Two-Cloud Secure Database for Numeric-Related SQLRangeQueries with Privacy Preserving

[1]Kanad Kartey, [2]Vivek Madawat, [3]Harshil Somia, [4] Pallavi Mathur
[1,2,3]B.E Student, Dept. of Computer Engineering, D.Y.Patil Institute of Engineering & Technology, Ambi,
Pune University, Maharashtra, India
4Professor, Dept. of Computer Engineering, D.Y.Patil Institute of Engineering & Technology, Ambi,
Pune University, Maharashtra, India

Abstract: In the current scenario, companies and people are outsourcing the database to achieve useful administrations and applications of minimum effort. These are buried in the cloud server, which is beyond the control of the owner of the data. SQL queries require a secure database schema for their undeniable operation, but this finally causes a spill of privacy in the cloud server. For the investigation of numerical range (>, <, etc.) they forget to provide an adequate security insurance. A part of the difficulties faced are the loss of privacy of statistical attributes, access patterns, etc. In the same way, a larger number of queries will release more information to the cloud server. Therefore, with regard to these issues, numerous researchers have done numerous works. Some of these research works have been analyzed in the best possible ways to achieve the desired level of privacy preservation in the case of cloud computing. Some of the works studied are fuzzy logic, range queries, the order of CryptDB that preserves the encryption and the architecture of several clouds.

***IndexTerms* - cloud computing, database, privacy preserving, range query**

I. INTRODUCTION

Cloud Computing use for means computer (hardware and software) that are provided as a service through a network (usually INTERNET)).The name comes from the common use of the symbol in the form of a cloud as an abstraction for the complex infrastructure that it contains in the diagrams of the system.Remote computing services in the cloud with data, software and calculation of the trust of a user. Cloud computing, consisting of hardware and software resources on the Internet as third-party management services provided. These services usually have access to advanced software applications and high-end network servers.

The goal of cloud computing is to use traditional methods Super Computing ,or high performance computing is, usually used by military and research institutions that make zig billions of calculations per second, consumer-oriented applications such as financial portfolio management, personalized information on data storage to provide supplies or, in general, computer games immersive. Cloud computing applications networks large group of server it is usually executed with special connections of consumer PC technology to extend the computing tasks in them.This has been announced .The infrastructure includes large sets of systems that are linked together. Often the virtualization .The techniques are used to maximize the power of cloud computing.

Models of features and services:

The most outstanding characteristics of cloud computing are based on the definitions used by the National Institute of Standards and Terminology (NIST) are described below:

- **On demand auto service**: The consumer can without human interaction unilaterally provide computer functions, such as server and stored on demand automatically with each service provider.

- **Broad access to the network** : The functions are available remotely and are accessible through standard mechanisms, promoting the use of thin or thin heterogeneous platforms (such as mobile phones, laptops and PDAs).

- **Sharing of resources:** The provider of computing resources is grouped to obtain more consumers with a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to the consumer demand to see. Thither is a sense of location independence, that the client generally has no control or knowledge of the exact localisation of the resources provided, but may be able to place themselves at a higher degree of generalization (e.g., nation, state or datacenter).). Examples of resource storage, processing, storage, network bandwidth and virtual machines.

- **Rapid elasticity** : The skills are implemented quickly and flexibly, in some cases it can be scaled quickly and quickly to scale in publications. For the consumer, the supply possibilities often seem to be unlimited and can be purchased in any quantity and at any time.

- **Measured service** : Cloud systems automatically control and optimize resources by using a measurement capability at some level of abstraction of the type of service (such as storage, bandwidth and attached active processing, user accounts). The use of resources can be managed, controlled and recorded, the transparency of the provider and the consumer of the service used.

Characteristics of cloud computing

Service models:

Cloud computing includes three models, namely, infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). The three service models or layer through a layer of end users, which encapsulates the perspective of the completed end user cloud services. The model is shown in the figure below. If a user in the cloud infrastructure level access, for example, can run their own applications in the resources of a cloud infrastructure and will remain responsible for the support, maintenance and security of these applications. When you access a service at the application level, these tasks are usually administered by the cloud service provider.

