Journal of Taibah University for Science

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tusc20

Secured data storage in the cloud using logical Pk-Anonymization with Map Reduce methods and key generation in cloud computing

Sindhe Phani Kumar, R. Anandan, Fairouz Tchier, G. Rajchakit, Choonkil Park & Ferdous M. O. Tawfiq

To cite this article: Sindhe Phani Kumar, R. Anandan, Fairouz Tchier, G. Rajchakit, Choonkil Park & Ferdous M. O. Tawfiq (2021) Secured data storage in the cloud using logical Pk-Anonymization with Map Reduce methods and key generation in cloud computing, Journal of Taibah University for Science, 15:1, 746-756, DOI: 10.1080/16583655.2021.2001938

To link to this article: https://doi.org/10.1080/16583655.2021.2001938

Published online: 15 Nov 2021.

JOURNAL OF TAIBAH UNIVERSITY FOR SCIENCE
2021, VOL. 15, NO. 1, 746–756
https://doi.org/10.1080/16583655.2021.2001938

Secured data storage in the cloud using logical Pk-Anonymization with Map Reduce methods and key generation in cloud computing

Sindhe Phani Kumar[a], R. Anandan[b], Fairouz Tchier[c], G. Rajchakit[d], Choonkil Park[e] and Ferdous M. O. Tawfiq[c]

[a]Department of CSE, Vels Institute of Science Technology & Advanced Studies (VISTAS), Chennai, India; [b]Department of CSE, Vels Institute of Science Technology & Advanced Studies (VISTAS), Chennai, India; [c]Department of Mathematics, King Saud University, Riyadh, Saudi Arabia; [d]Department of Mathematics, Faculty of Science, Maejo University, Chiang Mai, Thailand; [e]Department of Mathematics, Research Institute of Natural Sciences, Hanyang University, Seoul, Korea

ABSTRACT

The significant security assessment is rising because the vast amount of data can be renewed continuously in the cloud. Cloud information is clustered and refreshed productively using a progressive clustering procedure over the data. To verify the security of a user's connection to the cloud, the development of information to the servers could be used. Thus, the trustworthiness of the information plays a vital role in determining the authority of the information. Map Reduce is used to deal with enormous volumes of information, and informational indexes are circulated on the cloud. A parallel information preparation structure is then received, allowing for the collection of current information that joins over time. Information anonymization methods are then used to achieve security and high information utility when an update occurs, resulting in less data loss and refresh time over time.

ARTICLE HISTORY
Received 13 August 2021
Revised 5 October 2021
Accepted 20 October 2021

KEYWORDS
Pk-Anonymization; cloud computing; data security; key generation; Map Reduce; secure data storage

1. Introduction

Cloud computing is one of the significant new eras in the information advancement world. On account of its compositional structure and qualities (Flexibility/Elasticity, Scalability of the structure, number of systems included, Reliability and Sustainability), numerous advantages, including security advantages, consolidated division of data, and high availability [1]. The new thoughts exhibited by the Clouds, such as estimation likelihood, resource sharing, and data warehousing expand the security and insurance levels and can be prepared to confront new security challenges [2].

Cloud computing causes cloud users to give organizations at decreased costs. Security is considered the most critical limit for using cloud organizations. While a segment of the security concerns is not new, they are accessible in existing models, such as server break, loss of data, and secured key constraints [3]. As indicated by the National Institute of Standards and Technology cloud is portrayed as it is a stage that should be solid for verifying the data [4]. Information misuse makes a more substantial impact in the cloud. Cloud gives trademark points of interest, yet associations need to pick in perspective on expense cooperatively [5,6].

Cloud computing can help reduce costs, increase business readiness and empower to concentrate on ventures with an exceptional result on speculation. Nowadays digital misconduct is the worst risk to the general public [7]. It is independent of time, space, position, belief, country, urban or regional, rich or poor and capable or uneducated. Security remains the main limit in selecting Cloud computing for organizations and government offices [8]. Security and protection concerns are a huge obstacle, anticipating the broad selection of the public cloud over the business [9].

By and large, a cloud framework comprises fundamental server groups, the primary server groups are connected with one another. Every principle server group has n number of sub-datacentres and sub-datacentres are interconnected [10]. The sub-datacentres may have another arrangement of sub-datacentres, or it is logically associated with the users. The sample cloud topology is depicted in Figure 1.

Moving large amounts of data to the cloud is convenient for users since it alleviates the stress of managing infrastructure and data on-premises. Data as a service, platform as a service, and infrastructure as a

CONTACT G. Rajchakit kreangkri@mju.ac.th Department of Mathematics, Faculty of Science, Maejo University, Chiang Mai 52290, Thailand; Fairouz Tchier ftchier@ksu.edu.sa Department of Mathematics, King Saud University, P.O. Box 22452, Riyadh 11495, Saudi Arabia

