International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Privacy Preservation in cloud Environment using AES Algorithm

Akash Kumar[1], Dr. Bhuvana J[2]

[1]MCA, School of Computer Science & IT, Jain University, Bangalore, India.
[2]Professor, School of Computer Science & IT, Jain University, Bangalore, India.

Abstract - *This paper aims to develop cloud-based data describing components that allow data encryption and encryption. users can use this cloud-based web application whenever they feel uncomfortable in their lives and try to ignore it.*

The purpose of this paper is to provide Data Security which will be uploaded by the owner in encrypted format and later converted to encrypted form. In this paper, we consider encryption with a file system in which multiple data providers such as hospitals and physicians are authorized by individual records to upload their data to a trusted public cloud. User data is sent in encrypted form to ensure data security, and each data provider also sends encrypted data references to enable queries to encrypted data. We are proposing an Algorithm so that with the help of this algorithm we can encrypt and decrypt data .The Algorithm we use in our project is the AES (Advanced Encryption Standard) Algorithm so that we can encrypt the data and it will be stored in cloud.

Key Words: AWS, Cloud Based, CSS, Database, Html, AES, JavaScript, MySQL.

1. INTRODUCTION

New revolving technologies in hardware, middleware, virtual machine and distributed systems are needed to meet growing knowledge needs. Such technology should meet the needs of all types of clients from individuals and organizations. All services can be provided via cloud computing as they provide platform, infrastructure and software as a service using the technologies mentioned above. This is a payment model as you go. As these technologies require resources, network, hardware and virtualization on a larger scale than the integration of all technical issues leads to a complete loop of systems. Among all the problems related to cloud computing we focus on user privacy issues so that data is stored securely and data is secure. Cloud computing emerges as a paradigm for new computers and other business data protection platforms. Most of the data will be stored in the cloud after encryption so that data can be accessed anywhere and anytime without data cuts. Introducing the cloud services that will be provided for data storage in data storage is not just an issue. planning for tedious infrastructure management activities and reducing development costs and maintaining them. However, keeping user privacy concerns should be considered important when designing security and privacy guidelines because there is a potential for misuse of data. Various methods have been used to protect data security in the cloud environment. This study aims to integrate the complex cloud protection systems used in the cloud. In addition, critical encryption methods are classified as encryption and writing methods, and are assigned to the sub-categories. Additionally, the strengths and weaknesses of the provided methods are reported and other open issues are reported.

2. RELATED WORK

[1] This paper introduces a review on the use of the AES Algorithm AES block cipher. The key size can be 128/192/256 bits. Encrypts data in 128-bit blocks each. That means it takes 128 bits as input and extends 128 bits of encrypted cipher text as output. AES relies on the network-licensed exchange policy which means it is performed using a series of linked functions that include retrieving and pushing input data. A set of AES commands are now integrated with the CPU (provides GB / s output) to improve the speed and security of applications that use AES encryption and decryption. Although it has been 20 years since its launch we have failed to break the AES algorithm as it does not even happen with current technology. So far the only risk left is the use of the algorithm.

[2] The tendency to use data for coding and writing is very good, because the file is rich in information, and the data becomes a necessity. The use of information technology allows automated data extraction processes that will be used for the data acquisition of interesting and common information, which means the completion of manual work and the easy retrieval of data directly into electronic data maintenance. They need to be collected and stored in an orderly fashion, and their integration enables them to focus on the hospital's information system. It offers many opportunities to detect hidden patterns from this data.

[3] Java is based on the C ++ syntax, and is intended to be a java-based Structure between translated and integrated language. Java compiler into Byte Codes, secure and portable on all different platforms, including Java applications. These byte codes are actually commands compiled in one form, in what is known as a virtual java (JVM) machine, which resides in a standard browser. JVM is available on almost all OS. JVM converts these byte codes into precise machine commands during operation. Java is actually a three-component forum: Java programming language, Java classroom library and workspaces., Java Virtual Machine. Java is a simple to code. It does not use references, overload function etc., Java is an

object-oriented language and supports encapsulation, legacy, Polymorphism and strong binding, but does not support multiple legacy. Everything in java is an object except for the old data types. Java is portable. It is a structural neutrality which means that the java programs when combined can be used on any enabled machine. Java is distributed in its own way and used for editing Internet applications. Java is strong, secure, efficient and environmentally friendly. Java supports multiple readings. So the different parts of Java are a simple language. It does not use references, overload function etc., Java is an object-oriented language and supports encapsulation, legacy, Polymorphism and strong binding, but does not support multiple legacy. Everything in java is an object except for the old data types.Javies is portable.It is a structural neutrality which means that the java programs when combined can be used on any enabled machine. Java is distributed in its own way and used for editing Internet applications. Java is strong, secure, efficient and environmentally friendly. Java supports multiple readings. So different parts of the system can be done simultaneously.

