iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** V **Month of publication:** May 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secured Data Search over Cloud

K. Priyatham[1], Mr. Arif Mohammad Abdul[2], Mrs. M. Shanthi[3]
Student, Department of Computer Science, Assistant Professor
Department of Computer Science, GITAM University, Hyderabad

Abstract: Cloud computing is one of the best feature where organizations are interested. The security provided to the cloud ensures the confidentiality of the data in the cloud database to the organizations for the usage of cloud services. To ensure the security to the data, we use different tools in the cloud. Hence a tool by name Opses is used to improve the security level during the process of data search in the cloud. This tool results in the increase of security to the data in the cloud.
Keywords – Cloud computing, Opses tool, Cloud services, Cloud database

I. INTRODUCTION

Organizations use the cloud database to store the sensitive data. Intruders try to grab this data either from database or during the process of transmission. Hence the theft of data in the cloud became quite often and this results in the confidentiality issues to the data in the database. Hence the organizations are hesitating to adopt the cloud services as the security to their sensitive data gets lost. In order to improve the security to the data in the database and during the transmission of data, a powerful tool called Opses is used. This Opses tool uses the traditional methods but in a different manner to protect the security of the data. Here we encrypt the data at multiple levels with different algorithms to maintain the confidentiality of data in the cloud. Along with the traditional methods of encryption, we use CryptDB as the database to increase the security to the data. This Opses tool checks the security level of the client when the tool is used in the client system to ensure the security. If there is any malicious program running in the client's system hardware then it notifies the client about the malicious program. It also uses the servers to examine the encryption and decryption process resulting in the security. Servers like SUNDR, SPORC are used to maintain the confidentiality during the process of encryption and decryption process of data. When there is any attack or attempt to attack on the data during the process of encryption by the hackers, then the attack is updated to the client. Hence the client is aware of the security provided to the data during the encryption and takes the required preventive measures to secure the data. CryptDB is a SQL type of database, where the requests are sent to the database in the form of queries. The client gives the request in general text format where this request is further converted as SQL query and sent to the database. The CryptDB is different from other databases in terms of security. This CryptDB database provides additional security to the data in the database. To increase the security provided by the cloud service provider and the database to the data, the concept of DAAS (Database As A Service) is used. This DAAS provides the additional layer of security to the data resulting in the increased security level to the data in the database. This DAAS security is applied just before the data is stored in the database. Hence DAAS provides security layer just before the security layer provided by the database. To ensure the security during the transfer of data between the client and server or vice-versa, a widely used special tool for security called Scyther is used. When this tool is used, it identifies nodes during the transfer of data and checks the secure transmission of data. Hence additional layer of security is implemented during the data transfer. This Scyther tool gets activated, when it senses the transmission of data in the network. As the number of files increases in the database, the number of keys used for encryption also increases. Hence it becomes difficult to compute the large number of keys. So the concept of multi-key is a disadvantage when the number of keys gets increased. So the numbers of keys used for encryption are optimized by taking the same encryption key for the similar words in the file. Hence the number of keys that are being used gets reduced and the computation over this keys becomes easier. Along with the usage of multiple tools, a traditional concept of Tunneling is used. Tunneling encrypts the data during the transfer of data and decrypts the data if any higher or lower versions of IP address are sensed within the network. This tunneling ensures the additional layer of security to the data during the transfer of data. Though the network itself uses the concept of tunneling to avoid the problems of IP address conflicts in the network, we just concentrate on the security to the data ignoring the IP conflicts.

II. ARCHITECTURE

Typically, the architecture of Opses tool consists of client and server along with the identity module. Each module has its individual functionality for maintaining the confidentiality to the data in the cloud. This tool is used in public cloud and private cloud but the

registration of a client must be done in private cloud and the remaining tasks can be done in both private and public clouds. The client consists of the browser enabled application where, the client logins with the username and password. Then the client is prompted with another field called Identity Provider (IPR) to authenticate the client. When this identity is authenticated, then the client is provided with the complete access to the respective account. In the client window, client is able to upload files to cloud database and retrieves the file again by providing the relative keyword as a search key to identify the file in the database. When the client tries to upload a file, this file is encrypted and reaches the organization for further encryption of the file and then it is uploaded to the cloud database. Hence the encryption of file and checking the file takes place again before uploading to the cloud database. The encryption key used by the organization and the client are different and the client encryption key is unaware of organization though the encryption key is generated by the Organization. When the file is received from the organization, the database administrator encrypts the file once again before uploading into the database. When the administrator uploads file, the CryptDB performs onion layers encryption on the file and saves it in the database. Hence the confidentiality to the file is maintained and even if the administrator compromises in terms of security, there will be no loss of data. Hence the security provided to the data is strong enough to maintain the confidentiality of the data. During the process of encryption and decryption, servers like SUNDR, SPORC etc are used to maintain confidentiality during the encryption process. These servers identify the attacks on the encryption process and update the client about the attacks. These servers also detects any malicious server in the network and tries to avoid the usage of this malicious server and during this time it also tries rectify the malicious server in the network.

