, could freely designed a proxy could re-encrypt a cipher text related with a access policy to another one with different access policy.[6] Selective structure chosen plaintext secure and master key secure without random oracles is a proposed scheme. Proxy re-encryption techniques with recently introduced attributes based cryptosystem the first based PRE scheme. A secure and efficient file sharing via authenticated physical devices remains challenging one to achieve in cloud environment. [7]Because difference things of mobile devices are access the services and provided data by cloud. To provide secure data sharing between the physical devices and clients the Lightweight Identity-Based on authenticated Data Sharing protocol was introduced. It resist the CCA[Chosen-Ciphertext Attack] under hardness assumption of SDH[Strong-Diffie Hellman] problems. This protocol is based on Bilinear Pairing. It also evaluate the performance iterms of Response time, Communication and Computational overhead. There are many security issues and challenges are associated with storage and sharing of data in public cloud[8]. In order to resolve these kind of issues they design an updated secured architecture which can be applied in multi -party data sharing. In this section they provide the security against "honest-but-curious" servers and malicious softwares. To improve the cloud computing technologies the SIEM (Security Information and Event Management) was introduced by the author[9]. SIEM provide cloud based security services such as SECaaS (Security as a Service). This method which helps to recognize the cyber threats analytics. It analyze the data and determine the threats whether the cloud data has some threat or not. It will enhance to improve intelligent cyber threat analysis in the SIEM. Smartphone are more compatible with cloud computing architecture which provide proper cloud computing architecture which provide proper resources to distributed services. Smartphones are like a miniature of computer so there is a lot of chances for many security problems. Proper power management plays a major role in cloud architecture, so here the author[10] choose the algorithm in such a way it would not make the mobile devices more busy and consume more amount of time for encrypting the data. Traditional security approaches are not suitable for Smartphone-Cloud Architecture because of the high use of smartphones. By considering the above problem RSA algorithm is used to decrease the computational power. Cloud computing provide virtual IT infrastructures with same-set of resources that can be shared with multi-tenant users. Data Privacy is most challenging one to the user when they outsource their data with a cloud computing system. [11]To overcome the privacy problem encryption is one of the solution to protect and maintain the cloud-stored data. But the above method is very expensive one and the new method based on Pseudo-Random Permutation was introduced[5] for light-weight mobile devices. The permutation method which splits the file to multilpe chunks and distribute each chunks to multiple splitted file. It also provides low computation overhead. Cloud storage is one of the important service provided by cloud computing for data owners to host their data in the cloud.[12] The cloud computing brings new challenges to security threats for the outsourced data. By combing a Security Homomorphic Encryption with a traditional CP-ABE algorithm the author[6] introduced an algorithm called SE-CP-ABE [Secure Encryption CP-ABE] access control which provide an efficient security and secure and as well as provide flexible Ciphertext retrieval and reduces the retrieval time on cloud-stored data. An efficient and secure lightweight user authentication protocol for mobile cloud computing becomes a paramount due to data sharing by using Internet among users and mobile devices. Resource constraints of mobile devices is makes the data sharing more challenging.[13] A new secure user authentication is based on cryptographic hash, fuzzy extractor function and bitwise xor. User authentication scheme is more secure against possible passive attack and as well as active attack. It does not involve Registration Center (RC) in authentication process and which it is having lowest communication cost when compared with existing scheme. The factors behind the user authentication scheme includes motivation, threat model, fuzzy extractor function. Fuzzy extractor which generates the same output string even if it has different input string. The growth of mobile cloud storage is limited by security and privacy concerns.[14] As data are shared with authorized user in many mobile cloud users, so secure data sharing mechanism is required. The Lightweight Cipher text access control mechanism is used to overcome the required security. The above mechanism is based on Authorization Certificates and Secret sharing scheme. DDKD (Distributing a files Decryption Key to an unauthorized users Directly) is used which needs small amount of keys. But here one of the major disadvantage is authorization revocation because it is very complicated to access the file from the cloud server. EHR(Electronic Health Record) is a digital health documentary which contains not only the health records and it also contain the personal sensitive information. [15]But reliable sharing of EHR through the cloud is always remaining a challenge one. The access policy is not protected and it will also cause some privacy leakage too. In EHR scheme it can hide the entire access policy as well as it reover the hidden entity's from access matrix. ACF(Attribute Cuckoo Filter) is a flexible and efficient attribute matching algorithm. It also capable to locate and recover the attributes accurately. In ACF, an multiple table is used to avoid the element inserting collision. ACF achieve policy preserving as well as attribute recovery without produce much overhead.