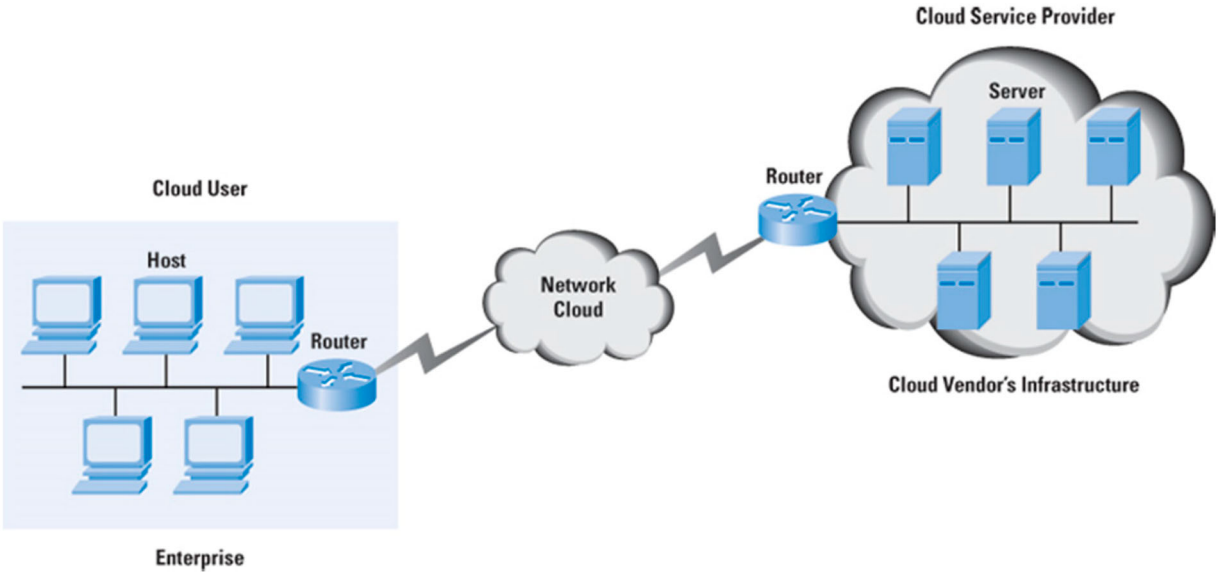

Figure 1. Sample cloud topology.

service are all examples of cloud computing services. This service also provides clients with a low-cost, scalable, secure, and dependable environment. There are internal and external dangers to data integrity in the cloud, even though it is more powerful and trustworthy than a personal computer system.

Map Reduce is a programming model for handling enormous informational indexes with a parallel correspondence calculation on a group [11]. A Map Reduce program is made out of a Map() technique that performs sifting and arranging, such as arranging understudies by the first name into lines. One line for each name and a Reduce() strategy that plays out a rundown activity, including the number of understudies in each line, resulting in name frequencies [12]. The Map Reduce System organizes by assembling the circulated servers, running the different assignments in parallel, dealing with all interchanges and information moves between different pieces of the framework, accommodating repetition and adaptation to noncritical failure, and generally the executives of the entire procedure [8].

Map Reduce can be applied to essentially more enormous datasets than product servers can deal. A huge server can utilize Map Reduce to sort a petabyte (thousand terabytes) of information in just a couple of hours [13]. The parallelism also offers some plausibility of recouping from halfway regression of servers or capacity during the activity [14]. On the off chance that one mapper or reducer falls flat, the work can be rescheduled – accepting the information is as yet accessible [15]. The workflow of the map and reducer is illustrated in Figure 2.

PK-Anonymity posts randomization strategy (PRAM) and control accurate exposure. PRAM fulfils PK-Algorithm in a controlled manner. One can control the PRAM's parameter so that PK is fulfilled [16]. PK properties are probabilistically randomized and, after that, rebuilt. So, it gives increasingly exact measurement and all the more dependably provides security for the data in the cloud [17]. In the PK method, nobody can animate which individual record originated from which more than I/k probability [18].

1.1. Attacks in cloud computing

As the world is moving towards cloud computing, it becomes increasingly advanced and error-free. A portion of the potential assaults on cloud computing is given next.

1.1.1. Denial of Service (DoS)

In the DoS assault, an aggressor over-burdens the objective cloud framework with administration demands, so it quits reacting to any new requests and consequently made all resources inaccessible to its clients. DOS assaults are of numerous kinds.

- Attackers can over-burden the objective with an enormous measure of unwanted information that reduces the system's transmission capacity and resources.
- Attackers can utilize space of different systems' administration conventions to over-burden target resources.
- Attackers can make HTTP demand in huge sum with the goal that the server cannot handle it.

For limiting DoS attack, we can group traffic based on approval, so we can double the traffic that is distinguished as unapproved and permit traffic that is recognized as approved. For this, firewalls can be utilized to allow or deny traffic based on getting to conventions, ports or IP addresses.

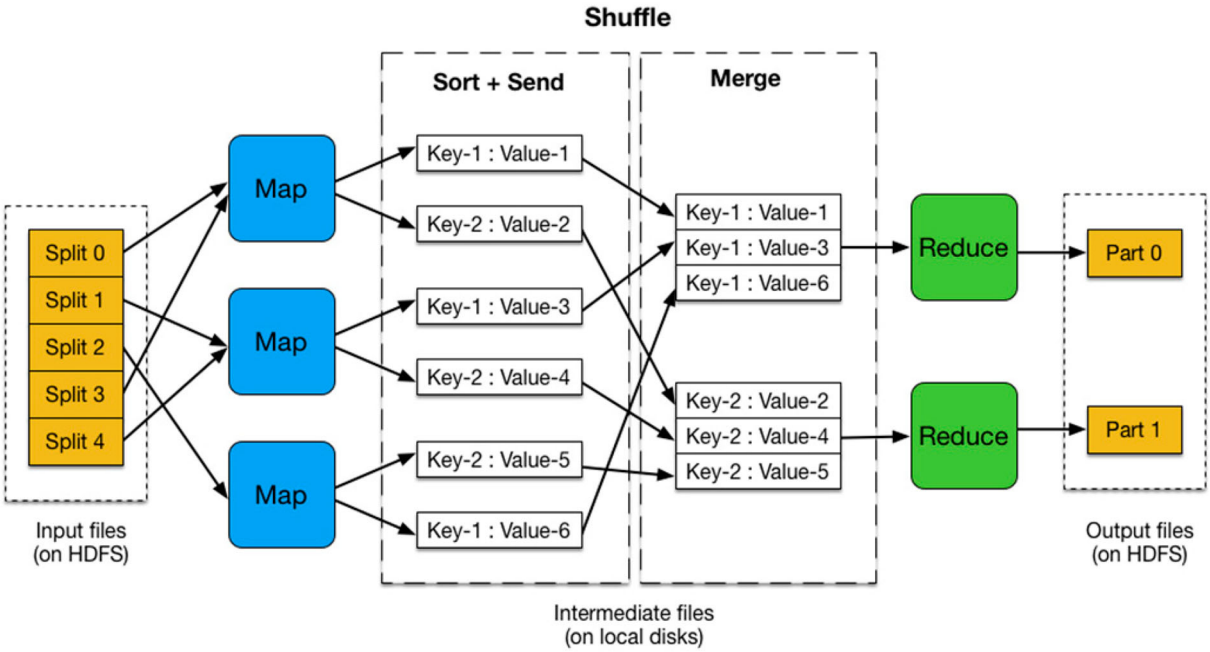

Figure 2. Map Reduce inputs and outputs.

