A SURVEY ON ADVENT OF THE DBaaS AND ITS ENHANCEMENTS

SUDHA K, MAGALAKSHMI S, PRIYADHARSHINI R, DHIVYAGANDHI M

Abstract— **Cloud computing is one of the upcoming technology of computer science in recent times. It uses the internet to maintain the data which is present into it and also the applications that provide numerous IT enabled service to its users. IaaS, PaaS, SaaS are some of the cloud provided services. The cloud users has become Para-amount in order to satisfy their expectation several additional services have been provided, DBaaS is one among them. The DBaaS allow the cloud users to be directly connected to the cloud database. It provides complete facility along with the security to manage their personal data by encrypting original data along with the access of SQL operation over the encrypted data which turns the DBaaS with more security that makes the normal DBaaS into SDBaaS (Secure Database as a Service). This paper portrays the survey on works that are carried out in the enhancement and development of the DBaaS and elaborate the issues involved in it with the table of comparison on its performance metrics.**

Index Terms*— *DBaaS, IaaS, PaaS, SaaS, SQL

I. INTRODUCTION

The term cloud refers to the network or the internet whereas cloud computing is the process of storing and processing the data into the network of remote location in spite of our own desktop computer.

In order to make cloud computing as a successful technology several things are needed to be addressed and enhanced such as Security management, load balancing, fault tolerance etc…

The research on the field of cloud computing is still in the development stage. The development activity starts from dividing the deployment model of cloud computing on the following ways.

A. *Public cloud*

A public cloud is a multi-user environment in which the resource, data and applications were outsourced and made commonly available to the public also it can be shared with any number of users (e.g. Amazon EC2)

B. *Private cloud*

The private cloud creates a shared environment between selective so that the resources and the applications were shared only between the limited users and the service is restricted to rest.

C. *Hybrid cloud*

Hybrid cloud is the mixture of both private cloud and public cloud whereas the critical data.

D. Community cloud

In community cloud the data or resources were shared between any two organizations in common. The communication lane is provided only between them.

The cloud also provides its service on the following category.

E. Infrastructure As A service (IaaS)

This service provides the support to the user by providing infrastructure as a service. The key feature to IaaS is virtualization that is nothing but the concept of on-demand-as service is indulged in it since the hardware resource (e.g.: virtual machines) were provided to the user based on requirement to the user.

F. Platform As A Service (PaaS)

This service support the user by providing the runtime environment (e.g.: Google app engine) whereas the user can make use of the web based application in spite of using from exact application.

G. Software As A Service (SaaS)

This service provides software application which is nothing but pay-as-per use that is developed and accessed via internet (e.g.: CRM)

Apart from the above service the cloud computing also provides various services. DBaaS is one among them and this paper fully deals with its advent and development.

The below mentioned are some of the issues in cloud computing technology which needs to be addressed.

H. Security risk

Though the data is outsourced into the internet in spite of our personal computer there is a need for the security enhancement in the data source, in which there is a

SUDHA K*, Computer science and engineering, Christ college of engineering and technology, Puducherry, India.*
MAGALAKSHMI S*, Computer science and engineering, Christ college of engineering and technology, Puducherry, India.*
PRIYADHARSHINI R*, Computer science and engineering, Christ college of engineering and technology, Puducherry, India.*
DHIVYAGANDHI M*, Computer science and engineering, Christ college of engineering and technology, Puducherry, India.*

chance for the third party or even the cloud providers to get the original value of the data and misuse to, so that proper confidentiality and availability for the data has to be ensured.

I. *Privacy*

The privacy is not yet properly provided to the user who owns for the data, in which the client who uploads the data will becomes the data owner and he/she has the complete rights over it which should not be open source to others.

J. *Fault tolerance*

As the clients valuable credentials are put into the cloud it has to be fault tolerance and should handle the failures effectively. It can be duly achieved by replication of data but it should not lead to data inconsistency.

