International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Cloud Storage with Added Data Security and Integrity

Reshmi Das M V[1], R Charanya[2]

[1],[2]Vellore Institute of Technology, School of Information Technology and Engineering, Vellore , Tamilnadu

Abstract: ***Cloud storage helps user to store and access data over the internet irrespective of their location. As the cloud services are cheap and very easy to access there has been a drastic increase in cloud users all over the world. These cloud providers provide storage services facilitating fast access to large set of data, but there have been many security concerns which include data privacy, confidentiality and integrity. Studies show that user's data might get compromised over the cloud as existing cloud service providers do not assure data privacy to their users. To protect user's data stored over cloud this work proposes a cloud storage system which will provide encrypted storage for their data. RC6 encryption is used in this system to provide data encryption over cloud. As the data are stored in encrypted format, it is difficult to misuse others data. Also SHA3-keccak algorithm is added to ensure data integrity. With added integrity user will be able to identify if his data is modified or corrupted disabling inappropriate contents from getting downloaded to the system.***

Keywords: cloud, data security, data integrity, rivest cipher 6, keccak-SHA3

1. Introduction

Cloud storage services help users to store, share and access their data over cloud using the help internet. With help of cloud data is stored and maintained remotely which makes it very easy for the user to access or share his data from any location by access to internet. Many of the services are free to few gigabytes, with added storage space on payment. For large organizations backing up their data over cloud is more easy and efficient as the data is backed up by over an external server which can be accessed over net. Many storage providers are popular among users which include dropbox, Google drive, sky drive and box. But hackers have succeeded to hack the user accounts on these services. With drastic increase in the usage of cloud storage services which is cheap and easy to access, concerns have been raised as user data might get compromised over the cloud. Many surveys have recorded several threats like dos attacks, cloud malware injection, side channel attack, man in the middle attack (MITM), authentication attacks which have succeeded to pose threats to user data stored over cloud leading to misuse of user's confidential data affecting user privacy over cloud. Existing cloud service providers provide only storage of user data, there is no security assured by their service providers. In order to overcome security issues this work proposes a cloud storage system which provides encrypted storage of data over cloud. With the help of encrypted storage data security can assured to a greater extent compared to the existing system. Even if the hacker succeeds to hack user account he will get access to the encrypted data which will be of no use to the hacker as it is in an encrypted format which makes sense only after decryption, and the decryption needs a secret key which only the user will know. Thus the hackers cannot misuse user data easily like the existing systems. With the addition of integrity check using SHA3-keccak[9] data integrity is checked to prevent any inappropriate contents from entering the system along with assuring integrity of user's data.

2. Literature survey

Louai A. Maghrabi in [1] has studied the threats affecting user's data privacy over cloud. He has done a survey on the students in his institution by studying how they use the cloud services and found 82.5%[1] of students use cloud services. Of this 81.8% of users use the cloud storage for storing their data. But more than 56% of them are not sure whether their data is safe, they doubt if someone else peek into his data and misuse it affecting the users privacy adversely. This reveals the level of security provided by the existing cloud service providers(csp), which demands for improved security measures over the cloud to protect user's data. In [2] Farhan Bashir Shaikh and Sajjad Haider has done a survey based on the existing results available and the feedback from users on the quality of service provided over cloud and the security concerns which threaten them. Based on this study this work has come up ranking security of data as biggest threat over cloud.

Many researchers have come up with proposals to protect data over cloud but one or other had disadvantages which makes them unfit for use in real time systems. In work [3] Arjun Kumar, Byung Gook Lee, HoonJae Lee and Anu Kumari have come up with a solution using elliptic curve cryptography (ECC). But this algorithm is complex and tough when implementing which makes it difficult to use in an real time system as the chances of failure and error's are very high. Also this algorithm requires complex mathematical computations which increase time overhead. M. A. AlZain, Ben Soh and Eric Pardede in [4] have come up with a solution using Shamir secret sharing algorithm. But using this algorithm is also not feasible as the algorithm demands n shares of the data which will stored over n cloud server's, which is very difficult to maintain and expensive. There have been proposals to use fully homomorphic[5] algorithm to protect data over cloud but this algorithm has implementation issues and added complexity in algorithm also it has snail like execution speed. Other works have used blowfish [6], proxy-re encryption[7] but these algorithms

have their drawbacks which make it not to the level needed for protecting user's data privacy over cloud.