1.1.2. Injection attack

In an injection attack, an attacker attempts to infuse malevolent help or virtual machine into the cloud. In this kind of assault, the assailant makes its own noxious help execution module or virtual machine and attempts to add it to the Cloud framework.

In the cloud computing framework, applications kept running by the client are considered with high proficiency and trustworthiness. So to keep the cloud free from injection assault, we can join the trustworthiness with equipment or utilize equipment for trust in light of the fact that it is hard to interrupt in the IaaS level for an aggressor.

1.1.3. Validation attacks

Validation/Authentication is a powerless point in cloud computing administrations, in which an aggressor often focuses. Today, most of the administrations still utilize a basic username and secret phrase sort of information-based confirmation. Yet, some special cases are monetary establishments that are utilizing different types of auxiliary verification, which make it increasingly hard for famous phishing attacks. Some validation assaults are

- Brute Force Attack
- Dictionary Attack
- Shoulder Surfing
- Replay Attacks
- Phishing Attacks
- Key Loggers

1.1.4. Man-in-the-middle attack

Here, the assailant captures messages in a public key exchange method and afterwards retransmits them, substituting his very own public key for the mentioned one. So, the two unique gatherings still have all the earmarks of being speaking with one another.

2. Literature survey

Wang et al. [1] proposed a K-Anonymity model to keep away from connecting attacks. Yet it can't deal with foundation information attack and homogeneity attacks, which are brought about by the missing trust selection in the database. Along these lines, a new approach is required to keep them away from both attacks.

Halabi et al. [2] surveyed the difficulties for the proactive attack identification in Cloud computing conditions. The long haul potential advantages of the Cloud computing condition were the decrease of expenses and the improvement of the business results. To make Cloud computing increasingly striking, the user needs to address the assortment of security dangers. In this overview, the comprehensive audit on Cloud computing was done.

Zhang et al. [4] proposed the k-Anonymity model, considering that an information owner needs to share a gathering of individual explicit information without uncovering the character of a person. This objective is accomplished by information speculation and concealment strategy to ensure the classified data and the re-identification attacks are analyzed.

Siadat et al. [6] discussed the security issues for Cloud computing and exhibited the system for a secure cloud on two of the three layers. The two layers centred were the capacity and the information layer. In this work, a protected combined question handling plan with the guide decrease and the Hadoop device. The XACML

execution was likewise discussed for the Cloud computing condition, in which the manufactures confide in applications.

Luna et al. [8] studied different dangers and attacks on the cloud and overviewed the security issues identified with Cloud computing. Cloud computing was viewed as the promising answer for getting to and utilizing the resources over the Internet. The incredible handling and capacity resources were given on request to lessen the expense and build the effectiveness of Cloud computing.

Arvind et al. [9] proposed a technique that presents a lot of calculations for delivering negligible full-space speculations and shows that these calculations perform up to a request for size quicker than past calculations on two genuine databases. Wang et al. [10] proposed another multidimensional model that gives an extra level of adaptability not found in single-dimensional methodologies.

Sinha et al. [11] discussed the security dangers and assurance of the resources in Cloud computing. The means to decrease the security issues and the worries in Cloud computing were likewise discussed. In this study, the advantages/qualities, shortcomings and application regions are likewise examined. The cloud arrangement in an undertaking framework has a portion of the significant security issues. The undertaking required the correct arranging and comprehension of the rising dangers, vulnerabilities and potential countermeasures.

Kim et al. [12] reviewed the related security issues in developing a single cloud to multi-mists. They centred on the advancement of the multi-cloud used to decrease the security dangers. The exchange is about the security conventions such as Byzantine Protocols and DepSky System for multi-cloud conditions. The support of innumerable users caused the administration accessibility level corruption. They examined different research works identified with the multi-cloud use procedure to decrease security dangers.

Hasan et al. [13] built up a protection-saving open reviewing framework for information security. They planned the recreation by thinking about the single user. They used the open key-based homomorphism authenticator and remarkably coordinate it with an irregular cover method and a programmed blocker.

Nakagawa et al. [14] proposed a safe Cloud storage framework that supports open examining for protecting the security of the users information. An outside reviewer was empowered to review the re-appropriated information of the user without learning the information content. The TPA was empowered to perform concurrent inspections of the different users effectively. The Homomorphic Linear Authenticator (HLA) and arbitrary veiling were utilized to ensure that the TPA is not familiar with any information stored on the cloud server during the reviewing procedure.

Kumar et al. [15] depicted a system rang base quest for finding the best anonymization. When the value of *k* is small, this procedure works altogether well. They demonstrated the practicability through analyses on genuine evaluation information for this methodology. To locate the ideal answer for small k esteems rapidly, the base up Approach works productively, and when k builds, the running time of a speculation plan increases.

The proposed a model isolates the key administration from the cloud supplier, facilitating the information, arranging partition. The key isolation secures the cloud supplier and customer from clashes once constrained to deliver information because of a legitimate order. Last and most noteworthy is personality and accesses the section, which consolidates character provisioning/non-provisioning, validation, organization, approval, and client profile.

Stergiou et al. [16] clarified that the cloud stage still accompanies each inner and outer security and protection danger, just as media disappointments, programming bugs, malware, executive blunders and pernicious insiders. As individuals and endeavours make a great deal of extra information that must be hung on and utilized, such as messages, individually secured records, symbol collections, charge archives, money-related exchanges, etc. They propelled to re-appropriate their convoluted local information in the board frameworks to the cloud because of its more prominent adaptability and cost-proficiency.

Zaaba et al. [17] managed security issues in SaaS are information security, organized security, information region allocation, information respectability, information isolation, information access, confirmation and approval, information secrecy, web application security, information loss, virtualization powerlessness, accessibility, reinforcement, personality the executives and sign-on technique.

Namasudra et al. [19] proposed, "Anonymization by Local Recoding in Data with Attribute Hierarchical Taxonomies". This framework is basically centred around individual security, which means the distributed informational collection isn't legitimate de-ID. De-recognizable proof methods avert the informational collection distinguishing proof from related data.