Structure of the service models

Security is the main concern of cloud computing. Cloud customers face security threats from both outside and inside the cloud. Protecting the information from the server itself is the Pro of the most important questions in relation to it. By definition of the "lower class" of the product stack that adapts adequately to most known security methods, the server controls. How does the server in the cloud accept partial trust (honest but curious)?

CryptDB [5], a framework, confidentiality for applications that use database management frameworks (DBMSes). CryptDB allows queries on encrypted data, as well as the set of characterized operators, and queries on highly encrypted SQL data. CryptDB tends to be the danger of a curious database administrator (DBA), private information (for example, health books, financial articulations, individual data) learn with an eye to the DBMS server while maintaining the information DBA private efforts Some instruments are used to achieve this security functionality.

One of the devices is the order that preserves encryption (OPE) [11] [12] in General as part of the process of the SQL query database through the encrypted information used. It allows executing order operations in encrypted text, since the plain text for the Eg data server can fabricate index by performing rank queries to order [10] and the encrypted information, such as plain text. However, there are good reasons why, despite all the encrypted text, cover the order.

Therefore, the objective of security to protect the paged information of a server in the cloud will be stored refined by dividing the clouds of sensitive knowledge in two parts and in two non-cartel.

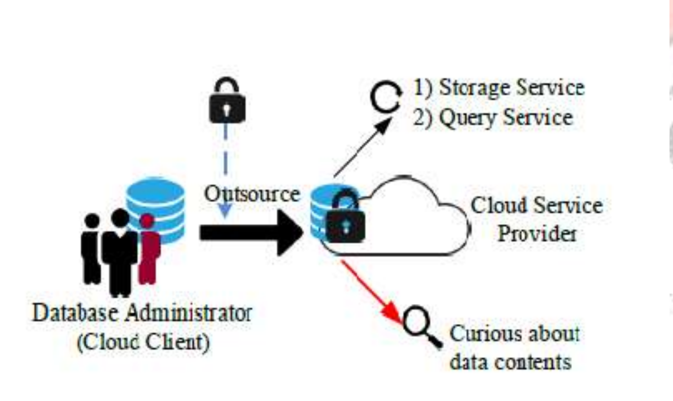

Fig. 1 Outsource database , service and privacy risk

Also a secure database service architecture is recognized cloud, in which the information and query logic is divided into two clouds, through the use of two non-consultation. From now on you can not perceive only a single cloud help to uncover private data. Differently as a succession of intersection protocols numerical questions relating to SQL pane [1] with the preservation of privacy give in addition carried out and it will not discover.

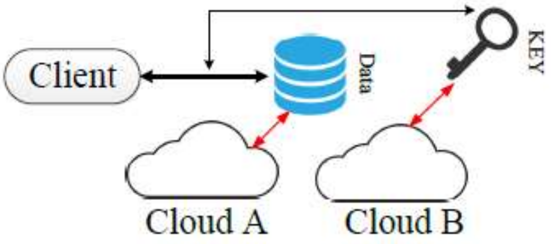

Fig. 2 Knowledge Partition of stored data

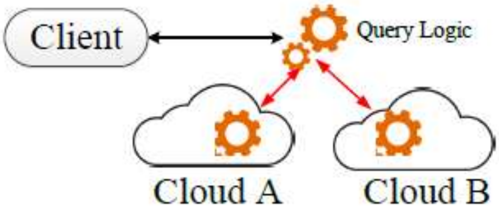

Fig. 3 Knowledge partition of query logic

II. MOTIVATION

Data protection is the most important factor in the cloud and modern data storage services. Many developers had an opportunity to protect security, but private data is not completely protected by any technique. All have private and confidential information, which they share with anyone, as well as with any company and organization, she has a large amount of private information, not the information provided by third parties. If the information is filtered, the organization is sure that it is a disgrace. With the destiny that we apply for the protection of confidential data. Today innovation has an opportunity in the preservation of privacy [7] in the cloud server in addition

