International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

# SECURE STORAGE, DISTRIBUTION AND PROCESSING OF IOT BASED DATA THROUGH MOBILE CLOUD COMPUTING-A SURVEY

**A.JYOTHI**
Computer Science Dept.
Anurag Group of Institutions
Ghatkesar, Hyderabad, India

**DR. B. INDIRA**
Computer Science Dept.
Kasturba Gandhi Degree& PG
College for Women, Secundrabad, India

**Abstract:** The Internet of Things(IOT) is an interconnection of various devices embedded with sensors, software and electronics, which connects to the internet through one of the communication channel -A mobile application. Although through mobile, data can be stored, distributed and processed but, due to the high volumes of data generated by IOT devices, a resource poor device like mobile would not able to handle the large data and should resort to the cloud for data storage, distribution, processing. Cloud has huge resources and provides many services for data. With aforementioned features of the cloud some security challenges are also inherited. Security and privacy of the data from the IOT devices plays a vital role as it would be stored on the cloud and a vast number of data storage and data security techniques have been proposed In this paper a survey is made on the various methods used for secured storage of data using Mobile Cloud Computing(MCC)

**Keywords**-*IOT, Mobile, Cloud, MCC, Security, Storage*

## I. Introduction

IOT is an emerging technology where various things or devices equipped with sensors, electronics, software and network connectivity, collects the data from the world and is processed. The data from the devices can be processed and can be used in diverse applications. Some of the applications are smart home, wearables, smart cities, healthcare, connected cars, poultry and farming. Most of the information and technology companies have already paved a way to IOT technology and are designing IOT devices. Few examples of these devices, (online) are Amazon Echo-It works through a voice assistant where a user can order to perform functionalities like to play music, read the weather report etc., Nest smart thermostat-It is a smart thermostat connected to the internet it will automatically adjust the temperature based on whether the user is in the home or away., Apple phone calls etc., fitbit & jawbone -These application gives more data about the users' workouts.

The communication can be between the different devices and also the user can interact with the devices through a desktop, a laptop or through a mobile application. we can have communication, navigational information and entertainment through the mobile therefore, it has become a major part of our daily lives and also the gateway for communicating with the IOT devices. The data is collected by the devices, processed and can be communicated to the user through the mobile application on the mobile. since the devices or things and even mobiles have very small resources for storing and processing of data. Huge resources which are provided by the cloud can be used by the mobile application for storage, processing and distribution of IOT data The integration IOT and mobile cloud computing can be done for storing, processing, and dissemination of data while using the cloud with many of the of its advantages, even security issues are also embedded. This paper is a survey on various security mechanisms on data in mobile cloud computing(MCC)

## II. IOT and Mobile Applications

The main interface of interaction between IOT and the user are the mobile devices such as smart phones, multiple connectivity options including Wi-Fi, Bluetooth, cellular and NFC that enable them to communicate to other devices or sensors. It is these default qualities of mobile devices that put them at the core of the IOT.

Mobile apps can interact with the IOT by functioning as a remote to IOT devices. The data required to operate the IOT devices can be enabled by communicating through the mobile application. some of the mobile applications are(online),[1] WeM Switch Smart Plug-It plugs into a regular outlet, accepts the power cord from any device, and can be used to turn it on and off on a set schedule or when you hit a button on your smartphone. It also monitors how much energy your devices are using, helping you make your home more energy efficient. User can see when the plugs are on, how much power they're using, and set schedules for operation right from the mobile app., August Smart Lock- With this smart lock, users never need keys again.it locks and unlocks automatically when leaves and get into the home, .user can grant guest keys to friends or the dog sitter, and can even view the activity log and grant access from the smartphone remotely.

Many such IOT devices are being used worldwide and in 2015, the world will have 25 billion connected devices [2]; Gartner, Inc. a research organisation [3]forecasts that 8.4 billion connected

things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020

## III. Security Challenges in IOT

Some of the security & privacy challenges faced by IOT are [4]

ubiquitous data collection-The collection of personal information, habits, and physical condition overtime by the IOT devices poses privacy challenges and increases the sensitivity of the data and to analyse the huge data that is being produced by IOT devices would not be possible because of scarce resources of IOT usage of consumer data-The data collected from the devices may not always to service the user but can also be shared with others. for example, a smart TV can track viewing habits of the customer and this info can be leaked to the data broker security-IOT poses many security risks, like computers and mobile devices inadequate security might lead to a security breach

## IV. Security Challenges in MCC

There are some physical threats to mobile devices. It is possible to loss, leakage, access or to unintentionally disclose the data or applications to unauthorized users, if the mobile devices are misplaced, lost or theft [5]. Attacks such distributed denial attack [6] and availability attacks are launched by taking the advantages of the vulnerabilities existing in the mobile