Singh et al. [20] proposed the valuable idea is "utility-based anonymization utilizing neighborhood recoding". This idea utilizes the neighbourhood recoding idea. It essentially and effectively depicts the worldwide recoding challenges. This method depicts the global recoding as mapping the areas; this space incorporates the semi- identifier qualities. The global recording has changed the qualities or summed up the information by utilizing the identifier characteristic in a particular quasi.

Mahmud et al. [21] proposed the security conservation idea is "Productive k-Anonymization Using

Clustering Techniques". This method centres around the k-anonymization technique. This technique requires anonymized information at the same time, it limits the information loss. This kind of result is obtained from the information adjustment time. In this framework, the k-anonymization strategy is used utilizing the clustering method. The significant value of this framework is great information quality.

2.1. Method for storing data dynamically in the cloud

Because the clients didn't have a local copy of the cloud-stored data, possibly cloud data storage isn't reliable. A new protocol system is developed to deal with these problems, which use the data scanning protocol method to verify data integrity and aid service providers in assisting their customers in verifying data security. These systems use homomorphism tokens, blocking extinction and unblocking factors, and distributed erasure-coded data as a flexible distributed file integrity auditing mechanism (FDSIAM).

2.2. Protocol for efficient and secure data storage

Users are increasingly outsourcing their data to service providers with ample storage space at a lesser cost. A safe and efficient storage technique is provided that ensures the secrecy and integrity of the stored data. A sober sequence is used to verify data integrity and create an elliptic curve cryptographic protocol. Before sending data and software to the cloud, cloud clients must complete a protocol step that adds privacy enforcement to the programmer and data. The secure authentication protocol is a credential that protects the information of the data from being seen by unauthorized parties. It is also utilized for dynamic data operations to maintain the same security and relieve consumers of data leakage and corruption issues.

2.3. Data storage security

The data are protected in the server based on the security technique selected by the user, ensuring that only the most sensitive information is transferred across servers. Data transmission over the Internet is risky because of unauthorized intrusions. In a cloud computing context, data encryption is critical. A secure cross-platform architecture with a consistent and innovative structure is implemented for offering security to the cloud model. Two-way handshakes are presented based on token management. Using the homomorphic symbol with distributed confirmation of erasure-coded data, our approach integrates storage correctness guarantee and data error localization (i.e. identifying a misbehaving server), we achieve our goal.

2.4. Secure and reliable storage service

The storage service allows customers to store data in the cloud and use well-qualified applications that are readily available without being concerned about data storage. However, while cloud service providers gain from this, users lose control over their own data, introducing new value ability hazards to cloud data accuracy. The homomorphism token and dispersed coded-data were developed as a flexible tool for auditing the integrity of distributed storage. As part of the new architecture, efficient and secure dynamic operations on outsourced data will be supported.

3. Proposed work

Logical Pk-Anonymization differs from the current Pk-Anonymization methodology in which it loses a lot of data and takes a long time to complete the conversion. As opposed to the security constraints, the existing Pk-Anonymization uses a scientific enhancement of K-Anonymity. It does not necessitate any kind of parametric assumption. It's essential to compare the probabilistic microdata calculation's security level with the deterministic counterpart. Large amounts of Big Data are reduced using techniques, such as map reduction. You won't find any duplicates in it. In addition, trustworthy data are aimed at the PK-Anonymization process. Three steps make up the Map Reduce algorithm. The information is mapped, rearranged, and reduced as part of the process. Map reduction information is subjected to the Logical Pk-Anonymization approach to overcome the proposed technique's shortcomings and increase performance.

An extreme estimate of k must be used to prevent anonymization from being unpredictable [19]. It will be difficult to anonymize the dataset if it is higher [20]. When information is gathered per the Logical Pk-Anonymity methodology, K records are vague as far as the semi-identifier is concerned. Elements connected with additional elements that have been given semi-identifiers [22] are commonly referred to as "semi" elements. Figure 3 illustrates the framework's recommended methodology.

When anonymizing, the first esteem in the record will be changed to give security. It must be limited to provide great anonymization. Moreover the loss of data is almost reduced in the proposed technique.

The total information obtained after performing Logical Pk-Anonymization is calculated as

$$IG(V) = E(T[v]) - \sum c \frac{|T[c]|}{|T[v]|} E(T[c]) \qquad (1)$$

where v is the index of each record, T is the time instance and c is the cluster set.

