World Engineering & Applied Sciences Journal 7 (3): 194-199, 2016
ISSN 2079-2204

DOI: 10.5829/idosi.weasj.2016.7.3.22982

Providing Secure Database as a Service with Encrypted Queryprocessing in Cloud

P. Reeta and J. Jesila Mol

Department-MCA, Faculty of Computing,
Sathyabama University, Chennai-600119, Tamilnadu, India

Abstract: The cloud computing is being used for scaling the provided service for providing the service over internet as per the requirement. The technology over the cloud computing is using the remote servers by internet for storing the application and data. The cloud storage is allowing the data to be getting stored in the digital form in the logical pools. The storage is most popular and trustable characteristics for rapid grow in cloud computing within the quality in intermediate accessibility through internet interface or the management system within web-based. The providers of cloud storage are storing the content or data in multiple cloud servers in distributed form. The security is the main concern in cloud storage. The issues of security are being concern while distributing the storage space in several locations, the risk of the unauthenticated physical space is also being concerned. To overcome on the major issues like automatic storage of cloud database and security in the cloud service, proposed technique is providing the better enhancement by utilizing the concurrent possible operations on the database services like confidentiality within cryptography. The context of data is placing the critical information in database of the cloud for ensuring confidentiality of data within the importance of paramount. The proposed technique is preserving the confide4ntiality of the stored content or data in the structure of database within the column and table information for the stored data. The secure DBaaS is providing the solution which is allowing the tenants of cloud for the advantages within the qualities of DBaaS like reliability, elastic scalability and availability without revealing unencrypted data to provider of cloud. The secure DBaaS is being applied on the any type of database; the encryption has been done within the AES (Advanced Encryption Standard) algorithm. The proposed technique is providing a better security model mechanism for authenticating, accountability and authorization for sharing the data over cloud environment.

Key words: DBaaS · Cryptography · AES · Banking Transaction · Metadata Management

INTRODUCTION

The cloud computing definition is being provided by the NIST (National Institute of Standards and Technology), NIST has stated that the cloud computing is enabling the convenient model, on-demand network accessing for pool sharing for configurable resources of computing which could provisioned rapidly and being released within minimum effort of management or interaction within service provider [1]. Recently, the huge growth of digital media is continuously demanding the rise of new network capacities and storage within the need of increased cost effective maintenance [2]. The proposed technique is solving the existing issues; the proposed technique is allocating the cloud space by banking process for any user, where users have to purchase the space. The existing system is processing the several guarantee approaches for confidential distribution of data for different providers of data by providing the additional advantages in form of secret key sharing. In this way, they had prevented the service provider top access and read the data or any portion of the data, but the security information could be able to get reconstructed by colluding the cloud providers [3]. The step has been forwarded through the proposed technique to ensure the possibility to execute the queries of range of data that is being robust in against of collusive providers. Several database management systems (DBMS) are offering the encryption of data at different file system through transparent encryption feature of file system. This proposed feature is building the trusted DBMS system over unreliable storage system [4]. However, the database management system (DBMS) is trusted and decrypting the data before using it. This

Corresponding Author: P. Reeta, Department-MCA, Faculty of Computing, Sathyabama University, Chennai-600119, Tamilnadu, India.

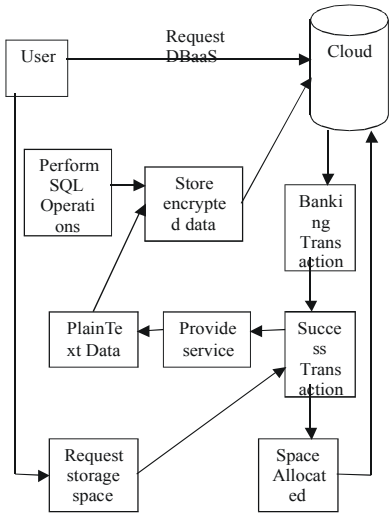
proposed approach is not applicable for considering the DBaaS context within the DBaaS, because it assume the cloud service provider is not trustable [5]. The service over the database, the model is providing the users power to create, modify, retrieve data and store, from anywhere and anytime by using internet access. It is introducing the several difficulties, in that one is data privacy. It is the context which specially provides the data privacy issues. The technique is exploring the execution of SQL queries fo encrypted data. The strategy is for processing the much possible queries for service provider without any decryption process of data which remind the processing of query has been performed at user site [6]. The DES is not providing the security against possible cloud attacks for proposing the systems which provides the security against of attack of the data modification within encryption concept for getting more secure and permission of accessing of data which could allow to accessing of data by deciding from data owner [7].

