IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Data Storage Security and Privacy in Mobile Cloud Computing Using Hierarchical Attribute Based Encryption (HABE)

Tejaswini Paka[1*], Sree Divya[2]

[1]Mahatma Gandhi Institute of Technology, Gandipet Hyderabad, India
[2]Dept.of Information and Technology, Mahatma Gandhi Institute of Technology, Gandipet Hyderabad

[*]*Corresponding Author: pakatejaswini@gmail.com, Tel.: +91-6302990323*

DOI: https://doi.org/10.26438/ijcse/v7i6.750754 | Available online at: www.ijcseonline.org

Accepted: 13/Jun/2019, Published: 30/Jun/2019

***Abstract*—** In spite of the fact that the electronic advances have experienced quick improvements as of late, cell phones, for example, PDAs are still similarly powerless rather than work areas as far as computational ability, stockpiling and so on, and are not ready to meet the expanding requests from versatile clients. By incorporating portable figuring and distributed computing, versatile distributed computing (MCC) extraordinarily expands the limit of the portable applications, however it additionally acquires numerous difficulties in distributed computing, e.g., information security and information honesty. In this paper, we use a few cryptographic natives, for example, another composes based intermediary re-encryption to plan a protected and proficient information circulation framework in MCC, which gives information security, information respectability, information verification, and adaptable information appropriation with get to control. Contrasted with customary cloud-based information stockpiling frameworks, our framework is a lightweight and effortlessly deployable answer for portable clients in MCC since no confided in outsiders are included and every versatile client just needs to keep short mystery keys comprising of three gathering components for every single cryptographic activity. At last, we present broad execution examination and exact investigations to exhibit the security, versatility, and productivity of our proposed framework.

Keywords*— *Distributed System, Mobile Cloud Computing,

I. INTRODUCTION

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an edge server. Clouds may be limited to a single organization (enterprise clouds,) be available to many organizations (public cloud,) or a combination of both (hybrid cloud.) The largest public cloud is Amazon AWS. Cloud computing relies on sharing of resources to achieve coherence and economies of scale**.[1]**

In cloud computing, many computing resources are provided as services over the internet. One of the main services provided by clouds is storage (e.g., Simple Storage Services—Amazon S3), which allows users to store their enormous amount of data to the remote clouds without bothering the complex management of storage hardware. Outsourcing big data to clouds provides many benefits, e.g., low costs, good reliability and availability, but the data security issues such as privacy and integrity brought by third party's cloud systems have been the major concerns for users utilizing such services. According to the surveys, more than 90% of US consumers wants to be asked to give permission for their data to be shared, and 88% of all potential consumers are worried about the privacy of their data. Since the data is stored and managed in the cloud, the data security highly depends on the IT management of the cloud services providers, and any security loophole in the cloud system might damage the security of the users' private data, e.g., **[2-6]**

Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to utilities such as water, electricity, gas, and telephony. Figuring is being changed to a model comprising of administrations that are commoditized and conveyed in a way like utilities, for example, water, power, gas, and communication. In such a model, clients get to administrations in light of their necessities paying little respect to where they are facilitated. A few processing standards, for example, Grid figuring have guaranteed to convey this utility registering vision. Distributed computing is the latest developing worldview promising to turn the vision of "registering utilities" into a reality. **[7-11]**

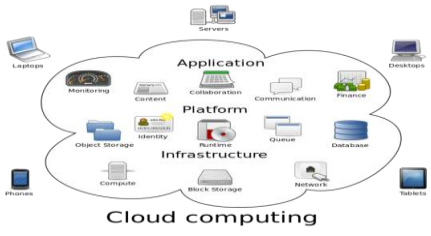

Fig.1.1 Cloud Computing

1.1 Mobile Cloud Computing:

Mobile Cloud Computing (MCC) is the combination of cloud computing, mobile computing and wireless networks to bring rich computational resources to mobile users, network operators, as well as cloud computing providers. The ultimate goal of MCC is to enable execution of rich mobile applications on a plethora of mobile devices, with a rich user experience. MCC provides business opportunities for mobile network operators as well as cloud providers. MCC can be defined as rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle.**[12]**