K. *Performance and bandwidth cost*

The management of the sensitive data is made on the cloud require more cost since it requires virtual machine, load balancer and security tools etc… which has to reduce. But the reduction of cost should not simultaneously reduce the performance.

L. Infrastructure management

The hardware resources used in the data centers has to be properly maintained which may cause several thermal issues that has to addressed and preventive measures has to be taken.

II. RELATED WORKS

The development of the DBaaS supports the cloud users by making several enhancements during its development process.

The ideology of providing database as a service starts with the concept of NetDB2 which is nothing but a database service on the internet

[1] since in order to perform data manipulation the user will depend upon the database at the host site which is not economic where we will be in a position to buy expensive hardware and software so that the database as a service has arrived which allow the user to make use of it and give them the opportunity of creating the data, storing, retrieving and updating the data completely in the internet and it is the process carried out in NetDB2. In order to provide security the data is encrypted and inserted into the database. This is the origin of DBaaS.

[2] Since the DBaaS is provided and available through the internet which is vulnerable to theft and so it is necessary to provide security to the data present in it this is achieved in DBaaS through the concept of CRYPTDB. It protects the database from the third party by encrypting the original data before uploading it into the database with the help of a proxy based server. Users were allowed to upload their valuable data using passwords so that retrieval also strictly requires the appropriate password. CRYPTDB also use chain encryption mechanism to encrypt even the password of the user it provide high level of security as well as restrict the intruder. It is different to use the traditional queries over the encrypted data but CRYPTDB support around 126 SQL queries that too on the encrypted data.

[3] The DBaaS prevent the confidentiality of the data from the intruder and third party but there is a chance for the DBA (Database Administrator) or the service provider to access the data in order to provide complete privacy to the user the encrypted data is decrypted and provided only to the data owner which is achieved by splitting of queries. The data is stored in the form of encrypted format so that whenever the client post an request for data the data is encrypted at the client side itself and necessary comparison is made on the stored encrypted data and the original value of the data is strictly accessed only to client where the job of the provider is to have partial access over the data. Also execution of the all kinds of SQL queries was focused.

[4] The confidentiality has to be maintained not only from the DBA or the existing database but also the service has to be provided with the same efficiency to the relational database also which also considered to be untrusted so that the balance of the data between the existing database as well the to any directed or RDBMS.

[5] The DBaaS support the access of the data in an encrypted format but the time complexity may exceed when compare to plain data in order to avoid it and to make effective processing on encrypted data the concept of bucketisation or partition is introduced in this service which involves partition of certain range of queries and wrap up with a label and stored into the database so that accessing is made easy with the label value also the aggregation queries of SQL is also made easy to implement with this approach.

[6] The main threat to DBaaS was security issue which was resolved with the help of cryptography schemes but still there is a situation where when there is a continuous request for service from the clients of multiple locations to a single cloud database then it will be difficult to handle multiple clients and provide service to them at a same time. In such condition the load balancing problem occurs this can be solved with the help of distributed cloud database architecture where the data is stored in multiple sites of cloud database which in turn provide fault tolerance.

[7] Using proxy server or the intermediate server consists of several limitations. The availability of the data is not guaranteed because the encryption and decryption works were carried out by the proxy it may be subjected to bottleneck problem and the single point of failure occur in the proxy it results to failure of the entire service and the availability of the data is disturbed. This is a big threat to the DBaaS. Since the proxy is removed and all the

encryption activity were done in the client side itself so that the data travel from the client side to the provider side in an encrypted format

[8] The growth of the DBaaS turned from Database as a service to Secure Database as a service (SDBaaS) where the client side is considered to be trusted and the provider is untrusted the table, data, meta data were encrypted in the trusted side itself i.e. is called Secure Database as a Service client and thus transformed from the client to the provider so that any adversary cannot get the plain data. With this SDBaaS itself all the concurrent, distributed operations were possible.

This is the way in which the development of the DBaaS has occurred.