Related Work: The author of [9] has proposed the application existence which needs the maintenance of sensitiveness of programs for untreated hosts. The paper is proposing the development and design for trusted database system. The trusted database system is occupying a little space for protecting the untreated amount space. The validated and encrypted database is colliding at the resistant hash function over trusted space; so, the untreated program could be reading the database and modifying [8]. The trusted database is integrating the hashing and encryption function with the data model of bottom-level, which is protecting the metadata and data as system is building the system for conventional database. The exploiting system of development synergies are providing the log structured and hashing storage. The author [9, 10] has proposes atomic proxy re-encryption where semi trusted entity is converting the cipher text without knowing the plaintext information. They predicted a secure and fast re-encryption which is highly popular technique for managing the file system. The adoption of BBS re-encryption has been stuck by several of security risks. The recently followed work has presented novel re-encryption methods for realizing the stronger security notion. The author [11] has recently proposed a technique PoW method for data encryption. The file is being divided in to several number of file, where every file has an exact commitment over the data owner to make prove the data chunk possession with the precise commitment without revealing any sensitive information. However this information is not introducing the high computation cost as required from the system generation over all commitments for requesting the challenging proof. The authors [12] have proposed a projection scheme of bit-positioned file as ownership proof. The main advantage over this construction is for violating the privacy against honest server of cloud storage. The authors [13] have proposed an architecture of three layers which is protecting the leakage of information over cloud storage. The provided architecture is providing the three layer architecture for data protection, where first layer is not allowing the service provider to view the confidential data; the second layer is providing the security over data indexing and third layer specify the data use and policy indexing.

Proposed Work

Overview: The proposed technique is providing a novel methodology for cloud database integration services within confidentiality over data within the execution possibility over the concurrent data encryption operations. The first solution is supporting the client's distribution geographically for direct connection of cloud database encryption and concurrent execution of independent operations by including the modified structure of database. The possibility over the combination of scalability, availability and elasticity is typically distributing the DBaaS cloud service over data confidentiality for demonstrating the secureDBaaS prototype which supports the concurrent execution of independent operations to remotely encrypted database from many clients distribution over the unencrypted setup of DBaaS.

Architecture



Architecture

Proposed Method and Algorithm: The users have an initial process for registration over the web end. The users are providing the personal information over the cloud registration for this process. The server is approving the storing function in the database. The details of user accounts would be maintained secretly.

Metadata Management and Encryption: The metadata is generating by secure process of DBaaS which is containing the information by using necessary statements of SQL over encrypted database in transparent way to users. The user could create generate tables in the provided database in the table over cloud. Every plaintext in the database is being transformed unsecure format table. The user will be accessing the DBaaS clients, after successful table generation, where user could be able to generate the table into data. The table data is being encrypted within AES (Advanced Encryption Standard) algorithm.

Algorithm Description

Aes (Advanced Encryption Standard): AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.

- AES operates on a 4×4 array of bytes termed the state. For encryption, each round of AES (except the last round) consists of four stages:
- Add Round Key - each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
- Sub Bytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
- Shift Rows - a transposition step where each row of the state is shifted cyclically a certain number of steps.
- Mix Columns - a mixing operation which operates on the columns of the state, combining the four bytes in each column using a linear transformation.
- The final round replaces the Mix Columns stage with another instance of Add Round Key.

Dbaas Process and Extend Cloud Memory Space: The user performs the database SQL operation, where user altering the table information or data in the cloud storage in the database. The modification of the table will be doing encoding and encrypting the content in the cloud storage. User doesn't need a table for deleting and inserting operation in database.

RESULT AND DISCUSSION

Experimental Setup: The proposed system implements with following system configuration such as Intel(R) Pentium (R) processor, G2020 CPU with 2.90 GHz clock speed, Windows 7 Professional operating system and 4 GB RAM.

The above mentioned Table 4.1 is presenting the comparison of existing and proposed table. The simulation output is producing the better accuracy for proposed system. the proposed technique is performing well with both the stored procedure.

Accuracy Performance: The above mentioned Figure 4.2 is presenting the comparison result of existing and proposed technique over the stored procedure in DBaaS and AES technique. The proposed technique is better in both the circumstances and providing better result.