1.2 ARCHITECTURE:

MCC uses computational augmentation approaches (computations are executed remotely instead of on the device) by which resource-constraint mobile devices can utilize computational resources of varied cloud-based resources. In MCC, there are four types of cloud-based resources, namely distant immobile clouds, proximate immobile computing entities, proximate mobile computing entities, and hybrid (combination of the other three model). Giant clouds such as Amazon EC2 are in the distant immobile groups whereas cloudlet or surrogates are member of proximate immobile computing entities. Smartphones, tablets, handheld devices, and wearable computing devices are part of the third group of cloud-based resources which is proximate mobile computing entities**.[13]**

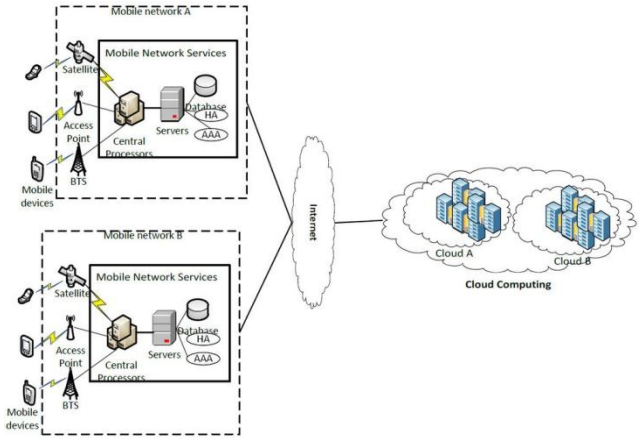

Fig.1.2 Mobile Cloud Computing

1.3 EXISTING SYSTEM

In the existing system, since broadcast encryption (BE) usually involves a group manager, and needs to determine the group of the data consumers before the data is uploaded to the cloud, the solution of using BE to ensure secure data-sharing usually cannot support dynamic data distribution. This is not applicable to the case that the data owner does not know the information of the potential data consumers when he uploads the data to the cloud. Besides, if the group manager is a third party (i.e., not the data owner himself), this solution may incur the key escrow problem since the group manager can read the data of all the group members.**[14]**

In recent years, many researchers have resorted to attribute-based encryption (ABE) to enforce fine-grained access control in cloud storage. On the one hand, those systems support dynamic and flexible access control based on the attributes of the data consumers. But on the other hand, an ABE system relying on a third party authority to issue secret keys for all system users usually suffers from the key escrow problem. The use of multi authorities ABE, e.g., can somehow ease the worry of this problem, but this general method cannot completely solve the key escrow issue. **[15]**

By letting the data owner himself be the attribute authority, the above key escrow problem can be avoided, but the number of secret keys of each data consumer in such a solution is usually linear to the number of the data owners. This might be a big bottleneck in open networks where each user may potentially be a data owner. Actually, the above problems as well as the inefficiency of existing ABEs in terms of computation and communication overheads have become the major obstacle in deploying ABE in real applications. Some of the disadvantages of existing system are

- The data storage is based on Time Durations.
- There is no Data security due to lack of Data Blocks.

1.3.1 Proposed System

In the proposed system, the system presents an efficient data distribution system in MCC, which allows mobile users to securely store their data in the cloud storage, and flexibly share their data with friends. We leverage several cryptographic primitives to achieve data privacy, data integrity, dynamical data modification and deletion, and flexible data distribution. Concretely, we first design an efficient type-based proxy re-encryption (TB-PRE), which allows a mobile user with a single secret key to keep the data privacy, and flexibly share his data with friends under permission**.[15]** Some of the advantages of proposed system are:

- User data will be very safe due to data integrity proof.
- More security due to data blocks by Merkle Hash Tree.

II. HARD WARE SYSTEM CONFIGURATION

Following are the typical hardware and software requirements of the proposed system.