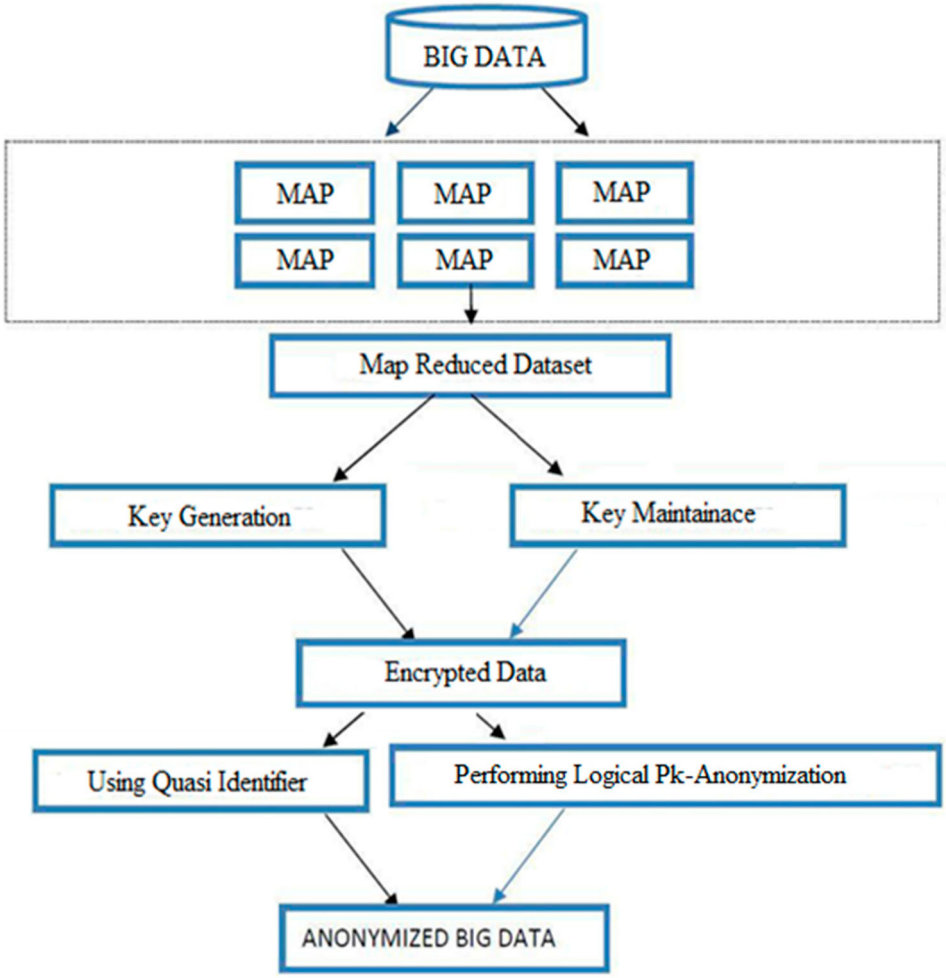

Figure 3. Architecture outline of logical PK-anonymity.

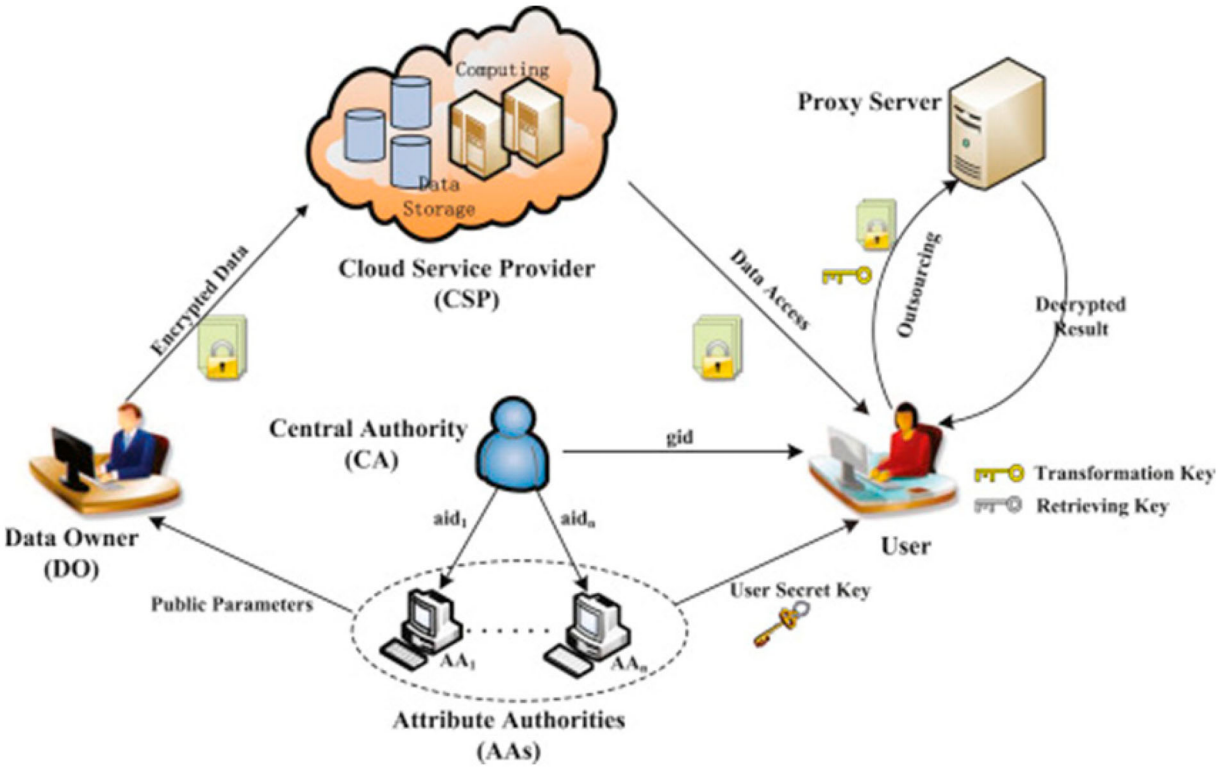

Figure 4. Key usage process.

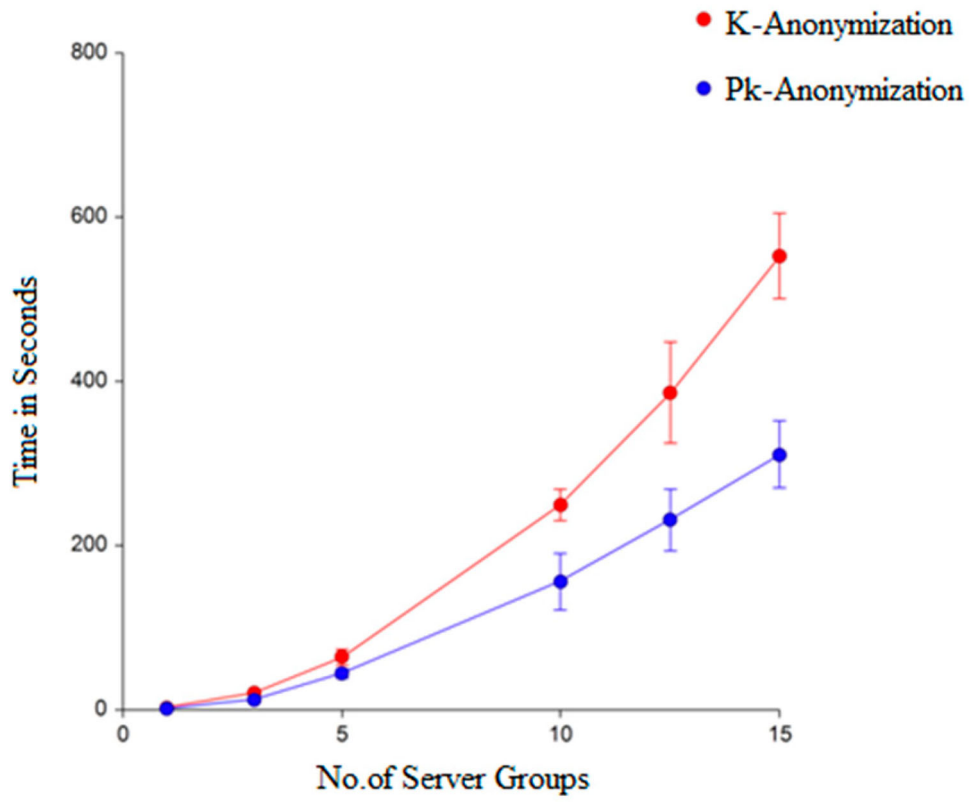

Figure 5. Framework establishment time.