3. Proposed model

In this work a cloud storage system is proposed which makes use of encrypted storage over the server than the actual file as in case of existing system. An offline cloud server is setup which will enable to demonstrate how the proposed system will work. Using this user can login if already registered else user has to register first, and then the user can select file he wants to share over cloud and upload the file. When the file gets uploaded user has to enter a secret key and then the file is hashed using keccak[9] algorithm also it gets encrypted automatically using RC6[8] algorithm and this encrypted file will be stored over cloud. User will have his files stored over the cloud in an encrypted format which is the cipher, so anyone if enter the system other than the registered user he won't be able to understand or use the file. Only after the file is decrypted anyone can read the file but only user knows the secret key used so the data privacy is preserved. After the upload user can decrypt his file by selecting the file and downloading, during the process he has to enter the secret key and when the download process is executed the file gets decrypted and a new hash value is generated which will be compared with the old hash value. If both hash values match the file's integrity is protected and file will be downloaded. User will have his normal text file in the downloads folder

4. Design

System design gives a clear view of how the proposed system is designed; the major functionalities are encryption, hashing and decryption. User can easily use this system by registering for an account and the logging in to his account. After logging in user is free to select his file of interest which the user wants to share over cloud. Now he just has to select upload option to store his file in an encrypted format over cloud. When upload option is submitted by user the file is hashed using SHA-3 keccak[9] and the hash value will be stored in the database also the file will get encrypted using the RC6[8] algorithm automatically. This process is clearly visible in the system design Fig1. In his system the user can also retrieve his files whenever he need access to, the user just has to select file stored over cloud and submit download option. When the download option is submitted file is downloaded but it will be in the cipher format which no one can understand, so the file has to be decrypted. This decryption process is done in the background by the system itself, the file is decrypted by the RC6[8] algorithm and now an integrity check is done. This integrity check process requires generating new hash value for the decrypted file and old hash value stored. If both hash values match the file will be downloaded successfully to the users system, else download process is terminated. With the help of this integrity check unwanted files won't be able to enter user system protecting user's privacy to a greater extent.

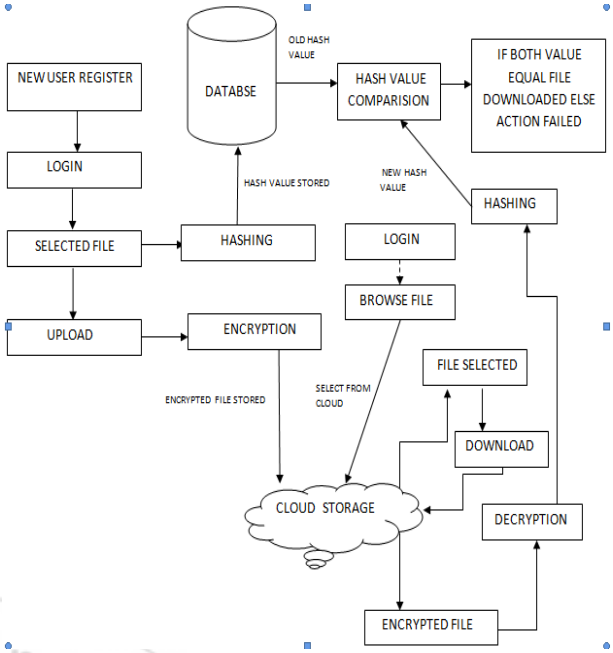

Figure 1: system design

5. Results

RC6[8] algorithm used for providing data encryption is known for its simplicity and it adds to the security provided. This algorithm is not vulnerable to known attacks like MITM, linear and differential cryptanalysis, side channel attacks and brute force attacks. In this work the performance is studied by recording time needed for executing the RC6[8] encryption and decryption process for files of various size, and a graph is generate Fig2 below is the graph generated, and the graph clearly explains that the algorithm execution time is very less which promises a system with no time overhead. Also RC6[8] code takes very less memory in terms of lines of code and also during execution