Quality and Efficiency: The above mentioned Figure 4.3 is presenting the comparison over existing and proposed technique. The simulation result is presenting the more efficiency and quality in compare to existing technique.

New Account Registration: The above mentioned Figure 4.4 is presenting the new account registration process, where user has to upload or provide their complete details to the bank server. The user will be able to create new account by providing the required details.

Table 4.1: Compare existing and proposed technique result

Database? Technique?	DBaaS	SQL	Accuracy percentage approximate
Proposed	90	95	92
Existing	70	80	78

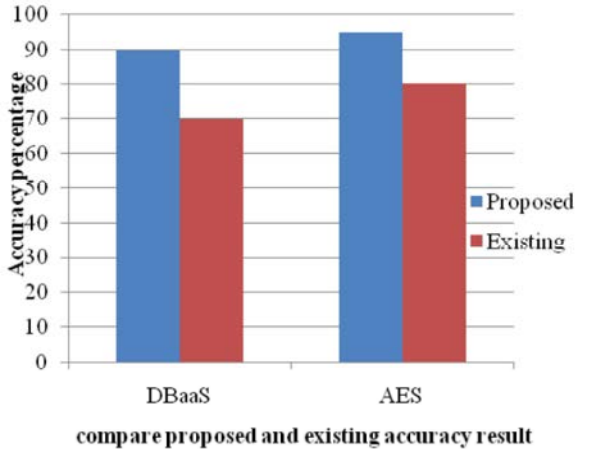


Fig. 4.2: compares existing and proposed technique result

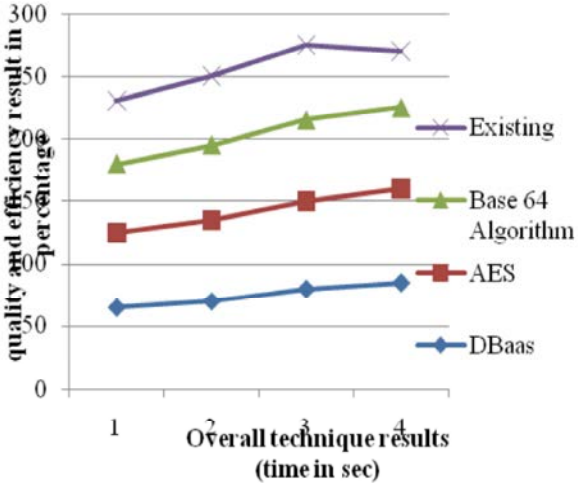


Fig. 4.3: Compare existing and proposed overall technique process result

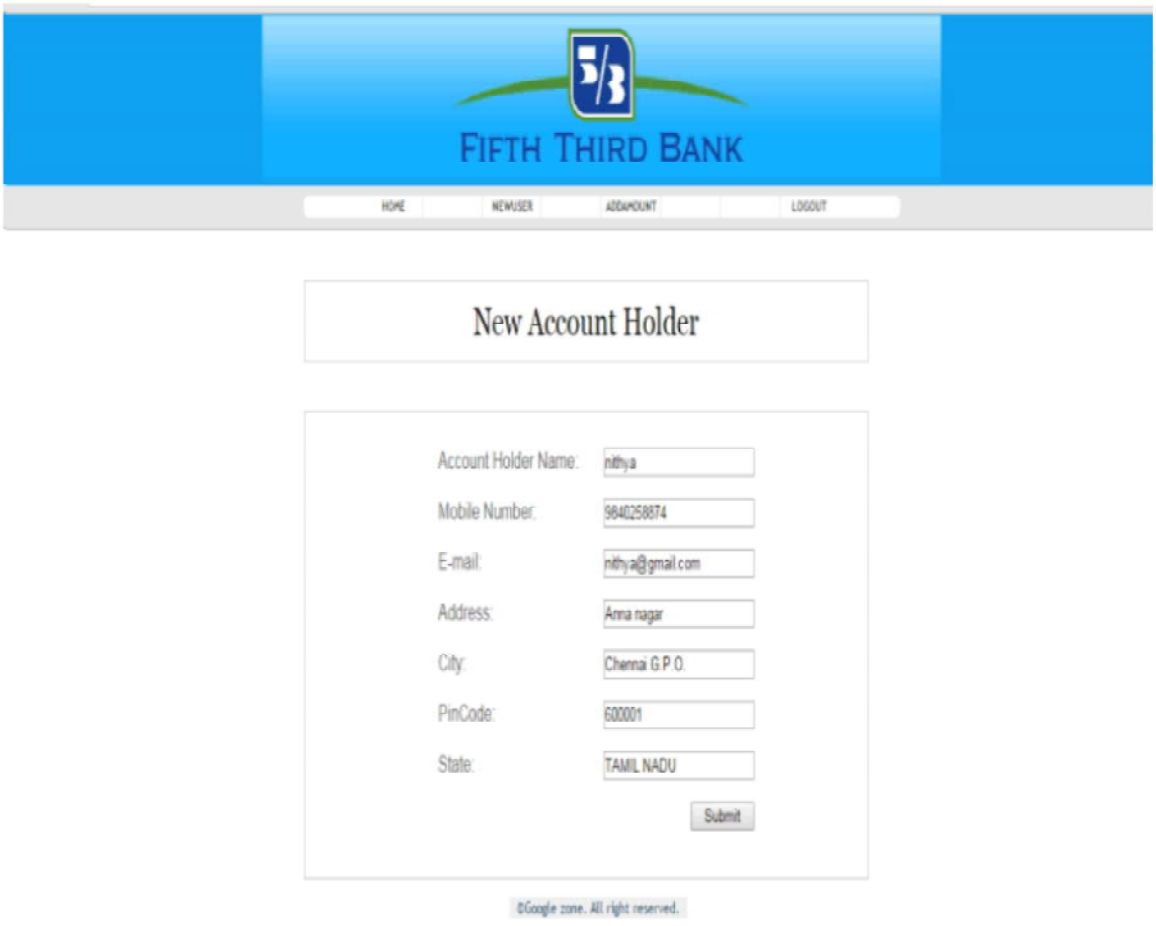


Fig. 4.4: New Account Registration

Adding Account: The above mentioned Figure 4.5 is presenting the user account details, where the details has been added or updated by the registered user.

Cloud Storage: The above mentioned Figure 4.6 has presented the cloud storage details, where user details are being uploaded in the secure cloud storage system.