3.1. Need for clustering

Clustering is the assignment of collecting many records so that items in a similar gathering are increasingly comparative to one another than to those in different groups. It is a fundamental assignment of exploratory information mining and a typical strategy for measurable information examination, utilized in numerous fields, including AI, design acknowledgment, processing of images, and so forth.

A cluster of information records can be treated as one gathering [23]. While doing cluster examination, we first segment the arrangement of information into gatherings, depending on information closeness and afterward dole out the marks to the gatherings [21]. The fundamental favourable position of clustering over arrangement is that it is versatile to changes and assists single with relevant features that recognize various groups. In the proposed work, an Enhanced Probability Clustering Method (EPCM) is used for performing clustering. The EPCM algorithm is used for performing clustering.

Input: Data sets – DS

Step-1 Load the dataset DS into a cloud environment.

Step-2 Calculate the probability mean value of every record T(c1) − T(cn), h $<=$ th $<=$ Max, h is the starting record value, th is the threshold and Max is the final recordset.

Step-3 Probability Mean $=$ T′(th)(Max − h) $*$ DS(r1..rn)

Step-4 For each cluster of parameter type

i. For each data record do

ii. Calculate Intrusion posteriori distributions exp Rth,N,r

iii. IPd $=$ $\frac{}{\nu \exp \text{comp(cn,th)}} *$ Mean

iv. until R(i) $=$ $=$ 0

v. end for

vi. end for

Step-5 To Parameter P_x generate cluster setCS_i

1. do
2. $CS_x(P) = P_x$;
3. $P_x = P_x{+}{+}$;
4. done

Step-6 Update cluster CS_x.

1. $M_x(CS) = CS_x$;

The proposed calculation to apply the Pk-Anonymization technique is portrayed below.

3.2. Algorithm Pk-Anonymization

Start

DS-Input Bigdata Set

I-Quasi Identifier

r-Initial level

Pk-original probability value to perform Pk-Anonymization

DS$*$-Anonymized Big dataset

Begin

Step-1: Input Big data set DS to simplify

Step-2: Specify the quasi identifier I(r)

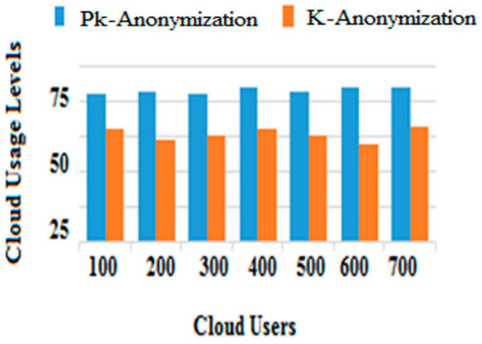

Figure 6. Cloud usage levels.

Step-3:If DS(r) has duplicate value
Step-4:callmap_reduce()
Step-5: DS∗(r) = sigma (DS(r) ∗ I(r)
Step-6:else
Step-7:Pk = max(P_r, P_{max})
Step-8:end if
Step-9:change the r value to k value
Step-10:DS∗(r(I)) = DS(r(k))
Step-11: Maintain a cluster DS∗ which contains anonymized data
End
Stop

In the above algorithm, a dataset is initially considered, which is encrypted using a cryptographic strategy. Later, these data are considered for performing Pk-Anonymization. Here a Quasi Identifier "I" is considered if there is a huge amount of data. Cluster sets are generated after Pk-Anonymization is applied. The data clusters after Pk-Anonymization is stored in the cloud, which is more secured, and unauthorized users are not allowed to access the data.

3.3. Key generation process

Attribute-Based Encryption (ABE) is utilized for one-to-numerous encryption. Using the character strings, the public key for encrypting the information is produced. In ABE, there are three principal factors: authority, information owner, and information user. The job of every entertainer is outlined in Figure 4. The principal job of the authority is to produce keys for the information owners and the information users for encoding or decoding the information [23]. The authority delivers the public key, and secret key depending on the traits. The created keys are kept up for future access. On the off chance that another information user enters the framework without the pre-characterized characteristics, the position will rethink the characteristics. It will recover the public key, and secret key [21]. The primary job of the information owner is to encode the information with the public key and the arrangement of properties.

The information owner keeps up the information for sharing. At first, the information owner enrols their information in the cloud server and make entry by approving the data from the cloud server. The information owners can process or make the information record. Furthermore, they can create the information storehouse for determining the information owner properties. The job of the information user is to decrypt the encoded information utilizing the private key obtained from the central authority [24,25]. While decrypting the information, the characteristics in the private key of the information user, and the properties in the encrypted information ought to be coordinated.