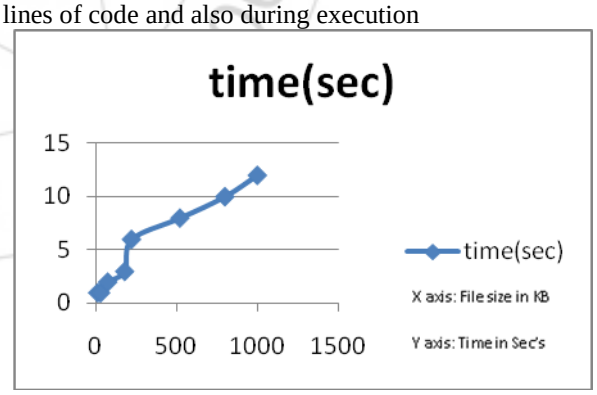

Figure 2: RC6 execution time

Even the hashing algorithm is very fast and provides more security than the older versions.

6. Future Work

In this work we have demonstrated that cloud data can be protected with using RC6[8] encryption and also data integrity can be assured using keccak[9] algorithm using an offline server. If this can be employed in the cloud storage systems as default then user can safely share their data over

cloud as the data will be getting stored in encrypted format which cannot be misused.

7. Conclusion

With use of RC6[8] encrypted storage and integrity protection with keccak[9] hashing, more secured storage is provided for user. As RC6[8] is not vulnerable to known attacks security is ensured compared to other algorithms which are vulnerable to side channel attack. Also the keccak[9] hash function is very fast compared to sha-2 ensuring high computation speed.

References

[1] louai a. maghrabi "the threats of data security over the cloud as perceived by experts and university students", 2014 IEEE
[2] Farhan bashir shaikh, sajjad haider, "security threats in cloud computing", 6th international conference on internet technology and secured transactions, 11-14 december 2011, abu dhabi, united arab emirates.
[3] Arjun Kumar, Byung Gook Lee, HoonJae Lee and Anu Kumari, "Secure Storage and Access of Data in Cloud Computing", 2012,IEEE.
[4] M. A. AlZain, Ben Soh and Eric Pardede, "A New Approach Using Redundancy Technique to Improve Security in Cloud Computing," Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference publications
[5] Feng Zhao , Chao Li , Chun Feng Liu, "A cloud computing security solution based on fully homomorphic encryption" Feb 2014, ICACT.
[6] Md Mozammil Alam, Sourav Hati, Debashis De, Samiran Chattopadhyay," Secure Sharing of Mobile Device Data using Public Cloud", 2014 IEEE.
[7] Jiang Zhang, and Zhenfeng Zhang," Secure and Efficient Data-Sharing in Clouds", 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies.
[8] H.E.H. Ahmed, H.M. Kalash and O.S. Farag Allah "Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images", 2012 IEEE.
[9] Bernhard Jungky, Marc StottingeR "Among Slow Dwarfs and Fast Giants:A Systematic Design Space Exploration of KECCAK", 2013 IEEE.

Author Profile

Reshmi Das. M. V recieved B. Tech in Computer Science and Engineering from Marathanassius College of Engineering in 2012 and now she is studying M. Tech at VIT University.

Charanya. R is Assistant Professor at VIT University, She has earned his Bachelors in Computer Science and Engineering and Masters of Engineering in Software Engineering from Anna University, She has published extensively in International Conference and Journals. Her research interest are in the areas are Cloud Computing, Software Engineering and network security