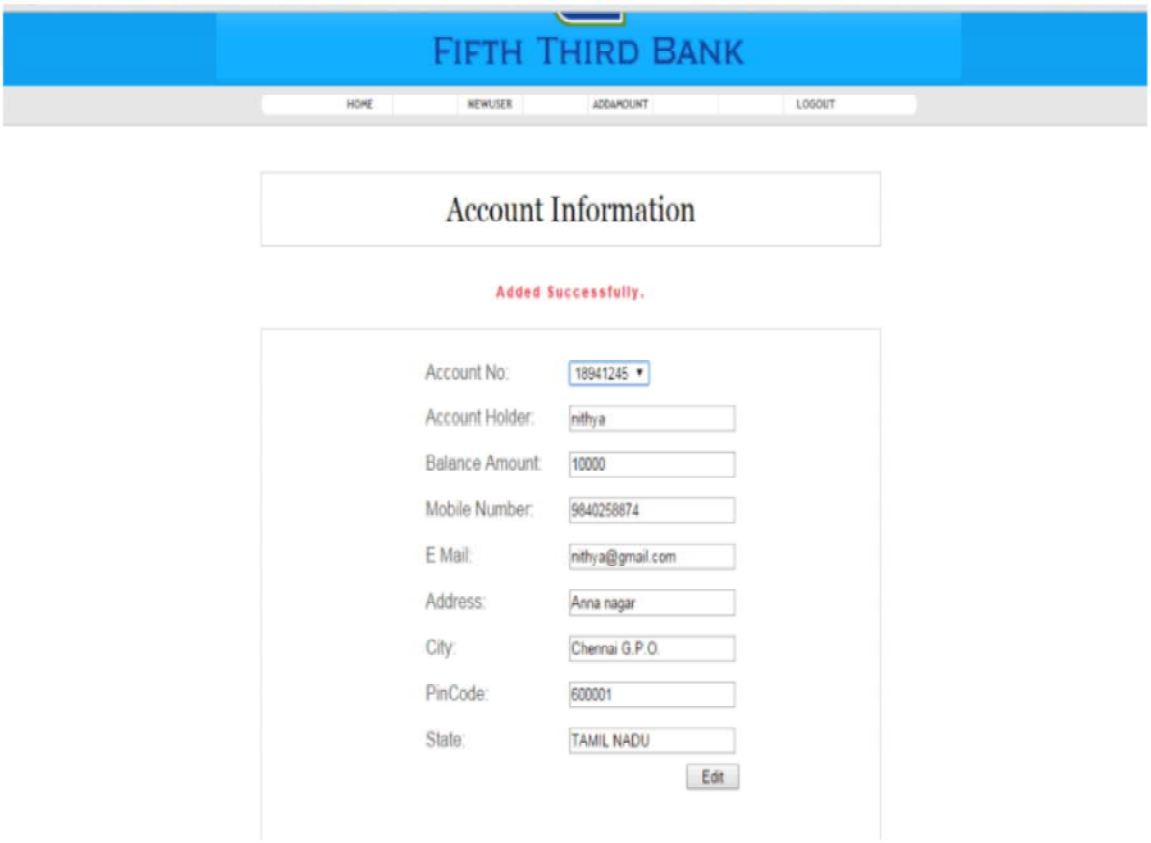


Fig. 4. 5: Account Information

Fig. 4.6: Cloud Storage

CONCLUSION

The proposed technique AES is providing a secure storage of data and automatic allocation in cloud memory, the problem hasn't any particular processing over cloud accessibility and data security within the proposed technique. The existing issues have been solved within the proposed technique for automatic allocation of memory over the banking process for shortage space for accessing the space in cloud. The storing procedure statement is creating the table in cloud space and encrypting data by the use of AES cryptography technique. The stored data could be get modify by the registered user only and unauthorized user will not be able to access without completing validation process.

REFERENCES

1. Dobale, Radha G. and R.P. Sonar, 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com Review of Load Balancing for Distributed Systems in Cloud Department of Computer Science and Engineering Amravati University, Maharashtra, India, 5(2).
2. A Secure Client Side Deduplication Scheme in Cloud Storage Environments Nesrine Kaaniche, Maryline Laurent Institut Mines-Telecom, Telecom SudParis, UMR CNRS 5157 SAMOVAR 9 rue Charles Fourier, 91011 Evry, France Email: fnesrine.kaaniche, maryline.laurentg@telecom-sudparis.eu 2014.
3. Mykletun, E. and G. Tsudik, 2006. Aggregation Queries in the Database-as-a-Service Model, Proc. 20th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security.
4. Agrawal, D., A.E. Abbadi, F. Emekci and A. Metwally, 2009. Database Management as a Service: Challenges and Opportunities, Proc. 25th IEEE Int'l Conf. Data Eng.