1. Processor - Pentium –IV
2. RAM - 2 5 6 MB (min)
3. Speed - 1.1 GHz
4. Hard Disk - 20 GB

2.1 Software Requirements:

1. Operating System : Windows 7.0
2. Application Server : Tomcat 5.0/6.X
3. Front End : HTML, Java, Jsp
4. Scripts : JavaScript.
5. Server side Script : Java Server Pages.
6. Database : MYSQL
7. Database Connectivity : JDBC

III. INPUT DESIGN

Information Design assumes a fundamental job in the existence cycle of programming advancement, it requires exceptionally watchful consideration of engineers. The information configuration is to nourish information to the application as precise as could reasonably be expected. So inputs gathered are composed viably with the goal that the mistakes happening while at the same time nourishing are limited. As indicated by Software Engineering Concepts, the info structures or screens are intended to give to have an approval authority over as far as possible, go and other related approvals. **[16]**

This framework has input screens in every one of the modules. Blunder messages are produced to caution the client at whatever point he submits a few errors and aides him in the correct way with the goal that invalid passages are not made. Give us a chance to see profoundly about this under module outline.

Info configuration is the way toward changing over the client made contribution to a PC based organization. The objective of the info configuration is to make the information passage legitimate and free from mistakes. The mistake is in the information are controlled by the info plan. The application has been created in easy to understand way. The structures have been composed in such a path amid the handling the cursor is set in the position where must be entered. The client is additionally given in a choice to choose a suitable contribution from different options identified with the field in specific cases. Approvals are required for every datum entered. At whatever point a client enters wrong information, mistake message is shown, and the client can proceed onward to the resulting pages subsequent to finishing every one of the passages in the present page. **[17]**

3.1 OUTPUT DESIGN

The Output from the PC is required to for the most part make a productive technique for correspondence inside the organization principally among the undertaking pioneer and his colleagues, at the end of the day, the director and the customers. The yield of VPN is the framework which enables the venture pioneer to deal with his customers as far as making new customers and allocating new activities to them, keeping up a record of the task legitimacy and giving envelope level access to every customer on the client side contingent upon the undertakings dispensed to him. After fulfilment of a task, another venture might be doled out to the customer. Client validation strategies are kept up at the underlying stages itself. Another client might be made by the manager himself or a client would himself be able to enlist as another client yet the errand of doling out ventures and approving another client rests with the director as it were.

The application begins running when it is executed out of the blue. The server must be begun and afterward the web wayfarer in utilized as the program. The venture will keep running on the neighbourhood so the server machine will fill in as the manager while the other associated frameworks can go about as the customers. The created framework is profoundly easy to use and can be effortlessly comprehended by anybody utilizing it notwithstanding out of the blue.

IV. SOFTWARE ENVIRONMENT

At first the dialect was called as "oak" however it was renamed as "Java" in 1995. The essential inspiration of this dialect was the requirement for a stage free (i.e., engineering nonpartisan) dialect that could be utilized to make programming to be inserted in different customer electronic gadgets.

- Java is a software engineer's dialect.
- Java is firm and reliable.
- Except for those limitations forced by the Internet condition, Java gives the software engineer, full control.
- At long last, Java is to Internet programming where C was to framework programming.

4.1 Java Architecture

Java design uses a compact, strong, high accomplishing condition for progression. Java uses adaptability by storing up the byte codes for the Java Virtual Machine, which searches for that broke down on each system a by the run-time condition. Java is an excited system, prepared to stack code when required from a contraption in a practically identical region or all through the globe.

Collection of code

When you gather the code, the Java compiler sets up maker code (called byte code) for an insightful contraption called Java Virtual Machine (JVM). The JVM is proposed to finish the byte code. The JVM is made for ousting the issue of convenience. The code is conveyed and also likewise set up for one maker and furthermore in like way investigated on all producers. This instrument is called Java Virtual Machine.

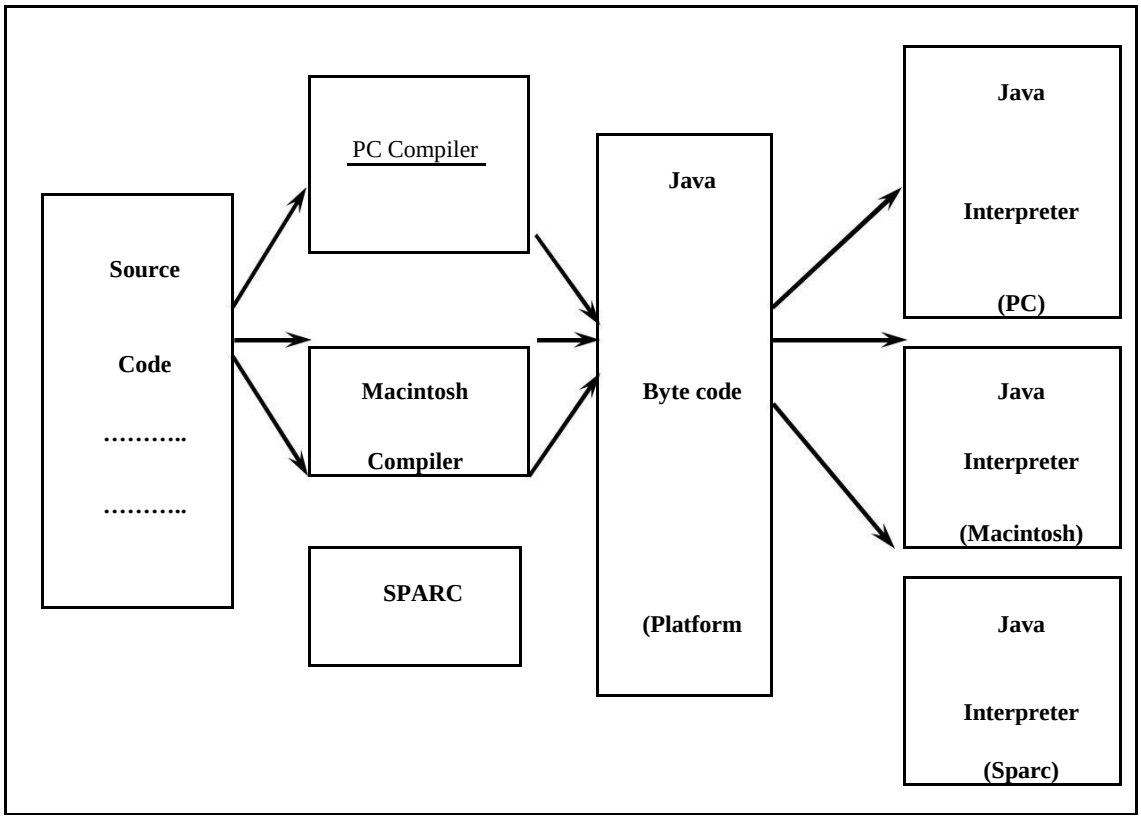

Fig.4.1 Compiling and interpreting Java Source Code

V. CONCLUSION

Mobile Cloud computing (MCC) is one of the versatile innovation slants later on in light of the fact that it joins the benefits of both MC and CC, in this way giving ideal administrations to versatile clients. The mobile world is evolving through significant transition from voice applications to data applications. In the US, more than 35% of the revenues come from data services and the data revenues will remain for over 50% of the revenues by the start of 2016. MCC attempts to engage the convenient client by giving universal and rich usefulness, paying little heed to the asset constraints of cell phone. The vision of MCC is an independent advanced condition in which distinctive cell phones get their calculation, stockpiling, administrations and different assets self-ruling and proficiently whenever and anyplace. Based on the present study a viable information related to appropriation framework in versatile distributed computing, which does not include any confided in outsider and gives a few valuable properties including information protection, information uprightness, information confirmation, dynamic information adjustments and erasures, and in addition fine-grained get to control is proposed .

REFERENCES

[1] Zhang, J., Zhang, Z. and Guo, H., 2017. Towards secure data distribution systems in mobile cloud computing. IEEE Trans. Mob. Comput, 16(11), pp.3222-3235.

[2] Dinh, H.T., Lee, C., Niyato, D. and Wang, P., 2013. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), pp.1587-1611.