III. RELATED WORK

John John Daugman and Piotr Zielinski have proposed a fast search algorithm for a large fuzzy database [9] that stores iris codes or data with a comparative binary structure. The nebulous nature of the iris codes and their high dimensionality is handled by the new procedure, Beacon Guided Search (BGS), which does so by breaking up a large turn of "beacons" in the search target space. BGS is considerably quicker than the present ES with a loss of immaterial precision. It requires considerably less memory and is not founded on the caching of stored data, which does away with the necessity for complex memory management. The preprocessing is basic and fast. It delivers up to 30% of bit errors in the inquiry and also up to seven cyclic rotations. The measure of abundance memory is small and quickly accessible: it reinforces dynamic maintenance, enhancing the simple order of new scripts.

Yin Yang, Hongwei Li, Mi Wen, Hongwei Luo and Rongxing LuSS, proposed an orderly ranking order scheme (RRQ) [10], which can reinforce both the rank query and the classified search. Established in the homomorphic Paillier cryptosystem, we use two super-large sequences for total multidimensional keywords. The first is used to add the multidimensional keywords of a buyer or seller to a collected number. The second one is connected to make a synopsis number accumulating the accumulated amounts of all the sellers. Security research shows that RRQ can achieve the confidentiality of keywords, confirmation, reliability of information and privacy of queries. In any case, meanwhile, the more complex prefiltering rules, for example, "y", "o", "no" do not end with the RRQ strategy.

RAPopa, C. Redfield, N.Zeldovich and H. Balakrishnan proposed CryptDB, a way for safeguarding private information in databases, from the curious cloud server . CryptDB includes, essentially, using range queries to productively complete the encrypted information using a novel SQL-based encoding scheme. Limits the discovered information to the interested database server. Irrespective of whether the protection safeguard assignment is met, some information is still detected in the operation.

Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant and Yirong Xu proposed Conserve order encryption for numerical data [11] that allows any comparison operation to connect directly to the encrypted information. The results of the query produced are solid (without false hits) and complete (without faults). OPES (Order Preserving Encryption Scheme) allows comparison operations to connect specifically to encrypted information, without deciphering operands. As a result, balance and rank queries and also queries MAX, MIN and COUNT, GROUP BY and ORDER BY can be prepared specifically from encrypted data. OPES results are correct and do not contain false positives, a value in a column can be modified or a new value can be inserted into a column without requiring changes in the encryption of other values and can be incorporated effortlessly with the frameworks of existing data. The encryption of non-numeric information, for example, the factor length strings are not terminated by OPES. In addition, when applying SUM or AVG to a group, the values must be deciphered.

Raluca Ada Popa, Frank H. Li and Nickolai Zeldovich, proposed "An ideal security protocol for order preservation coding", which achieves perfect security. The fundamental method used is that of the variable / mutable ciphertext, which implies that the encrypted texts for some clear text values change and it is demonstrated that impermanent ciphers are required for perfect security. mOPE is superior to any OPE scheme for 1-2 extension requests. The same security OPE (sTOPE) [7] is executed in such a way that only the order of the elements present in the database is known. mOPE and STOPE use the Merkle hash to protect clients against a malevolent server. Although it filters the order information of the data in plain text. In addition, the prototype only issues a single query at a time when it is possible to place more orders of fine grains.

J.-M. Bohli, N. Gruschka, M. Jensen, LL Iacono and N. Marnau, proposed the multicloud architectures of security and privacy improvement [8]. This document works as a general document where the creators talked about open cloud and multiple cloud security. The high potential for security perspectives in cloud computing has also been discussed. Homomorphic encryption and secure multi-part calculation protocols are exceptionally encouraging with respect to technical security and regulatory compliance. However, there is no one ideal way to deal with security and legal compliance in a way that can not be applied. The confinement of these methodologies only originates in their restricted applicability and in the high multifaceted nature that is used.

MA AlZain, E. Pardede, B. Soh and JA Thom, proposed the security of cloud computing from single to multiple clouds, indicating security in single clouds and multiple clouds [13]. In addition, it shows some limitations and points of interest in security in cloud computing. Individual clouds work in three phases SaaS, PaaS, IaaS. Clients and business organizations do not lose their private data due to a vengeful attacker in the cloud. It has a great capacity to reduce the security possibilities that influence the cloud computing client. Find conceivable confinement to conceivable. However, the availability of the service is still disappointing and there is also a loss of management accessibility.