III. SYSTEM OVERVIEW

The usage of the servers like SUNDR, SPORC increases the confidentiality of the data. SPORC is a generic framework for building a wide variety of applications. SPORC flexibility can be defined by using the prototype applications namely, causally-consistent key-value store and a browser-based collaborative text editor. But theoretically, we use Fork consistency and Operational transformation. SPORC provides a generic collaboration service where it provides access to the control list to perform operations even if it is disconnected. SPORC comprises of set of client devices in the network which has access to the control list where the access to the users can be updated and potentially used to identify the malicious server in the network. The server receives updates from the clients and orders them. In order to fulfill the tasks, here SPORC uses the concept of Fork consistency and Operational transformation (OT). Operational transformation (OT) provides general model for synchronizing the shared state and performs the tasks required for the clients. In Operational transformation, an application defines set of operations from which the modifications to be performed over a document are constructed. Fork Consistency prevents the malicious server or forging the unauthorized client's operations by using the SPORC digitally signed user's private key. This is not a perfect method to secure data but this process results in better security to the data in the network. SUNDR is a server, which has a different type of file system where the hacker or intruder is unaware of the file system and this result in greater security to the data. SUNDR protocol is a protocol used by SUNDR, where the concept of fork consistency is used and it identifies the misbehaving server and from forging and notifies to the client. The timestamp box is used for the applications done on the file by the user and this timestamp box refreshes for every 5seconds and the user applications can be notified with respect to time. After the completion of encryption process at user level, the encrypted file is sent to the database where the onion layer of encryption is done before the data is stored into the database. The database administrator monitors the performance of the database and grants the access of file to the user depending upon the request sent by the user. Hence even if the database administrator compromises in terms of security there will be no loss of data. The algorithm used during the process of encryption at user level is symmetric AES of 128bit. There are many other algorithms for encryption but this algorithm results in better performance when the cipher text of greater than 64bit is obtained. The sequential steps of algorithm is,

A. Encrypt the entire text using the key of the user.
B. Send the cipher text to the respective user.
C. Check the cipher text of the file obtained during the encryption and the cipher obtained with the file.
D. Decrypt the file at user browser, if the cipher text matches.

During the process of onion layer of encryption done by the CryptDB, each layer uses different algorithms to maintain the confidentiality. Algorithms like DET, RND, Homomorphic encryption etc are used for different level.

When DET algorithm is decrypted complete data is obtained. When RND algorithm is decrypted, then the structure of data is leaked

but not the complete data. The RND algorithm is applied over the DET algorithm. Homomorphic encryption is lower level of encryption where this is applied only arithmetic operations like additions and multiplications. These algorithms help in maintain the security to the data and computing over encrypted data in the database. The transaction requests like storing the data in the database, retrieving the data from the database is are encrypted and sent to the database. These encrypted requests must compute over the encrypted data and produce required output. Similarly the data that is sent to the user is decrypted at the user's browser in order to maintain the confidentiality of the data during the transfer of data from the server to user. Hence the three major data threats, database administrator compromise, data loss during the transfer and during the process of encryption and decryption are avoided. But during this process the concept of sharing is ignored.