[3] Fernando, N., Loke, S.W. and Rahayu, W., 2013. Mobile cloud computing: A survey. Future generation computer systems, 29(1), pp.84-106.

[4] Rahimi, M.R., Ren, J., Liu, C.H., Vasilakos, A.V. and Venkata subramanian, N., 2014. Mobile cloud computing: A survey, state of art and future directions. Mobile Networks and Applications, 19(2), pp.133-143.

[5] Wang, M., Chen, Y. and Khan, M.J., 2014. Mobile cloud learning for higher education: A case study of Moodle in the cloud. The International Review of Research in Open and Distributed Learning, 15(2).

[6] Rao, N.M., Sasidhar, C. and Kumar, V.S., 2012. Cloud computing through mobile-learning. arXiv preprint arXiv:1204.1594.

[7] Jia, W., Zhu, H., Cao, Z., Wei, L. and Lin, X., 2011, April. SDSM: a secure data service mechanism in mobile cloud computing. In Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on (pp. 1060-1065). IEEE.

[8] Feng, D.G., Zhang, M., Zhang, Y. and Xu, Z., 2011. Study on cloud computing security. Journal of software, 22(1), pp.71-83.

[9] Qureshi, S.S., Ahmad, T. and Rafique, K., 2011, September. Mobile cloud computing as future for mobile applications-Implementation methods and challenging issues. In Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on (pp. 467-471). IEEE.

[10] Huang, D., Xing, T. and Wu, H., 2013. Mobile cloud computing service models: a user-centric approach. Ieee network, 27(5), pp.6-11.

[11] Wang, Y., Chen, R. and Wang, D.C., 2015. A survey of mobile cloud computing applications: perspectives and challenges. Wireless Personal Communications, 80(4), pp.1607-1623.
[12] Raja, C.V., Chitra, K. and Jonafark, M., 2018. A Survey on Mobile Cloud Computing.
[13] Gu, F., Niu, J., Qi, Z. and Atiquzzaman, M., 2018. Partitioning and offloading in smart mobile devices for mobile cloud computing: State of the art and future directions. Journal of Network and Computer Applications.
[14] Skourletopoulos, G., Mavromoustakis, C.X., Mastorakis, G., Batalla, J.M., Dobre, C., Panagiotakis, S. and Pallis, E., 2017. Towards mobile cloud computing in 5G mobile networks: applications, big data services and future opportunities. In Advances in Mobile Cloud Computing and Big Data in the 5G Era (pp. 43-62). Springer.
[15] Li, Y., Gai, K., Qiu, L., Qiu, M. and Zhao, H., 2017. Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, 387, pp.103-115.
[16] Sookhak, M., Yu, F.R. and Tang, H., 2017. Secure data sharing for vehicular ad-hoc networks using cloud computing. In Ad Hoc Networks (pp. 306-315). Springer.
[17] Khan, S., Shiraz, M., Boroumand, L., Gani, A. and Khan, M.K., 2017. Towards port-knocking authentication methods for mobile cloud computing. Journal of Network and Computer Applications, 97, pp.66-78.
[18] Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M.A., Choudhury, N. and Kumar, V., 2017. Security and privacy in fog computing: Challenges. IEEE Access, 5, pp.19293-19304

Authors Profile

Mrs Tejaswini Paka is a PG Student at Mahatha gandi Institute of Technology, Gandeipt. She holds a B. Tech Degree in Conputer sciences from JNTUH . Her areas of Intrest include , Cloud computiung, Moble cloud coumpting.

Mrs N Sree Divya is Assistant Professor in the deparmnt of Information and technology, at Mahatha gandi Institute of Technology, Gandeipt. She holds a B. Tech Degree in Conputer sciences & Information Tecnology from JNTUH and M.tech in Computer Sciences. Her areas ofIntrest include , Cloud computiung, Moble cloud coumpting and Vehicular adhoc Networks. She has published 03 Internatnla jounrals of repute and presnted 08 technical papaers in various Nationla and Internationa conferences of Repute. She has attended over 15 refersher programmes/ FDPs/ workshops. She has 12 years of teaching and research for UG and Pg