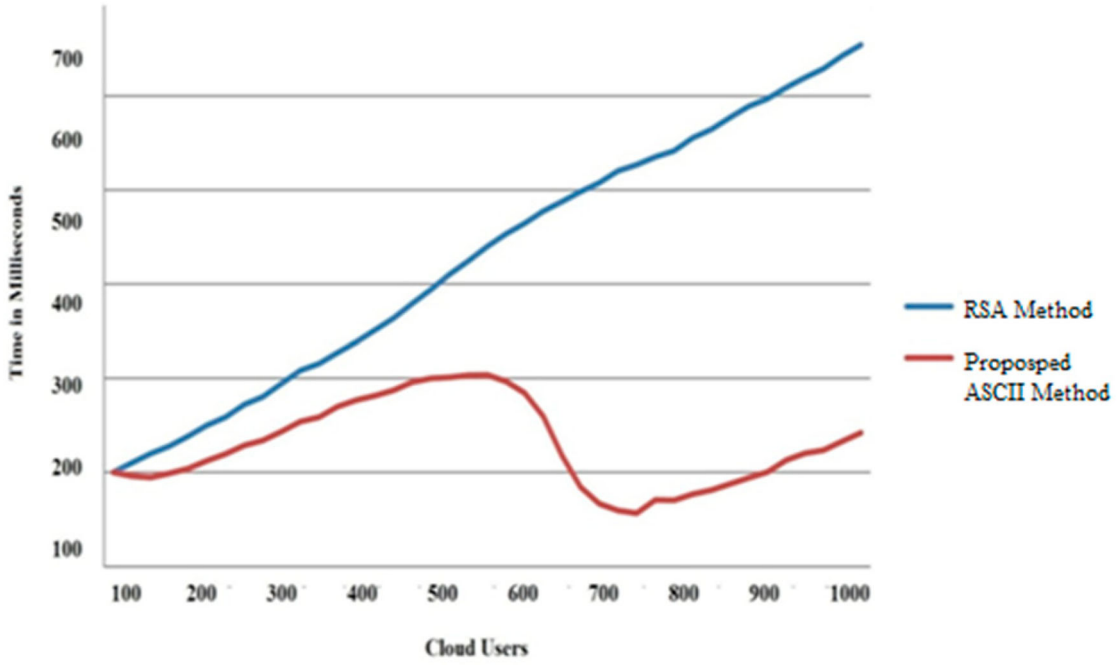

Figure 7. Data encryption time.

The process of ASCIIencryption is depicted below.
Input: SD- > Secret Date, K- > Key,Pid- > Public id
Encrypt ()
Begin
String1 [] = SD
String2[] = to_convert_ASCII(SD)
Split(String2,10) until length(String2)
String2[] = DeciConv(String2)
split(String2) Until String[SD] < 10
Cipher[] = String2[SD]*Pid
Return Cipher[]
Return String1[]
End
The proposed AES calculation checks the plain message. The production of the encryption key depends on two keys: public key and private key [26]. When the new encryption key is created, the plaintext is encoded. As a result, the content is delivered.

4. Results

The proposed is implemented in java. The dataset related to financial activities is considered from https://relational.fit.cvut.cz/dataset/Financialrepository in which the data have to be successfully stored in the cloud by applying the proposed strategies. The proposed Pk-Anonymization is compared with the traditional K-Anonymization model. The proposed Pk-Anonymization technique is applied to the dataset after the dataset is applied with the encryption method. The framework establishment time is illustrated in Figure 5.

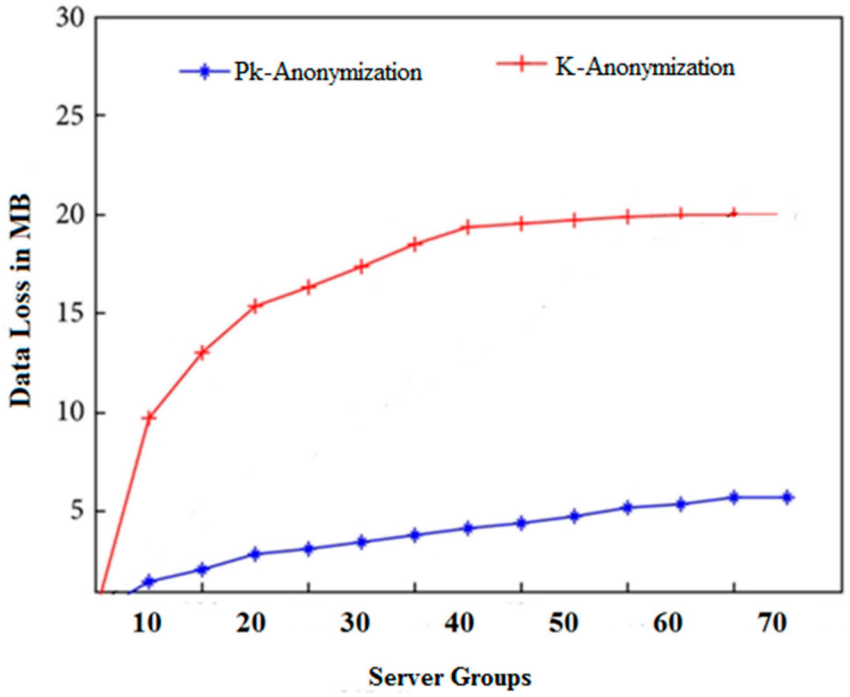

Figure 8. Data lost rate.

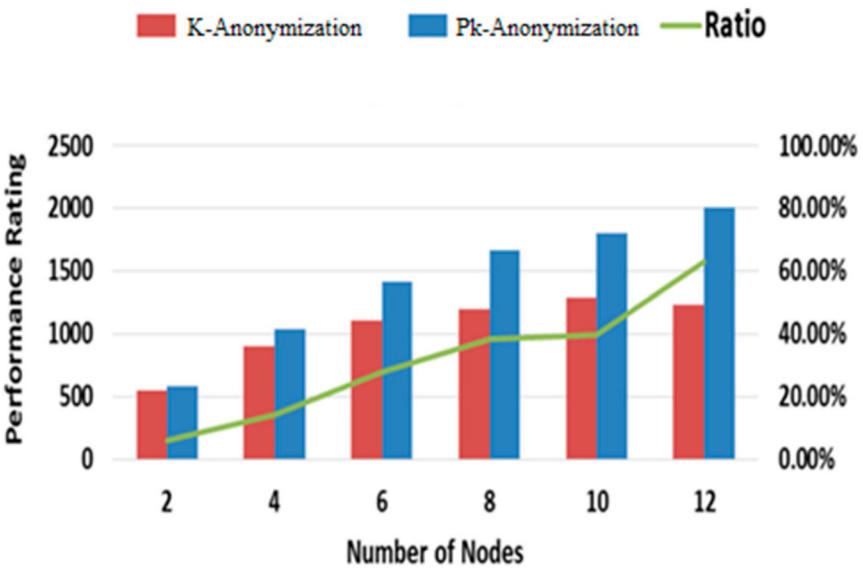

Figure 9. Performance analysis.

The proposed method provides a secured data storage environment for storing the data and accessing the data, and the cloud usage levels of the proposed method are depicted in Figure 6.

