Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 7, July 2020, pg.109 – 114

Feasible Approach on Mobile Cloud Computing for Integrity and Secure Data Sharing

P Seshu Kumar[1]; MOHAMMED ALISHA[2]

[1]Roll no 186L1D5806, Amalapuram Institute of Management Sciences and College of Engineering, East Godavari, Andhra Pradesh, India

[2]M.Tech., (Ph.D), Associate Professor, Amalapuram Institute of Management Sciences and College of Engineering, East Godavari, Andhra Pradesh, India

[1] sk.mca9@gmail.com; [2] mohammedalisha@gmail.com

Abstract— Cloud computing is an emerging technology that will receive more attention in the future from industry and academia. The cost of this technology is more attractive when it is compared to building the infrastructure. However, there are many security issues coming with this technology as happens when every technology matures. Those issues include issues related to the previous issues of the internet, network issues, application issues, and storage issues. Storing data in a remote server leads to some security issues. Those issues are related to confidentiality of data from unauthorized people in remote sites, integrity of stored data in remote servers and the availability of the data when it is needed. Also, sharing data in cloud when the cloud service provider is mistrusted is an issue. In this paper we discussed above the issue of sharing the information in cloud registering securely is settled. Information insurance can be kept up by using ABE and BRE calculation.

Keywords— Cloud computing, Integrity, ABE, BRE, Data sharing.

I. INTRODUCTION

Each and every day millions of people around the world are using hand-held “mobile’ devices (i.e. Smartphones, PDAs and Tablets) in order to run software applications which (securely) provide them with access to important information, such as; the people, locations, products and services available around them [1]. These software applications also provide users with a method to interact with people that they may do business with or with whom they associate. The technology used to make all of this possible is known as Mobile Cloud Computing or MCC.

MCC essentially brings new and exciting applications to mobile devices beyond what could have been possible by regular Mobile Computing (MC) applications, all done by combining both cloud computing and mobile computing technologies [2]. By combining both CC (Cloud Computing) with MC a new infrastructure has been invented which relieves the stress off of mobile devices from requiring huge amount of processing power as well as storage, as the storage and 'heavy lifting' of computing intensive work is now taken over by the cloud [3], which resides outside of the mobile computing ecosystem. In short Cloud Computing offers various services (e.g. IAAS, PAAS and SAAS) to Mobile Computing as a means to tackle the issue of lack of storage space and processing power most mobile devices offer; which have a tremendous impact on service quality [4].

Currently, MCC is a very hot topic of discussion in the technology world as well as in academia. The IT industry highly anticipates that Mobile Cloud Computing will have a drastic effect on people's life styles and work patterns in a future networked world. IBM predicted that there will be "1 trillion cloud-ready devices by 2015" and stated that users of MCC will primarily work using web-based applications via remote servers which are accessed through networked devices [5]. Although Mobile Cloud Computing may seem like an amazing technological advancement which all individuals and businesses should be taking advantage of. There still remains a lot of mystery around the subject as well; more specifically around Data Security surrounding where highly confidential business data would be stored, as well as how the data will be transmitted securely and reliably between cloud service users and the cloud, etc.

II. RELATED WORK

This section presents an overview and security issues of MCC. Due to the limitations of mobile devices in the MCC environment, data-intensive and compute-intensive applications cannot be run on these devices, because they consume massive resources of energy. Therefore, these applications have been divided to allow the cloud to process core computing tasks. Mobile devices are also allowed to take the responsibility of some simple tasks. There are some issues that affect the performance of MCC, such as data delivery time, network handover delay and data processing in the mobile device and data center. The elastic application division mechanism is used as a solution to mitigate these challenges.

Most of the existing proposed frameworks have been documented in literature to ensure the issues of integrity and confidentiality for MCC. In fact, limited solutions have been introduced to ensure both of these issues. Jia et al. [6] proposed a secure mobile user-based data service mechanism (SDSM) that outsources security management and data to clouds in a trusted way. This will allow mobile users to move data and share data overhead to the cloud without revealing any information to unauthorized users. SDSM ensures the confidentiality of data stored on the cloud and fine-grained access control with minimum communication overheads and cost of updating access policy. It uses identity based encryptions and proxy re-encryption schemes to secure data service. It has three main entities, including the data owner, the data sharer and the cloud service provider. The data owner and data sharer can store and retrieve files by utilizing the cloud storage service. The data owner can also share files and grant access privileges to the data sharer for these files. This solution has three limitations. Firstly, it does not ensure the integrity of data stored on the cloud.