5. Ganapathy, V., D. Thomas, T. Feder, H. Garcia-Molina and R. Motwani, 2011. Distributing Data for Secure Database Services, Proc. Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc.
6. Varsha S. Agme, Archana C. Lomte and Varsha S. Agme, 2014. Cloud Data Storage Security Enhancement Using Identity Based Encryption BSIOTR, India 2 Prof. Archana C .Lomte, BSIOTR, Pune, India .
7. Ensuring Distributed Accountability for Data Sharing in Cloud Using AES and SHA.
8. Lonare Vikas Vitthal and J.N. Nandimath, PG Scholar, Computer Department, SKNCOE, Pune, Savitribai Phule Pune University, Professor, Computer Department, SKNCOE, Pune, India.
9. Maheshwari, U., R. Vingralek and W. Shapiro, 2000. How to build a trusted database system on untrusted storage, in Proc. Symposium on Operating System Design and Implementation - OSDI'00, pp: 135-150.
10. Ateniese, G., K. Fu, M. Green and S. Rosenberger, 2005. Improved proxy re-encryption schemes with applications to secure distributed storage, in Proc. Network and Distributed System Security Symposium, NDSS'05, pp: 1-15.
11. Ng, W.K., Y. Wen and H. Zhu, 2012. Private data de-duplication protocols in cloud storage. In Proceedings of the 27th Annual ACM Symposium on Applied Computing, SAC '12, New York, NY, USA, ACM, pp: 441-446.
12. Di, Pietro R. and A. Sorniotti, 2012. Boosting efficiency and security in proof of ownership for de-duplication, In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, ASIACCS '12, New York, NY, USA, ACM, pp: 81-82.
13. Squicciarini, A., S. Sundareswaran and D. Lin, 2010. Preventing Information Leakage from Indexing in the Cloud, Proc. IEEE Int'l Conf. Cloud Computing.