III. TECHNIQUES AND ALGORITHM

[1] *Blowfish* - The database as a service starts providing its service with the *blowfish* algorithm to achieve the encryption and decryption process. It is a 64 bit block cipher where the entire processes were carried out with 64 bit chunks. This algorithm use a user defined function for encryption and decryption the data owner encrypts the data meanwhile supplies the keys to decrypt only the owner holds the key and it is not given in the hand of the provider.

[2] *Chain encryption keys -* A good technique has been introduced for the data confidentiality since encrypting user's data alone is not sufficient it is necessary to encrypt the user's password also the CRYPTDB support this by *chain encryption keys* to user password. The process behind it is whenever a data is stored into the database the data is encrypted and the user will provide a password to the data and thus the chain keys were rooted in users password apart from user if any intruder tries to login the database the database which will not be possible even when the server is compromised as the password are rooted with chain keys. It uses the *symmetric key* encryption technique so that it uses the same key for both encryption and decryption.

[3] *Histogram-construction techniques* - Storing sensitive data in hands of cloud provider creates several issues since the DBA is not trust worthy. To avoid it the results were partitioned with the help of *histogram-construction techniques.*

[4] *Hash-based* - Uses *hash-based* method for the outsource of the data in the untrusted server and uses the B+ tree into the DBMSs

[5] *Bucketisation* - For effective retrieval and maintenance of data it is necessary to reduce the time complexity which is done through *bucketisation*. The bucketisation make effective access to the data by the way in which it partition the attributes and wrap up with a label so that with the help of labels accessing is performed on each bucket. Each bucket possess bucket id and each table contains field name.

[6] *Heuristic greedy hill climbing algorithm -* Fault tolerance is one of the features which are needed to be possessed by the cloud services so distributing the data and maintaining make the cloud database to fault tolerance. *Heuristic greedy hill climbing algorithm* is used for it. The hill climbing is a heuristic approach which in turn find whether the time taken to search result increase or not. If the search time increases then the process finds the best combination of variables by changing each variable at a time.

[7] *Removal of intermediate proxy* - In order to make the DBaaS to SDBaaS the intermediate proxy has been removed and all the processes when carried out into the client side itself. It is subject the originally encrypted key to re-encryption which is carried out while both read and write operation.

[8] *SDBaaS* - The advent of *SDBaaS* provides much security to the data which use the concept of Secure DBaaS client. The Secure DBaaS client includes original text, encrypted text, metadata and encrypted metadata.

IV. ADVANTAGES

- The arrival of DBaaS provides a convenient mechanism for the user to store their sensitive data in to the database through internet without purchasing the entire database.
- This service is pay-as-per user. So that the user can maintain their valuable data into the database and can pay according to their use.
- The security to the data is provided with the encryption standards. This does not provide the readability and accessibility to the intruder.
- The use of SQL queries into the encrypted data makes the reliability of the service in a secure manner.
- The implementation of encrypted data in the client side [8] make the data to travel securely from the client to the provider and

V. DISADVANTAGES

- The cost of designing the database as a service may be higher.
- The security threats are in high rate so many steps has to be taken to refine the security problems.
- Special care has to be taken and separate queries have to be used for the execution of the SQL queries over the encrypted data.
- If all the encryption process is made to carry on the client side then the service may not be a suitable on to the thin clients.