IV. IMPLEMENTATION

Modules

1 data owner

2. user data

3. CSP (clouddienstanbieter)

4. Admin

Description of the modules:

(1). DATA OWNER

Industries and people will subcontract the database to practical and low-cost applications and services to perform them. IT companies that want to outsource their database in the cloud, which contains valuable and confidential information (such as account information, Transaction \ records, disease information), and then access the database (such as SELECT, UPDATE, etc.). The owners of the data to outsource the encryption to their intruder data content to protect the databases in a format and encryption data, the owners can use some popular encryption algorithms.

(2). INFORMATION USERS

The data user has already downloaded the necessary files from the cloud in the cloud. In the data in the cloud that is so coded content, the original data content is displayed (decoded), the users must obtain the permission (key) of the owner of the data. The user analyzes the query request and the numbers, how many columns are involved. In our project, the user sends the encrypted query request to cloud A and the user can select the file using the search engine with range queries.

(3). CSP

CSP can all functions in the module . The cloud service providers show who are responsible for the available and accessible data, and for protecting the physical environment and executing them. People and organizations buy or rent the ability of the providers for the user, the organization or the data warehouse of the application. In our project, there are two clouds, probably cloud A and cloud B, the highest security standards, to provide the content of the data that is loaded by the owner of the data. Both A cloud and a cloud are B not collusion, that each cloud is only aware of its own data.

(4). ADMINISTRATION

The administrator is responsible for the authentication, the owners of the data and the users of the data. The administrator's shipping key to the user's email ID in order to segment the authentication data. Users can log in, secrete only by using this key. We can easily identify the people authorized to identify this authentication process and discover that each intruder tried to hack confidential information.

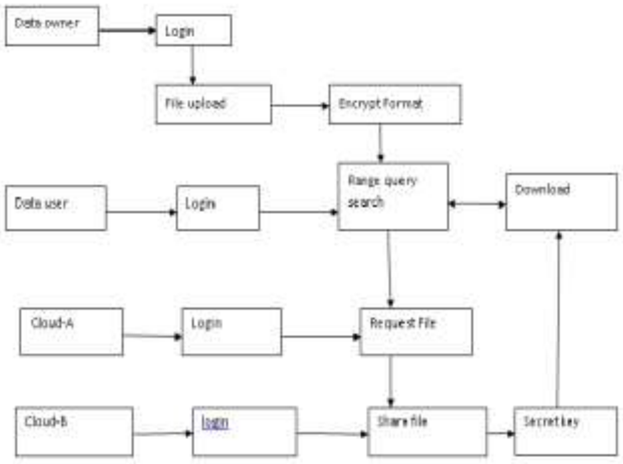

Fig. 4 Data Flow Diagram of the System

V. LITERATURE SURVEY

(1) in the direction of safe and reliable storage services in cloud computing

Authors: C. Wang, f. Wang

Cloud storage allows users to remotely store their data and enjoy high-quality cloud applications without the burden of local hardware and software administration. Although the benefits are clear, this service is also physically in possession of the paged data, the waiver inevitably provides new security risks on the accuracy of the data in the cloud. To address this new problem and achieve more secure and reliable cloud storage service, we propose in this document a flexible distributed storage integrity audit mechanism, use of homomorphic tokens and distributed Erasure encoded data. The proposed design allows users to verify storage in the cloud with very light communication and calculation costs. The result of the audit not only provides a solid guarantee of accuracy of storage in the cloud, but at the same time it arrived at the location of errors, that is, the identification of the data of the server fallen quickly. When considering that data in the cloud is dynamic in nature, the proposed draft continues to support safe and efficient dynamic processes in the paged data, including modification, deletion, blocking and attachments. The analysis indicates that the proposed rule is extremely effective and durable against Byzantine failures, malicious data modification attacks and even server collusion attacks.