[4] In an attempt to set up a standard Java Database API; Sun Microsystems has developed Java Database Connectivity, or JDBC. JDBC provides a standard SQL database access point that provides a consistent interface for various RDBMS. This consistent interaction is achieved through the use of the "plug-in" website, or drivers. If the database vendor wishes to receive JDBC support, he or she must provide the host of each domain a website and Java operating system. For broader JDBC acceptance, Sun is based on the JDBC framework at ODBC. As you found out at the beginning of this chapter, ODBC has extensive support for various platforms. Basing JDBC at ODBC will allow marketers to bring JDBC drivers to market faster than building a new communication solution. Java Database Connectivity (JDBC) is a Java-based programming interface (API) for programming language, which explains how a client can access a website. It is a Java-based data access technology used to communicate on a Java website. It is function of the Java Standard Edition platform , from Oracle Corporation. Provides query and information retrieval services on the website, and is directed to related archives. The JDBC-to-ODBC bridge enables you to connect to any ODBC-accessible data source in the Java virtual machine (JVM) machine.

[5] URLs and URL Links provide a high-quality way to access online resources. Sometimes your plans require poor network connectivity, for example, if you want to write a client server application.

In client server applications, the server provides certain services, such as processing web queries or sending current stock prices. The client uses a service provided by the server, either displays the results of the site query to the user or makes stock purchase recommendations from the investor. The communication that takes place between the client and the server must be reliable. That is, no data can be dropped and it should reach the client side in the same way the server sent it. TCP provides a reliable, point-to-point communication channel that is an online client-server application that uses to communicate with each other. To communicate via TCP, the client system and server system establish another connection. Each system binds the socket to the end of its connection. For communication, each client and server reads and writes to the socket tied to the connection.

[6] One of the newest features of java packages. Packages for both composing and visibility control methods can define classes within a package that is not accessible by code outside the package. It can define class members that are only displayed to other members of the same package. Java uses file system indexes to store packages. For example .class files for any classes that you mentioned are part of My Package should be stored in a directory called My Package , of your java development system. For example a package is advertised as a package java.awt.image; needs to be saved to java \ awt \ image instead of windows.

[7] The java package, java.lang contains basic classes and close interactions close to the time system used which includes the root sections that make up the category, the types bound to the language definition, basic variables, mathematical functions, configurations, security functions and other system information native less. Integrated data structures are the core of the Java.util package package API clusters and data structure sequences that are most influenced by design pattern considerations. Provides class and interactive framework interactions. Includes classes that use a flexible, well-refined access control system. Packages also support generation and storage of cryptographic public key pairs. Ultimately this package provides classes that support signed / supervised items and protects against random number production.

[8] Swing is a Java widget toolkit. It is part of the Sun Microsystems Java foundation class-API to provide visual user experience for Java applications. Swing was upgraded to provide a more complex set of GUI components than an invisible window toolkit. Swings provide a traditional look and feel that mimics the look and feel of several looks and feel unrelated to the basic platform. Swings has introduced a method that allows the look and feel of every part of the app to be changed without making major changes to the app code. The introduction of connected visual and emotional support allows the swing parts to mimic the appearance of the native parts while maintaining the benefits of a stand-alone stand. The above feature also makes it easy to make the rounded app look very different from the traditional programs if necessary.

3. ANALYSIS AND INTERPRETATION

In our paper, here we store the file in order to upload that data effectively for the user's recording system. Cloud provides us with flexible features, using a computer cloud is

essential in helping businesses and individuals identify and deliver the promise of digital change.

System design is the process of defining structure, components, modules, work areas and system data to meet specific needs. One can see it as the application of programming theory to product development. There is a mix of system analysis, system design and system engineering. If the broader theme of product development "combines the idea of marketing, design, and production into a single product development product," that will be design is the act of taking market knowledge and creating the design of the produce for the later so that it can be produced for the System to design is therefore a process of defining and developing systems to meet specific needs of the user / Customer.