## V. Secure Data Storage and Distribution Mechanisms

Mobile cloud computing enables storing, sharing and distribution of IOT data through mobile and cloud. cloud has huge resources and provides numerous services. Much of the research is being done

on as, mechanisms are also being proposed Many authors have proposed security mechanisms for the data on the cloud [7], [8], [9] ,[10], [11] has tried to check the integrity of the data on the cloud .as the data might get lost and not be available because of the dishonest cloud or might be because of the errors caused while data updation

Encryption is an approach to accomplish data privacy, but encryption alone is not the solution for data security Actually, traditional data encryption scheme limits the data access by only allowing the user with corresponding decryption key to read the data. To have an efficient data sharing with access control over the private data in the cloud, advanced cryptographic encryption schemes such as broadcast encryption (BE) [12],[13] attribute-based encryption(ABE)[14],[15] and proxy re-encryption(PRE)[16],[17],[18]have been employed in the design of cloud storage systems.

Wang [19] proposed a security approach to protect mobile user's data on media cloud. This approach is based on three parts such as secure sharing, scalable watermarking and Reed-Solemon coding. The secure sharing is used to upload multimedia contents in diff erent pieces to diff erent clouds and the watermarking is used for authentication purpose. Whereas, the Reed-Solemon error correction coding ensures the reliability of multimedia transmission over error-prone wireless networks.

Ali et al.[20],SeDaSC (Secure Data Sharing in Clouds) is proposed by Mazhar Ali et al. for both conventional cloud and MCC. This methodology has three entities such as user, a cryptographic server (CS) and the cloud. The user submits the data, group members list and access control list to CS. The CS is responsible for encryption, decryption, key management and access control. Firstly, the CS generates the symmetric key and encrypts the data by this. Next, the CS divides the key into two parts, one is for group members and other part is for access control purpose. Then, the encrypted data is stored in the cloud on behalf of the user. When a group member wants to download the data from the cloud, it sends the request with its key part to CS. Then, after authentication by CS, it allows to decrypt and download the data from the cloud to the requested user.

Authors in Qiu et al.,[21] propose proactive dynamic secure data scheme (P2DS) to ensure the mobile user's data protection from unauthorized access in cloud. This scheme is based on attribute based semantic access control and proactive determinative access algorithms. Jin et al. [22]; Odelu et al.[23], the authors utilize cipher text policy attribute based encryption (CP-ABE) to protect from unauthorized access. These schemes are referred as SL-CP- ABE (Secure and lightweight CP-ABE) and CP-ABE-CSCTSK (CP-ABE- constant size ciphertext and secret keys) respectively. These schemes provide access control in MCC environment and allow the mobile user to outsource securely computational processing to cloud from mobile devices with reduced encryption and decryption operation

jiang Zang[24]has proposed a data distribution system in mobile cloud computing which does not involve a third party and also provides functionality such as data privacy, data authentication, data dynamics and fine grained access control by designing a scheme called as type based proxy re-encryption (TB-PRE) it is a variant of PRE(proxy re-encryption ).TB-PRE allows the data owner to classify his data into different categories .e.g., by the content of the data.The owner of the data protects his data in each category with a unique type For efficiency, a secure symmetric encryption is employed to encrypt the data under a chosen secret key for each data category, and the TB-PRE scheme is then used to encrypt the symmetric secret key. Since each data category may contain many data files, the data owner also constructs a Merkle Hash Tree (MHT) for each data category and only

stores the metadata consisting of the root of the MHT corresponding to each category at his own local storage for checking data integrity and performing dynamic data operations. The use of MHT enables the data owner to achieve minimum overhead when performing dynamic data operations. Besides, the BLS signature scheme is used to authenticate the roots of the MHT such that the data consumer cloud also checks the integrity of the data files as well as authenticate the identity of the data owner

TB-PRE scheme takes the advantage of Merkle tree and BLS signature to ensure security and efficiency of the data on the cloud TB-PRE scheme is said to be more efficient than ABE(Attribute Based Encryption) and can be a right candidate to the devices with limited capacity .They have said to design a scheme which does not suffer from key escrow problem

Another scheme proposed on data sharing for mobile cloud computing is by Ruixuan[25].They have proposed a Light weight Data Sharing Scheme(LDSS).It is based on Attribute Based Encryption (ABE) to have efficient access control on cipher text .It uses proxy servers for encryption and decryption process The operations that are done in Attribute based encryption are just escalated to the proxy servers ,which very much reduces the computational over head on client side on client side mobile device

Data privacy in LDSS-CP-ABE(Lightweight Data Sharing Scheme),can be achieved by introducing , a version attribute to the access structure. The decryption key format is modified so that it can be sent to the proxy servers in a secure way. The user revocation problem is dealt by adding the lazy re-encryption and description field of attributes