(2) the cloud computing framework in public shares a safe dynamic group

Authors: K. Xue and p. Hong

With the popularity of group data sharing in public cloud computing, the confidentiality and security of the data exchange group have become two main problems. The cloud provider is not a trusted third party because of its benefits of a half-trust nature, so traditional security models do not easily share the frameworks in the cloud-based group more generally. In this document, we propose a new secure group sharing framework for the public cloud, which can effectively use the server's help in the cloud, but do not expose sensitive data to the attackers and the cloud provider. Frame combines enhanced TGDH, proxy signature and proxy re-encryption together in one record. Through the application of proxy signing technology, the group leader can effectively receive Executive privilege with one or more selected members of the group. The enhanced TGDH control makes it possible to negotiate the Group and, with the help of servers in the cloud that were not all members of the online group, constantly updates the Group of key pairs. By adopting proxy re-encryption, highly computationally intensive operations can be delegated cloud servers without revealing private information. The comprehensive security and performance analysis shows that our proposed scheme is highly efficient and meets to share the security requirements of the secure group based on the public cloud.

(3) address computer security problems in the cloud

Authors: D. Zissis and D. Lekkas

The recent appearance of cloud computing, the perception of infrastructure architectures, the distribution of software and the development models of all, changed drastically. Concerns about a critical problem for the success of IT systems, communication and information security have driven the rapid transition to the cloud. For security reasons, if several unexplored risks and challenges of this transfer to the cloud will deteriorate much of the effectiveness of the traditional safeguards introduced. Therefore, the purpose of this document is twofold; First, evaluate cloud security through the identification of unique security requirements and, secondly, try to present a viable solution that eliminates these possible threats. This document proposes the introduction of a reliable third party, in charge of safeguarding the specific characteristics within a cloud environment. The proposed solution requires cryptography, in particular public key infrastructure in concert with SSO and LDAP authentication, to secure the integrity and confidentiality of information and communication. The result offers a horizontal level of available service, it saves all the institutions involved, which enforces a safety network, within which a great assurance.

(4) an overview of mobile cloud computing: architecture, applications and approaches

Authors: H. t. Dinh, C. Lee

With the volatile development of mobile applications and the evolution of the concept of swarm computing, the mobile Cloud Computing (MCC) was inserted to be a possible technology. So, it forces a substantial requirement for fluid applications and services in the cloud for users of fluid devices. This is a neat opportunity for commercial enterprise and research at MCC. This article first talks about the definitions of cloud computing, mobile computing and mobile cloud computing (MCC). And so, on that point is a universal description of MCC in its concepts, key characteristics, service and execution examples. Subsequently, it is the architecture of the MCC and its challenges. Lastly, draw some applications, current and subsequent research questions.

(5) Verifiable calculation in a large database with incremental updates

Authors: X. Chen, j. Li

The concept of verifiable data bank (VDB) can be a client with limited resources, securely store a very large database on an untrusted server so that it can then register, retrieve and update a record, assigning a new value. In addition, the client detects any attempt by the server to manipulate the data. If the database is submitted more frequently to small changes, the client must calculate and update the encrypted version (encrypted text) on the server at all times. For very large amounts of data, they are extremely expensive resources limited to the client, both operations from scratch. In this document we formalized the concept of a verifiable databank with incremental updates (Inc-VDB). We also propose a General Inc-VDB framework through the integration of the basic commitment of the body vector and encrypt the incremental MAC encryption mode. We present a concrete Inc-VDB system, the underlying Computational Diffie-Hellman (CDH). In addition, we demonstrate that our design can achieve the desired safety properties.