Itani [7]proposed an energy efficient integrity verification scheme for mobile devices. It ensures the integrity of files for mobile users, which are stored on the cloud, using the concept of trusted computing and incremental cryptography. It has three components, including the cloud service provider, the mobile client and a trusted third party. The management and allocation of the cloud resources is the responsibility of the cloud service provider. The cloud service provider provides the storage services that are utilized by mobile clients. The installation and configuration of the coprocessors on the cloud and ensuring the integrity of a party. The coprocessor generates a message authentication code, and each coprocessor is responsible for a specific group of mobile clients. This solution minimizes the processing overhead on the mobile device, since most of the integrity verification is done by the trusted third party. However, it does not ensure the confidentiality of the user's data. In addition, the performance is poorer if the number of mobile clients increases for each coprocessor. Compared with the previous two proposed solutions, there is less processing overhead on mobile devices, since fewer mobile clients perform integrity verification on their devices.

III. PROPOSED WORK

A. ARCHITECTURE AND MODULES

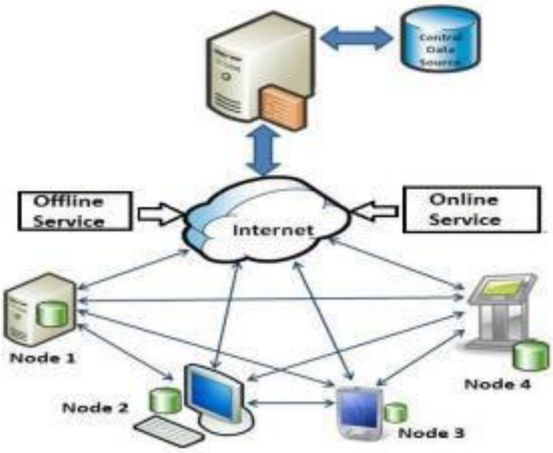

Figure 1: System model

The architecture of the proposed framework is appeared in the figure which demonstrates the clients and the tasks included. The nitty gritty portrayal of the architecture is clarified as takes after:

Nodes: The User is in charge of transferring and sharing its own information on the cloud.

On-line and Off-line Services: In On-line Service information will encrypted and straightforwardly exchange to the separate client. In Off-line Service if there is no Internet Connection the information will get encrypted first and afterward it will get put away in Main Server. Until the point when the framework does not goes ahead line the information won't be shared over the cloud

Cloud Service Provider: Cloud specialist co-op is in charge of giving all the expected administrations to its clients as indicated by their requests.

Encryption and Decryption: Here we are utilizing the blend of ABE and BRE calculation to encode and decode the records.

Document Upload and Download: The records which are transferred on cloud are encrypted frame. Clients can download the record which is decoded on the off chance that he is approved.

B. PROPOSED SYSTEM ENCRYPTION ALGORITHM

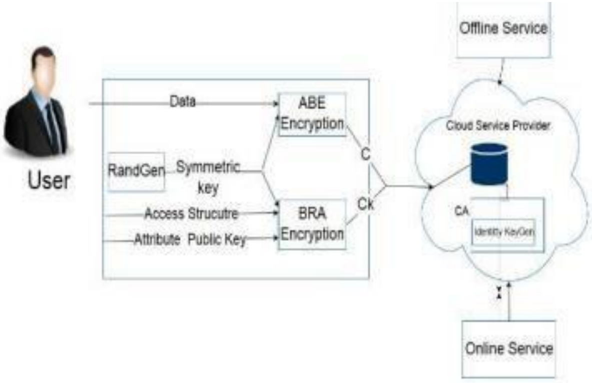

Figure 2: Encryption Diagram

In our proposed framework information is encrypted before transferring to the cloud. Blend of Attribute Based Encryption and Byte Rotation Algorithm are utilized for the encryption of the information. ABE will distinguish the attributes of the information and BREA will perform grid tasks on the piece of the information to be encrypted. In the wake of performing encryption task, an arbitrary key is created close by the encrypted information. Information will be send in encrypted organization to separate client. To unscramble this information recipient needs to enter the One Time Password (OTP) which will be coordinated with key produced utilizing ABE algorithm.