Using HTML, cascade, and java script we can create our own interactive app, and we can use the loping feature in HTML language because we can use long slide code or any module we have to repeat. MySQL language provides data storage on the website.

The final user flow of my model will be done by the covering i.e., user / customer. Here the owner can upload the files in encrypted format so that data cannot be seen by others users and they will be deleted from encrypted users.

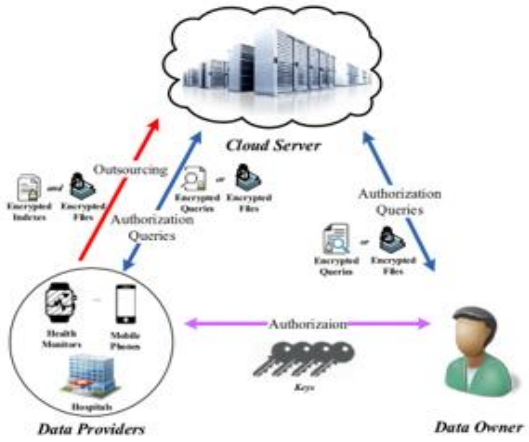

Fig:1- A working model

Data will flow as the owner begins to upload the file to the cloud in encrypted format where authorization questions will be collected. Later that data will be provided to hospitals, Cell Phones.

4. IMPLEMENTATION

This section describes how we process data and algorithms for efficient data retention with the help of encryption and decryption. It also analyzes opportunities related to the use of user data

4.1 Data Division

First, we must remember that AES is a block cipher. Unlike broadcast ciphers, it encrypts data in bit blocks instead of bit-by-bit. Each block contains a 16-bit column in a four-dimensional structure. Since one byte contains 8 bits, we get a 128-bit block size (16x8 = 128) .So, the first step for AES encryption separates blank text (encoded text) into these blocks.

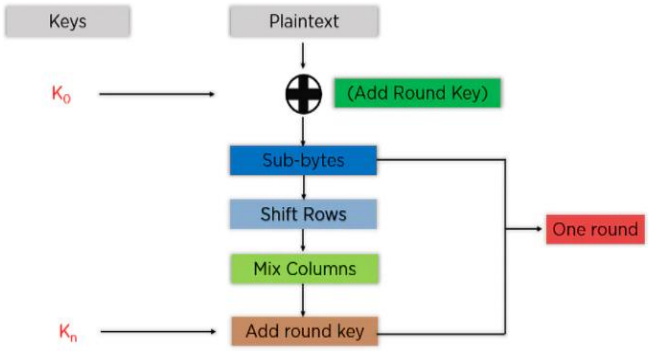

Fig:2- working of AES Alogrithm

Add Rotate Key, Transfers block data stored in state system using XOR function with the first key generated (K0). Passes state result system as input in the next step. The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block size / chunk of 128 bits. It converts these individual blocks using the keys 128, 192, and 256 bits. When encrypting these blocks, they combine them together to form a ciphertext text.It is based on an exchange-permission network, also known as the SP network. Contains a series of linked functions, which include replacement input (output) and other features that include slower (permissions).

4.1.1 Add round key

Transfers the block data stored in the state system using the XOR function with the first key generated (K0). Passes state result system as input in the next step.

4.1.2 Sub – bytes

In this step, it converts each plot of land system into a hexadecimal, divided into two equal parts. These sections are rows and columns, mapped with a replacement box (S-Box) to produce new values for the final state plan.

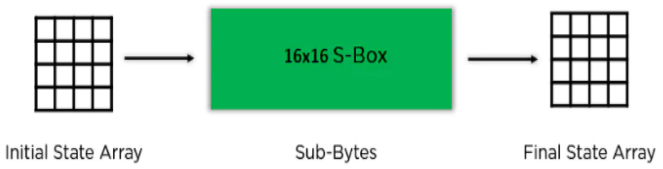

Fig.3. Sub-Bytes

1) **4.1.3 Shift Rows**

2) It exchanges the elements of the row between each other. Skip the first line. It moves the elements to the second row, one area to the left. It also shifts elements from the third row in two consecutive positions to the left, and shifts the last three vertical lines to the left.

3) **4.1.4 Mix Columns**

Repeats the unmodified matrix for each column in the region system to get a new column for the same similar district members. Once all the columns have been repeated with the same constant matrix, you get your next step plan. This particular step should not be performed in the final round.