Sr. no	AUTHORS	APPROACHES	ADVANTAGES	DISADVANTAGES
1.	John Daugman, Piotr Zielinski	Fast search algorithm for a large fuzzy database	takes less memory, Doesn’t require complex storage administration.	interpret any fuzzy query statement into a crisp query and evaluate
2	R.A.Popa, C. Redfield, N.Zeldovich and H.Balakrishnan	CryptDB,	limits the uncovered data to the untrusted database server.	a few information is uncovered in the process.
	Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu	Order Preserving Encryption for Numeric Data	Query results are sound (no false hits) and complete (no false drops). MIN,MAX,SUM/ AVG can be prepared	Encryption of non-numeric information aren't finished by OPES. Data for SUM or AVG to a group should decrypted.
	Raluca Ada Popa, Frank H. Li, Nickolai Zeldovich,	"An Ideal-Security Protocol for Order-Preserving Encoding",	mOPE is superior to any OPE scheme by 1-2 requests of extent. Only the order of items present in the database is known.	issues only single query at a time where more finegrain ordering is possible.
	J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau,	Security and privacy enhancing multicloud architectures	Provides technical security and regulatory compliance.	both security and legal compliance cant be implemented together.
	M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom,	The Cloud computing security from single to multi-clouds,	Find conceivable to conceivable confinement.	The service availability is a disappointment loss of administration accessibility.

VI. CONCLUSION

In this document, we have examined the various techniques and protocols associated with upholding the secrecy of data outsourced to the external cloud server. In society to progress in this area, some of the works include fuzzy logic, range queries, order preservation encryption and the architecture of several clouds. The fuzzy logic implemented Beacon Guided Search (BGS), which requires substantially less storage and no complex storage mechanism. Rank queries operate by implementing the RRQ and can achieve keyword confidentiality, verification, data integrity and privacy of queries. Then came CryptDB, which fundamentally includes the use of range queries to productively complete the encrypted information using a novel SQL encryption system. Nevertheless, some data are even exposed to the cloud server. The society that preserves encryption is one of the instruments used by CryptDB that allows comparison operations to link specifically to encrypt data, without deciphering the operands. Only the encryption of non-numeric information is not possible with this creature. Afterwards, the architecture of several clouds was introduced, which brought out the idea of dividing sensitive information and query logic into two different non-collusive clouds that do not possess knowledge about each other. All the same, this architecture is not valid for queries like SUM / AVG.

VII. ACKNOWLEDGEMENT

The authors would like to thank the editors, the researchers for making their resources available, and the teachers for their guidance. We thank the authority of the university for providing the required infrastructure and technical support. Finally, we express our sincere thanks to friends and family.

REFERENCES

[1] Kaiping Xue, Shaohua Li, Jianan Hong, Yingjie Xue, Nenghai Yu, and Peilin Hong "Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving", IEEE Transactions on Information Forensics and Security ,2017

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al., "A view of cloud computing", Communications of the ACM, vol. 53, no. 4, pp. 50–58,2010.

[3] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou,"Toward secure and dependable storage services in cloud computing", IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[4] D. Zissis and D. Lekkas,"Addressing cloud computing security issues", Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.

[5] R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: protecting confidentiality with encrypted query processing," in Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, pp. 85–100, 2011.

[6] D. Boneh, D. Gupta, I. Mironov, and A. Sahai, "Hosting services on an untrusted cloud," in Advances in Cryptology-EUROCRYPT 2015. Springer, pp. 404–436, 2015.

[7] R. A. Popa, F. H. Li, and N. Zeldovich, "An ideal-security protocol for order-preserving encoding," in Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP'13). IEEE, pp. 463–477, 2013.

[8] J.-M. Bofhli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau,"Security and privacy-enhancing multicloud architectures," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 212–224, 2013.

[9] F. Hao, J. Daugman, and P. Zielinski, "A fast search algorithm for a large fuzzy database," IEEE Transactions on Information Forensics and Security, vol. 3, no. 2, pp. 203–212, 2008.

[10] Y. Yang, H. Li, M. Wen, H. Luo, and R. Lu, "Achieving ranked range query in smart grid auction market," in 2014 IEEE International Conference on Communications (ICC2014). IEEE, Vol.2, No.4,April 2014

[11] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data. ACM, pp.563–574, 2004.

[12] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order-preserving symmetric encryption," in Advances in Cryptology–EUROCRYPT 2009. Springer, pp. 224–241, 2009.

[13] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud computing security: from single to multi-clouds," in Proceedings of the 45th Hawaii International Conference on System Science (HICSS2012). IEEE, pp. 5490–5499, 2012.