III. CONCLUSION

In recent years , many studies on data sharing in cloud are based on attribute-based encryption algorithm, CP-ABE algorithm and LDSS and we studied different techniques for data sharing security. One solution to achieving secure data sharing in the cloud is for the data owner to encrypt his data before storing into the cloud. With more mathematical tools, different schemes are getting more multiple keys for a single application. Thus it considers how to compress secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. The Key generation problem being solved, in which the confidentiality of the secure stored data in the unfriendly environment, where user are not fully trusted or may not be compromised. Additional to it they overcome the revocation problem for all attributes. The overall system performance is improved greatly by reducing the computation overheads in encryption and decryption phases.

REFERENCES

[1] LiliMeng, Haixiang He, Benyue Chen,LufengMot,"A New Method to Achieve Reception of Data Integrity",20IO 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE).
[2] Matthew Pirretti∗ , Patrick Traynor, and Patrick McDaniel ,Brent Waters,"Secure Attribute-Based Systems",(2010) Secure attribute-based systems. Journal of Computer Security, 18(5), 799–837. doi:10.3233/jcs-2009-0383 .
[3] NazilaGolMohammadi, Zoltan´ Ad´ am Mann, Andreas Metzger, MarittaHeisel,James Greig,"Towards an End-to-End Architecture for Run-time Data Protection in the Cloud",2018 44th Euromicro Conference on Software Engineering and Advanced Applications.
[4] Samer Abdul Ghafour,ParisaGhodous,Christine Bonnet,"Privacy Preserving Data Integration Across Autonomous Cloud Services",2015 IEEE 8th International Conference on Cloud Computing.
[5] TAN Shuang1 , TAN Lin2 , LI Xiaoling1 , JIA Yan1,"An Efficient Method for Checking the Integrity of Data in the Cloud",international conference on Security and privacy in communication networks.
[6] Xiaohui Liang,Zhenfu Cao,Huang Lin,"Attribute Based Proxy Re-encryption with Delegating Capabilities", Proceedings of the 4th International conference on Information, Computer, and Communications Security - ASIACCS'09
[7] Arijit Karati, Ruhul Amin, SK Hafizul Islam," Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment",2018 IEEE Transactions on Cloud Computing.
[8] Chuan Fu, Jun Yang, Zheli Liu and Chunfu Jia,"A Secure Architecture for Data Storage in the Cloud Environments", 2015 9th International Journal on Innovative Mobile and Internet Services in Ubiquitous Computing.
[9] Jong-Hoon Lee, Young Soo Kim," Toward the SIEM Architecture for Cloud-based Security Services", 2017 IEEE journal on Communications and Network Security.
[10] Md. AI-Hasan, Kaushik Deb," User-Authentication Approach for Data Security Between Smartphone and Cloud", 2013 International Journal on Authentication scheme.
[11] Mehdi Bahrami and Mukesh Singhal," A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing", 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering.
[12] PING XIONG1, QI-XIAN GAN1, XIN-XIN HE1, QUAN ZHAO," A SEARCHABLE ENCRYPTION OF CP-ABE SCHEME IN CLOUD STORAGE". 2013 10th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP**).**
[13] SANDIP ROY, SANTANU CHATTERJEE," Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services",2017 IEEE Access on secure authentication scheme.
[14] Xuanxia Yao, Xiaoguang Han," A Lightweight Access Control Mechanism for Mobile Cloud Computing", 2014 IEEE International paper on Mobile Cloud Computing.
[15] ZUOBIN YING, LU WEI, QI LI, XIMENG LIU AND JIE CUI," A Lightweight Policy Preserving HER Sharing Scheme in the Cloud". 2018 IEEE Access on Policy Preserving Scheme,doi:10.1109/access.2018.2871170