4.1.5 Add Round Key

The appropriate round key says XOR'd and state array are located in the previous step. If this is the last cycle, the resulting state system becomes the cipher text of a particular block; if not, it goes as far as the inclusion of a new regional plan for the next step that is round.

4.1.6 Encryption scheme:

In order to reduce the calculation load on the user side, the computer function must be on the server side, so we need an encryption system to ensure simultaneous operation and security on the server side. Homomorphic encryption allows certain types of calculations to be made in the corresponding cipher text. The result is a cipher text of the result of the same operations performed on a blank text. That is, homomorphic encryption allows the cipher text calculation without knowing anything about the explicit text to get the correct encrypted result. Despite its excellent location, the first fully homomorphic encryption scheme, which uses the appropriate lettuce over the polynomial ring, is very complex and inefficient for use. Fortunately, due to the use of the vector space model in high-return, only the functions of adding and multiplying by the total values are required to calculate the related points from the encrypted index search. Therefore, we can reduce the original homomorphism in a complete way into a simplified form that only supports complete functionality, allowing for greater efficiency than that of the full data.

4) 4.2 Classification

The most powerful methods of analyzing recurring block ciphers such as Data Encryption Standard (DES) are attacks aimed at exposing small circular keys. These methods include dierential and linear cryptanalysis. In this regard, the authors introduced a new classification system for repetitive block ciphers based on their critical schedules. In short, this program creates two phases of ciphers based on the fact that the information of the circular subkey generated by the key system displays any information about other circular subkeys or key.

5) 4.3 Clustering

Integration is a file system that requires the identification of related data to be encrypted and extracted. It relies on a visual approach that reflects the distribution of data to people in order to understand it. Data will be sent to their phones so that data can be easily accessed anywhere.

6) 4.4 Outlier detection

External discovery or confusing discovery involves looking at data objects in a data set of any confusion that is not consistent with certain behaviors.

7) 4.5 Sequential Pattern

A sequential pattern is a method that focuses on finding similar patterns in data activity over time. This application is useful for revealing periodic data deviations.

8) 4.6 Association Rules

Organizational rules are statistical related data uploaded to the cloud. That data will be displayed on mobile phones and will be stored in the cloud and can be accessed later.

With Data to Encrypt and Delete Encryption, there is an AES algorithm to consider. Each method in the algorithm will eventually produce results among each other and with these results, it is used to determine the efficiency and accuracy of the system.

5. RESULTS AND DISCUSSION

While vulnerabilities regarding the confidentiality of data outsourced to the cloud can easily be addressed through the adoption of industry standard encryption technologies, the creation of complex machine readable access rights to the decryption keys becomes a challenging problem. The syntax of XML-based rights expressions is complicated and obscure when the user-related conditions become sophisticated. The functionality of being able to handle a wide variety of possible access scenarios is typically built into any righs ex-pression language, but it is often difficult to cleanly partition out those subsets needed by a particular privacy preserving application. How to efficiently generate rights expressions reflecting the requirements of an organization and being secure at the same time becomes a future challenge While vulnerabilities regarding the confidentiality o data outsourced to the cloud can easily be addressed through the adoption of industry standard encryption technologies, the creation of complex machine readable access rights to the decryption keys becomes a challenging problem. The syntax of XML-based rights expressions is complicated and obscure