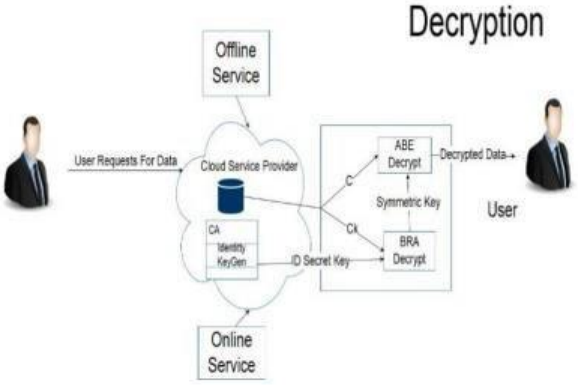

Figure3:DecryptionDiagram

C. PROPOSED SYSTEM ALGORITHM

Step-1: Start
Step-2: Accept the data from the user.
Step-3: The Attributes of the data from the users' formats are obtained by the Attribute-Based Encryption.
Step-4: With the help of these Attributes, Random Key is generated, and type of data is obtained for encryption by BRE algorithm.
Step-5: The data is converted into equal number of blocks and N x N matrix will be generated on the basis of these blocks.
Step-6: Based on no. of blocks, pool of threads will be created.
Step-7: Run the threads in multi core system to create encrypted data in short amount of time.
Step-8: A secret key is generated in order to open the encrypted file which is stored in the cloud.

Step-9: The secret key is shared to the user via email or mobile number of the authorised user. This key will be used to decrypt the encrypted file.
Step-10: The file selected will be decrypted in the original form using the key.
Step-11: Stop.

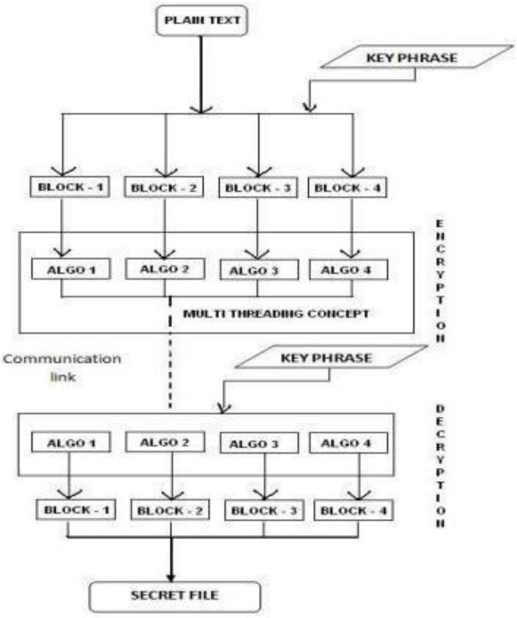

Figure 4: Flow Diagram

IV. CONCLUSIONS

Cloud computing now is everywhere. In many cases, users are using the cloud without knowing they are using it. Small and medium organizations will move to cloud computing because it will support fast access to their application and reduce the cost of infrastructure. The Cloud computing is not only a technical solution but also a business model that computing power can be sold and rented. Cloud computing is focused on delivering services. Organization data are being hosted in the cloud. The ownership of data is decreasing while agility and responsiveness are increasing. Organizations now are trying to avoid focusing on IT infrastructure. They need to focus on their business process to increase profitability. Therefore, the importance of cloud computing is increasing, becoming a huge market and receiving much attention from the academic and industrial communities. In this paper we discussed the feasible approach to maintain integrity and secure data sharing in cloud computing.

REFERENCES

[1] M. Hammoudeh and T. A. Alsboui, “Building programming abstractions for wireless sensor networks using watershed segmentation,” in Smart Spaces and Next Generation Wired/Wireless Networking, pp. 587–597, Springer, Berlin, Heidelberg, 2011.

[2] A. Aloraini and M. Hammoudeh, “A survey on data confidentiality and privacy in cloud computing,” in Proceedings of the International Conference on Future Networks and Distributed Systems, ICFNDS ’17, (New York, NY, USA), pp. 10:1–10:7, ACM, 2017.

[3] J. K. Mohsin, L. Han, M. Hammoudeh, and R. Hegarty, “Two factor vs multi-factor, an authentication battle in mobile cloud computing environments,” in Proceedings of the International Conference on Future Networks and Distributed Systems, ICFNDS ’17, (New York, NY, USA), pp. 39:1– 39:10, ACM, 2017.

[4] A. Carlin, M. Hammoudeh, and O. Aldabbas, “Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges,” International Journal of Advanced Computer Science and Applications, vol. 6, no. 6, 2015.

[5] G. C. Deka, Handbook of Research on Securing Cloud-Based Databases with Biometric Applications. IGI Global, 2014.

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

[7] W. Itani, A. Kayssi, and A. Chehab, “Energy-efficient incremental integrity for securing storage in mobile cloud computing,” in Energy Aware Computing (ICEAC), 2010 International Conference on, 2010, pp. 1–2.