TABLE.1 COMPARITIVE ANALYSIS FOR STRENGTH AND LIMITATIONS IN DBaaS

S.NO	APPROACH USED IN THE ENHANCEMENT OF DBaaS	STRENGTHS	LIMITATIONS
I.	Providing DBaaS with blowfish as encryption and decryption algorithm.	The ideology of providing DBaaS avoids purchase of the hardware or software component. It provides service through online and saves the cost of purchase which is economically cheap.	When the DBaaS arrives initially focuses only on providing DBaaS and its security. It does not address the execution of the various SQL queries over the encrypted data.
II.	Protecting the user password by chain encryption.	Taking security measures on the DBaaS by encrypting the original data as well as use chain encryption technique for user password that makes the DBaaS much secure and provide confidentiality to the data.	The symmetric key encryption use same keys for encryption and decryption process. If any intruder identifies the key then it will be easy to gain the plain data.
III.	The database administrator is not considered as a trustworthy.	Execution of all kinds of queries in the encrypted database increased the flexibility level of the service.	Addressing of the security problem alone will not satisfy the client it is necessary to provide privacy to the data holder.
IV.	The intermediate proxy which is used to convert the original message to encrypted message and vice versa.	The removal of proxy based server avoids the bottleneck problem and increases the availability of data.	The proxy less architecture avoid bottle neck problem but it add more task on the client side.
V.	Use of SDBaaS makes all the encryption works to be done in the client side itself.	The arrival of SDBaaS makes all encryption work on the client side itself and provides good performance.	The Secure DBaaS client is tasked with more work i.e. all the encryption process is instructed to do on it.

VI. CONCLUSION

Cloud computing has created a revolution in the field of computer science. It satisfies the user with the service provided by it. The advent of the DBaaS support the data management and thus connect the client directly to the database constant security enhancement were made on this service which starts form the cryptographic schemes and even the SQL queries were allowed to use on it. But still the privacy to the user has not ensured properly, where the data own by the data holder have the complete access rights on it and he should decide the mode of access of the other clients. So the privilege has to be strictly set up by the data holder.

VII. REFERENCES

[1] H. Hacigu¨mu¨ s,, B. Iyer, and S. Mehrotra, “Providing Database as a Service,” Proc. 18th IEEE Int’l Conf. Data Eng., Feb. 2002.

[2] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan,“CryptDB: Protecting Confidentiality with Encrypted Query Processing,” Proc. 23rd ACM Symp. Operating Systems Principles, Oct. 2011.

[3] H. Hacigu¨mu¨ s,, B. Iyer, C. Li, and S. Mehrotra, “Executing SQL over Encrypted Data in the Database-Service-Provider Model,” Proc. ACM SIGMOD Int’l Conf. Management Data, June 2002.

[4] E. Damiani, S.D.C. Vimercati, S. Jajodia, S. Paraboschi, and P.Samarati, “Balancing Confidentiality and Efficiency in Untrusted Relational Dbmss,” Proc. Tenth ACM Conf. Computer and Comm. Security, Oct. 2003

[5] E. Mykletun and G. Tsudik, “Aggregation Queries in the Database-as-a-Service Model,” Proc. 20th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, July/Aug. 2006.

[6] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R.Motwani, “Distributing Data for Secure Database Services,” Proc. Fourth ACM Int’l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.

[7] L. Ferretti, M. Colajanni, and M. Marchetti, “Supporting Security and Consistency for Cloud Database,” Proc. Fourth Int’l Symp. Cyberspace Safety and Security, Dec. 2012.

[8] L. Ferretti, M. Colajanni, and M. Marchetti,,” Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases,”

[9] D. Agrawal, A.E. Abbadi, F. Emekci, and A. Metwally, “Database Management as a Service: Challenges and Opportunities,” Proc. 25th IEEE Int’l Conf. Data Eng., Mar.-Apr. 2009.

[10] A. Boldyreva, N. Chenette, and A. O’Neill, “Order-Preservingn Encryption Revisited: Improved Security Analysis and Alternative Solutions,” Proc. 31st Ann. Conf. Advances in Cryptology (CRYPTO ’11), Aug. 2011.

Sudha K, Working as an Assistant professor in Christ College of Engineering and Technology, Puducherry, India

Magalakshmi S, Perusing B.Tech degree in Christ College of Engineering and Technology, Puducherry, India

Priyadharshini R, perusing B.Tech degree in Christ College of Engineering and Technology, Puducherry, India

Dhivyagandhi M, perusing B.Tech degree in Christ College of Engineering and Technology, Puducherry, India