when the user-related conditions become sophisticated. The functionality of being able to handle a wide variety of possible access scenarios is typically built into any rights expression language, but it is often difficult to cleanly partition out those subsets needed by a particular privacy preserving application. How to efficiently generate rights expressions reflecting the requirements of an organization and being secure at the same time becomes a future challenge While vulnerabilities regarding the confidentiality of data outsourced to the cloud can easily be addressed through the adoption of industry standard encryption technologies, the creation of complex machine readable access rights to the decryption keys becomes a challenging problem. The syntax of XML-based rights expressions is complicated and obscure when the user-related conditions become sophisticated. The functionality of being able to handle a wide variety of possible access scenarios is typically built into any right expression language, but it is often difficult to cleanly partition out those subsets needed by a particular privacy preserving application. How to efficiently generate rights expressions reflecting the requirements of an organization and being secure at the same time becomes a future challenge While vulnerabilities regarding the confidentiality of data outsourced to the cloud can easily be addressed through the adoption of industry standard encryption technologies, the creation of complex machine readable access rights to the decryption keys becomes a challenging problem. The syntax of XML-based rights expressions is complicated and obscure when the user-related conditions become sophisticated. The functionality of being able to handle a wide variety of possible access scenarios is typically built into any rights expression language, but it is often difficult to cleanly partition out those subsets needed by a particular privacy preserving application. How to efficiently generate rights expressions reflecting the requirements of an organization and being secure at the same time becomes a future challenge While vulnerabilities regarding the confidentiality of data outsourced to the cloud can easily be addressed through the adoption of industry standard encryption technologies, the creation of complex machine readable access rights to the decryption keys becomes a challenging problem. The syntax of XML-based rights expressions is complicated and obscure when the user-related conditions become sophisticated. The functionality of being able to handle a wide variety of possible access scenarios is typically built into any rights expression language, but it is often difficult to cleanly partition out those subsets needed by a particular privacy preserving application. How to efficiently generate rights expressions reflecting the requirements of an organization and being secure at the same time becomes a future challenge While vulnerabilities regarding the confidentiality of data outsourced to the cloud can easily be addressed through the adoption of industry standard encryption technologies, the creation of complex machine readable access rights to the decryption keys becomes a challenging problem. The syntax of XML-based rights expressions is complicated and obscure when the user-related conditions become sophisticated. The functionality of being able to handle a wide variety of possible access scenarios is typically built into any rights expression language, but it is often difficult to cleanly partition out those subsets needed by a particular privacy preserving application. How to efficiently generate rights expressions reflecting the requirements of an organization and being secure at the same time becomes a future challenge While vulnerabilities regarding the confidentiality of data outsourced to the cloud can easily be addressed through the adoption of industry standard encryption technologies, the creation of complex machine readable access rights to the decryption keys becomes a challenging problem. The syntax of XML-based rights expressions is complicated and obscure when the user-related conditions become sophisticated. The functionality of being able to handle a wide variety of possible access scenarios is typically built into any rights ex pression language, but it is often difficult to cleanly partition out those subsets needed by a particular privacy preserving application. How to efficiently generate rights expressions reflecting the requirements of an organization and being secure at the same time becomes a future challenge

This project aims to provide an easy-to-use data protection system that will be provided to the customer so that data is protected only when data is needed and we access the data. In this case the user, owner, key manager will be created where the owner will create a user profile where the username and password will be taken later the key will be generated and displayed and sent to the registration email for encryption. Later that can be achieved and can be downloaded by the user. When the user downloads the file again a single key will be created so that the text will now be encrypted. The software itself will only fit and be installed on PCs or can be distributed over the clouds to be accessible anywhere.

Based on cloud data acquisition, Data will be encrypted for security purposes to minimize data misuse, and it is done with the help of the AES algorithm to become the most efficient and accurate encryption algorithm.

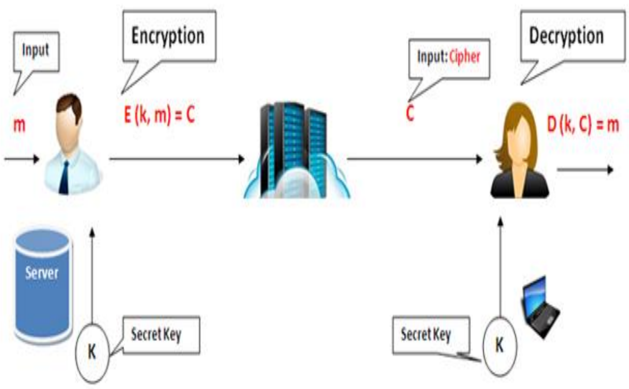

Fig.4. AES SCENARIO

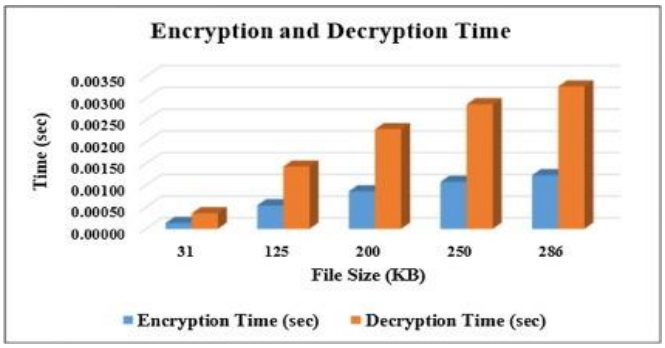

Fig.5. AES GRAPH

6. CONCLUSIONS

In this paper, we explore the problem of encrypting multiple choice queries in the cloud-based data encryption and decryption field. Unlike previous functions, our MEIM proposed method allows a certified data holder to access secure, relevant, and effective query data for multiple data providers. To address the practical question, we have introduced MDBT as a data framework. In order to reduce the productivity question of the data owner, and allow the cloud server to ask securely, we recommend a novel compilation system for mass storage. To make our model more efficient, we propose a very sophisticated symmetric encryption system to satisfy a statistically valid question. In addition, we use strong security evidence to prove that our systems are secure. Finally, we demonstrate that the MEIM method works very well on computers by using our schemes and operating on virtual storage.