## VI. Conclusion

With the omnipresence of IOT and MCC , integration of IOT and MCC fetches many advantages and also disadvantages. The communication between the IOT devices, mobile and cloud brings in number of challenges This paper presents some of data security, storage and distribution mechanisms, which would be very useful for the researchers for security enhancements

## VII. References

[1].https://beebom.com/examples-of-internet-of-things-technology/

[2]. dave evans, cisco internet bus. solutions grp., the internet of things how the next evolution of the internet is changing everything 3 (2011), available at http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[3]. http://www.gartner.com/newsroom/id/3165317

[4].https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf

[5].Milligan, P.M.,Hutcheson, D.2008, Business risks and security assessment for mobile devices, Information Systems Control JournalVolume 1, Page 24

[6]. Liu, L., Zhang, X., Yan, G., Chen, S., 2009. Exploitation and threat analysis of open m/obile devices, In: Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, pp. 20 –29.

[7].GiuseppeAteniese,RandalBurns,RezaCurtmola,JosephHerring, Lea Kissner, Zachary Peterson, and Dawn Song. Provable data possession at untrusted stores. In Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS '07, pages 598–609, New York, NY, USA, 2007. ACM.

[8].Ee-Chien Chang and Jia Xu. Remote integrity check with dishonest storage server. In Sushil Jajodia and Javier Lopez, editors, Computer Security - ESORICS 2008, volume 5283 of Lecture Notes in ComputerScience,pages 223–237. Springer Berlin Heidelberg,2008.

[9]. Ari Juels and Burton S. Kaliski, Jr. Pors: Proofs of retrievability for large files. In Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS '07, pages 584–597, New York, NY, USA, 2007. ACM.

[10].Alina Oprea, Michael K. Reiter, and Ke Yang. Space-efficient block storage integrity. In In Proc. of NDSS 05, 2005.

[11].Hovav Shacham and Brent Waters. Compact proofs of retrievability. In Josef Pieprzyk, editor, Advances in Cryptology - ASIACRYPT 2008, volume 5350 of Lecture Notes in Computer Science, pages 90– 107. Springer Berlin Heidelberg, 2008.

[12].AmosFiat and Moni Naor. Broadcast encryption. InDouglasRStinson,editor,AdvancesinCryptologył CRYPTO93,volume773of Lecture Notes in Computer Science, pages 480–491. Springer Berlin Heidelberg, 1994.

[13]. Noam Kogan, Yuval Shavitt, and Avishai Wool. A practical revocation scheme for broadcast encryption using smartcards. ACM Trans. Inf. Syst. Secur., 9(3):325–351, August 2006.

[14].Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypteddata. In Proceedingsofthe13thACMconferenceonComputer and communications security, CCS '06, pages 89–98, New York, NY, USA, 2006. ACM.

[15] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, Advances in Cryptology - EUROCRYPT 2005, volume 3494 of LNCS, pages 557–557. Springer Berlin / Heidelberg, 2005.

[16]. Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy

cryptography. In Kaisa Nyberg, editor, Advances in Cryptology - EUROCRYPT'98, volume 1403 of LNCS, pages 127–144. Springer Berlin / Heidelberg, 1998.
[17]. Ran Canetti and Susan Hohenberger. Chosen-ciphertext secure proxy re-encryption. In Proceedingsof the 14th ACM conference on Computer and communications security, CCS '07, pages 185–194, New York, NY, USA, 2007. ACM.
[18]. Ran Canetti and Susan Hohenberger. Chosen-ciphertext secure proxy re-encryption. In Proceedings of the 14th ACM conference on Computer and communications security, CCS '07, pages 185–194, New York, NY, USA, 2007. ACM.
[19].Wang, H., Wu, S., Chen, M., Wang, W., 2014. Security protection between user and the mobile media cloud. Commun. Mag., IEEE 52, 73 –79 .
[20].Ali, M., Khan, S.U., Vasilakos, A.V., 2015a. Security in cloud computing: opportunities and challenges. Inf.[ Sci. 305, 357–383.
[21]. Qiu, M., Gai, K., Thuraisingham, B., Tao, L., Zhao, H., 2016. Proactive user-centric securedata scheme using attribute-based semantic access controls for mobile clouds in finanacial industry.Futur.Genr compute.syst.
[22]. Jin, Y., Tian, C., He, H., Wang, F., 2015. A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing, in Big Data and Cloud Computing (BDCloud),
[23].Odelu, V., Das, A.K., Rao, Y.S., Kumari, S., Khan, M.K., Choo, K.-K.R., 2016. Pairing- based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. Comput. Stand. Interfaces.
[24].Jiang Zhang, Zhenfeng Zhang, and Hui Guo,2106.Towards Secure Data Distribution Systems in Mobile Cloud Computing. IEEE Transactions
[25]. Ruixuan Li, Chenglin Shen, Heng He, Zhiyong Xu, and Cheng-Zhong Xu, 2014A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing.IEEE Transactions on cloud computing.