The proposed data encryption method is more accurate. The time for performing encryption on the data provided by the cloud user encryption time is compared with the traditional methods. The results show that the proposed method exhibits better results (Figure 7).

The data after encryption will undergo Pk-Anonymization, and then during the process, the data will be lost, and then it will be grouped as a cluster. The lost data rate is illustrated in Figure 8.

The overall performance of the proposed method is compared with the proposed method, and the results show that the proposed method performance is better than existing methods. The performance levels are illustrated in Figure 9.

5. Conclusion

PK-Anonymization performs superior functionalities than K-Anonymity as far as information utility and data loss. With the goal that the security of the enormous information will be lost, the Pk-Anonymization concept provides more security to the cloud environment. To perform anonymization, keeping up the degree of anonymization is significant. It proposes a flexible, versatile, dynamic and logical security structure depending on Map Reduce on the cloud. The outcomes demonstrated that as the protection level of users is low, the anonymization brings about data loss than those with high-security levels. The running time of anonymization likewise relies upon the size of information and cardinality of the datasets. The Logical Pk-Anonymization secrecy method is fit for anonymizing information that is already encrypted to a sensible degree of protection while holding the information utility. The proposed method exhibits better performance than traditional methods. The proposed model can handle a large group of users; however, load balancing is a challenging task that needs to be handled. In the future, user validations also need to be performed for controlling the data access by unauthorized users. The Pk-Anonymization model can be updated by reducing the computational capabilities to reduce the overhead on the cloud model.

Acknowledgment

This research was supported by the researchers Supporting Project Number (RSP-2021/401), King Saud University, Riyadh, Saudi Arabia.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research was supported by the researchers Supporting Project Number [RSP-2021 / 401], King Saud University, Riyadh, Saudi Arabia.

ORCID

G. Rajchakit http://orcid.org/0000-0001-6053-6219
Choonkil Park http://orcid.org/0000-0001-6329-8228

References

[1] Wang Q, Chen D, Zhang N, et al. PCP: a privacy-preserving content-based publish–subscribe scheme with differential privacy in fog computing. IEEE Access. 2017;5:17962–17974.
[2] Halabi T, Bellaiche M. Towards quantification and evaluation of security of cloud service providers. J Inf Secur Appl. Apr. 2017;33:55–65.
[3] Noor TH, Sheng QZ, Yao L, et al. Cloudarmor: supporting reputation-based trust management for cloud services. IEEE Trans Parallel Distrib Syst. Feb. 2016;27(2):367–380.
[4] Zhang W, Lin Y, Xiao S, et al. Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing. IEEE Trans Comput. 2016;65(5):1566–1578.
[5] Yang Y, Peng X, Fu D. A framework of cloud service selection based on trust mechanism. Int J Ad Hoc Ubiquitous Comput. 2017;25(3):109–119.
[6] Siadat S, Rahmani AM, Navid H. Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model. J Supercomput. 2017;73(6):2682–2704.
[7] Li X, He J, Zhao B, et al. A method for trust quantification in cloud computing environments. Int J Distrib Sensor Netw. 2016;12(2):5052614.
[8] Luna J, Taha A, Trapero R, et al. Quantitative reasoning about cloud security using service level agreements. IEEE Trans Cloud Comput. Sep. 2017;5(3):457–471.
[9] Arvind K, Manimegalai R. Secure data classification using superior naive classifier in agent based mobile cloud computing. Cluster Comput. 2017;20(2):1535–1542.
[10] Cloud computing service metrics description. National Institute of Standards and Technology, Standard, 2018.
[11] Sinha A, Jana PK. A hybrid mapreduce-based k-means clustering using genetic algorithm for distributed datasets. J Supercomput. 2018;74(4):1562–1579.
[12] Kim H. Enhancing trusted cloud computing platform for infrastructure as a service. Adv Elect Comput Eng. 2017;17(1):9–14.
[13] Hasan ASMT, Jiang Q, Luo J, et al. An effective value swapping method for privacy preserving data publishing. Secur Commun Netw. 2016;9:3219–3228.
[14] Nakagawa T, Arai H, Nakagawa H. Personalized anonymization for set-valued data by partial suppression. Trans Data Priv. 2018;11:219–237.
[15] Kumar S, Nayak C. An approach to detect malicious feedback rating for measuring web service reputation, 2016.
[16] Stergiou C, Psannis KE, Kim B-G, et al. Secure integration of IoT and cloud computing. Future Gener Comput Syst. Jan. 2018;78:964–975.
[17] An YZ, Zaaba ZF, Samsudin NF. Reviews on security issues and challenges in cloud computing. IOP Conf Ser Mater Sci Eng. 2016;160:012106.
[18] Jain P, Gyanchandani M, Khare N. Big data privacy: a technological perspective and review. J Big Data. 2016;3:25.

[19] Namasudra S, Roy P. Secure and efficient data access control in cloud computing environment: a survey. J Multiagent Grid Syst. 2016;12:69–90.
[20] Singh VK, Singh T. Present data security issues and their resolving technique in cloud computing. Int J Sci Technol. 2016;1:1–6.
[21] Mahmud R, Kotagiri R, Buyya R. Fog computing: a taxonomy, survey and future directions. In: Di Martino B, Li KC, Yang LT, Esposito A, editors. Internet of everything: algorithms, methodologies, technologies and perspectives. Singapore: Springer; 2018. p. 103–130.
[22] Singh S, Jeong YS, Park JH. A survey on cloud computing security: issues, threats, and solutions. J Netw Comput Appl. 2016;75:200–222.
[23] Yu Y, Xue L, Au MH, et al. Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Gener Comput Syst. Sep. 2016;62:85–91.
[24] Goryczka S, Xiong L, Fung BC, et al. m-Privacy for collaborative data publishing. IEEE Trans Knowl Data Eng. 2014;26(10):2520–2533.
[25] Soria-Comas J, Domingo-Ferrer J, Sanchez D, et al. t-Closeness through microaggregation: strict privacy with enhanced utility preservation. IEEE Trans Knowl Data Eng. 2015;27(11):3098–3110.
[26] Zhang X, Yang LT, Liu C, et al. A scalable two-phase top down specialization approach for data anonymization using map reduce on cloud. IEEE Trans Parallel Distrib Syst. 2014;25 (2):363–373.