Although our work only focuses on Encrypting and clearing data system encryption, it can be expanded by looking at various scenarios, mobile data collection, recommendation system, and so on. However, devices, such as cell phones, have limited memory and memory function. In all of this, we will discuss less expensive schemes in our future work.

References

[1] C. Wang, B. Zhang, K. Ren, J. Roveda, C. Chen, Z. Xu, "Healthcare monitoring system has helped to increase privacy and oppressive behavior," at INFOCOM'14, Toronto, Canada, 2014.

[2] J. Sun, X. Zhu, C. Zhang, Y. Fang, "HCPP: A Cryptography based secureehr system for patient privacy and emergency medical care," at ICCDCS'11, Minneapolis, Minnesota, 2011.

[3] M. Li, S. Yu, N. Cao, W. Lou, "Keywords for private data search enabled in cloud computing," at ICCDCS'11, Minneapolis, Minnesota, 2011.

[4] J. Benaloh, M. Chase, E. Horvitz, K. Lauter, "Patient Management: Ensuring the Privacy of Electronic Medical Records," at: ACM CCS'09 Workshop, New York, NY, 2009.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou. 24, no. 1, pages 131 - 143, 2013.

[6] M. Li, S. Yu, K. Ren, W. Lou, "Protecting personal health records from cloudcomputing: Managing patient access to clean and refined data in multiple owner settings," at SecureComm'10,

[7] J. Liu, X. Huang, J. Liu, "Secure sharing of personal health records on an incloud computer: a signature-based policy," FutureGener Comp Sy. , Vol. 52, pages 67-76, 2015.

[8] P. Scheuermann, M. Ouksel, "Multidimensional B-trees for associativesearch in the data system," Inform Syst., Vol. 7, no. 2, pages 123 - 137,1982.

[9] K. Xue, J. Hong, Y. Xue, D. Wei, N. Yu, P. Hong, "CABE: A NewComparable Attribute-based Encryption Construction with 0-Encodingand 1-Encoding," IEEE Trans Comput . , vol. 66, nxa. 9, pages 1491 - 1503,2017.

[10] K. Xue, S. Li, J. Hong, Y. Xue, N. Yu, P. Hong, "SQL Quotations Related to SQL Numbers With Confidentiality," IEEE Trans Inf Forensics Secur. , vol. 12, no. 7, pages 1596 - 1608,2017.

[11] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, "Searched symmetricencryption: advanced definitions and effective constructions," in CCS'06, Alexandria, VA, 2006.

[12] Y. Zhu, Z. Huang, T. Takagi, "The K-NN query is secure and controllable over encrypted cloud data and important privacy," J Parallel Distr Com, vol. 89, when. C, pages 1 - 12, 2016.

[13] D. Song, D. Wagner, A. Perrig, "Effective methods of single-data encryption," at IEEE S & P'00, Berkeley, CA, 2000.

[14] D. Boneh, G. Crescenzo, R. Ostrovsky, G. Persiano, "Encryption for public keyword search," EUROCRYP'04, Interlaken, Switzerland, 2004.

[15] Y. Zhu, Z.Wang, Y. Zhang, "Protect k-NN query from Encrypted Cloud Data with Unlimited Key Disclosure and Offline Data Owner," PAKDD'16, Auckland, New Zealand, 2016.

[16] B. Iyer, S. Mehrotra, E. Mykletun, G. Tsudik, Y. Wu, "Safe Storage in RDBMS," by EDBT'04, Heraklion, Crete, Greece, 2004.

[17] Y. Zhu, Z. Wang, J. Wang, "Collusion-Resisting Secure Nearest NeighborQuery over Encrypted Data in Cloud," in IWQoS'16, Beijing, China, 2016.

[18] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, "Order digital encryption," SIGMOD'04, New York, NY, 2004.