IV. CONCLUSION

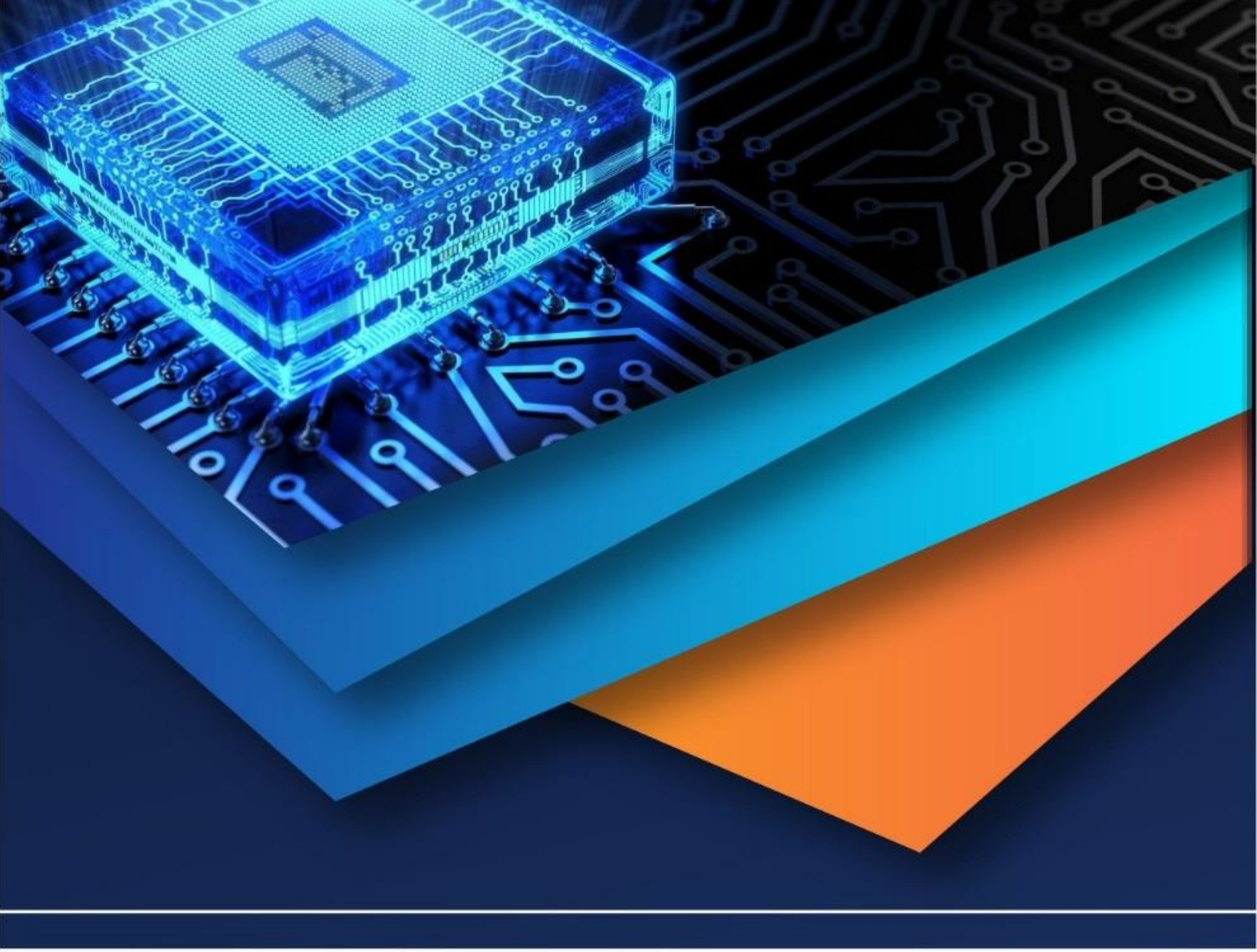
The three major data threats are avoided. The Opses helps in maintain the security to the data during the transfer. This tool enables the users to search the data from the database without any loss of data, when the data enters into web from the database. This tool always provides good medium for identification of misbehaving servers and notifies the users about the threat level to the data. This tool is one among the strong tool to improve the security provided to the data in the web during the process of searching.

V. FUTURE Work

The concept of files between the users is omitted as the user is unable to identify the unauthorized users. The medium of communication is also omitted. The process of authentication of the users must be strong enough to improve the security level provided by the tool. Users are unaware of the files that are being uploaded by the other users.

REFERENCES

[1] Cryptocat: Adopting Accessibility and Ease of Use as Security Properties by NadimKobeissi, Arlo Breault
[2] DAAS: Database As A Service by Carlo Curino, Evan P. C. Jones, Raluca Ada Popa, NirmeshMalviya, Eugene Wu, Sam Madden, HariBalakrishnan, NickolaiZeldovich
[3] Multi-Key Searchable Encryption by Raluca Ada Popa and NickolaiZeldovich
[4] CryptDB: Protecting Confidentiality with Encrypted Query Processing by Raluca Ada Popa, Catherine
[5] M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan MIT CSAIL 5. SPORC: Group Collaboration using Untrusted Cloud Resources by Ariel J. Feldman. 6. SUNDR: Secure Untrusted
[6] Data Repository (SUNDR) by Jinyuan Li, Maxwell Krohn, David Mazi`eres, and Dennis Shasha.
[7] The Cloud databases: http://en.wikipedia.org/wiki/Cloud_database
[8] Cloud database types: http://readwrite.com/2011/01/12/7-cloud-based-database-service.
[9] Building web applications on top of encrypted data using Opses by Raluca Ada Popa, Emily Stark, Jonas Helfer, Steven Valdez, Nickolai Zeldovich, M. Frans Kaashoek, and Hari Balakrishnan MIT CSAIL and Meteor Development Group.
[10] Survey on databases in the cloud environment by Priyatham, Arif Mohammad Abdul, and Shanthi.
[11] Database management in Cloud Computing: http://www.itmanagerdaily.com/database-management/
[12] Featured databases in cloud computing:http://www.databasejournal.com/features/mssql/should-you-move-your-mysql-database-to-the-cloud.html
[13] Tools for providing security to cloud: http://www.hongkiat.com/blog/cloud-security-tools/
[14] The Cloud management: http://searchcloudcomputing.techtarget.com/report/Cloud-management-tools-guide-for-beginners
[15] Cloud computing tools: Improving security through visibility and automation: http://www.csoonline.com/article/2131715/identity-access/cloud-computing-tools--improving-security-through-visibility-and-automation.html



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY