Hindawi
Journal of Function Spaces
Volume 2023, Article ID 9873072, 1 page
https://doi.org/10.1155/2023/9873072

Retraction

Retracted: Data Verification of Logical Pk-Anonymization with Big Data Application and Key Generation in Cloud Computing

Journal of Function Spaces

Received 22 August 2023; Accepted 22 August 2023; Published 23 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. P. Kumar and R. Anandan, "Data Verification of Logical Pk-Anonymization with Big Data Application and Key Generation in Cloud Computing," *Journal of Function Spaces*, vol. 2022, Article ID 8345536, 10 pages, 2022.

Hindawi
Journal of Function Spaces
Volume 2022, Article ID 8345536, 10 pages
https://doi.org/10.1155/2022/8345536

Research Article

Data Verification of Logical Pk-Anonymization with Big Data Application and Key Generation in Cloud Computing

Sindhe Phani Kumar and R. Anandan

Department of CSE, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai 600117, India

Correspondence should be addressed to Sindhe Phani Kumar; phanikumar_s@pace.ac.in

Received 11 March 2022; Accepted 3 May 2022; Published 23 June 2022

Academic Editor: Muhammad Gulzar

Background. As more data becomes available about how frequently the cloud can be updated, a more comprehensive picture of its safety is emerging. The suggested artworks use a cloud-based gradual clustering device to cluster and refresh a large number of informational indexes in a useful manner. *Purpose*. Anonymization of data is done at the point of collection in order to safeguard the data. More secure than K-Anonymization, Pk-Anonymization is the area's first randomization method. A cloud service provider (CSP) is an independent company that provides a cloud-based network and computing resources. Customers' security and connection protection must be verified by an authority before facts may be transferred to cloud servers for storing information. *Method*. Logical Pk-Anonymization and key era techniques are proposed in this proposed artwork in order to verify the cloud records, as well as to store sensitive information in the cloud. Cloud-based informational indexes are used in the proposed framework, which is effective at handling large amounts of data through MapReduce; a parallel data preparation form is obtained; to get all information as new facts that joins after a while, information anonymization techniques to carry out each protection and immoderate information utilization while updating take place; information loss and clean time is reduced for substantial amounts of data. As a result, the safety and records software might be in sync.

1. Introduction

Cloud computing (CC) is referred to as one of the most essential modern eras inside the issue of records improvement. Because of its compositional shape and advances (flexibility/elasticity, form scalability, number of structures covered, reliability, and sustainability), it offers numerous benefits, inclusive of protection benefits, consolidate branch of facts, and excessive availability [1]. The new ideas were established with the useful resource of the usage of Clouds, as an instance, hazard estimation, inexperienced utilization of community assets thru the notion of sharing, and essential repositories, which increases the privacy, secrecy, and coverage stages and may be prepared to address new protection issues [2].

Cloud computing permits cloud clients to price decrease expenses for his or her services. Because safety is the most crucial constraint for the usage of cloud services, its miles are often ignored. While certain safety issues are not new, they will be useful in current designs, inclusive of server damage, records loss, and guarded key limits [3]. Cloud is portrayed as a degree that need to be strong for confirming the records [4], consistent with easily nonregulatory federal entities placed inside the United States. Mishandling data has a far-carrying out effect at the cloud. Cloud gives trademark interest additives, but establishments must pick out a price attitude cooperatively [5, 6].

Cloud computing can allow you to reduce charges, decorate organization preparedness, and pay hobby on jobs with an excessive go back on funding. Virtual misconduct is now a first-rate danger to most of the people of humans [7]. Inspite of time regardless of time, place, personality, or attitude, town or nearby, affluent or destitute, successful or illiterate. Security is an essential limit inside the use of cloud computing in organizations and government workplaces [8]. Concerns approximately safety are a tremendous impediment to extremely good adoption of the general public cloud over the financial agency [9].

A cloud framework, as an entire, has vital server organizations; the primary server groups are connected to each differently; every critical server business enterprise organization has n form of subdatacenters, and every subdatacenter is related to each other [10]. The subdatacenters may additionally furthermore have a couple of configurations of subdatacenters or be logically associated with the clients. Figure 1 shows the structure of a sample cloud.

MapReduce is a paradigm for controlling, organizing, and handling a big variety of numerous varieties of informative indexes with a launched relevance calculation on a subset [11]. Map discounting is a way utilized in information execution to reduce massive volumes of statistics into usable cumulative common not unusual overall performance. A MapReduce software program is deliberate and accomplished using the Map() and Reduce() strategies. A Map method is essentially primarily based at the break up-map method, wherein split divides massive volumes of enter challenge into smaller obligations and map executes the first-rate computation operation on each of those smaller subduties. [12]. The reduce() technique collects all aggregated, associated information returned via the map() technique and produces a single output fee. The MapReduce System organizes thru assembling the circulated workstations, computing multiple operations in parallel, showing all sorts of computations, and changing a number of the several additives of the community, version to nonvital fault, and generally the executives of the entire technique [8].

MapReduce may be used for obligations which might be possibly to be extra distant than what product workstations can deal with. MapReduce can be used by a powerful laptop to reorganize an exabyte (thousand petabytes) of statistics in a fragment of the time [13]. Furthermore, the simultaneous arrival of the calculations permits for recouping from midway decline of allocated server or storage performance in some unspecified time in the destiny throughout the method [14]. When one mapper or reducer fails, the task is rescheduled, permitting the facts to be beneficial [15]. Figure 2 shows the map's and reducer's art work flow.

Using the Pk-Anonymity post randomization method (PRAM), manipulate accurate exposure. PRAM has been demonstrated to meet the Pk-Algorithm in a regulated way. The parameters of PRAM may be modified to make sure that Pk is met [16]. PK homes are probabilistically randomized and rebuilt in case you want to provide an expanding sort of correct sizes and extra always offer safety for information inside the cloud [17]. In the Pk way, no person wants to animate which character document originated from which more than I/properly sufficient opportunity [18].

1.1. Cloud Computing Attacks. As the world moves toward cloud computing, it becomes more advanced and mistakes become less common. The following are examples of capability attacks against cloud computing:

1.1.1. Denial of Service (DoS). In this type of attack, a malicious actor increases site traffic on the cloud environment so that the device stops responding to new requests and, as a result, renders all things unreachable to its victims. DOS attacks come in a variety of flavors.

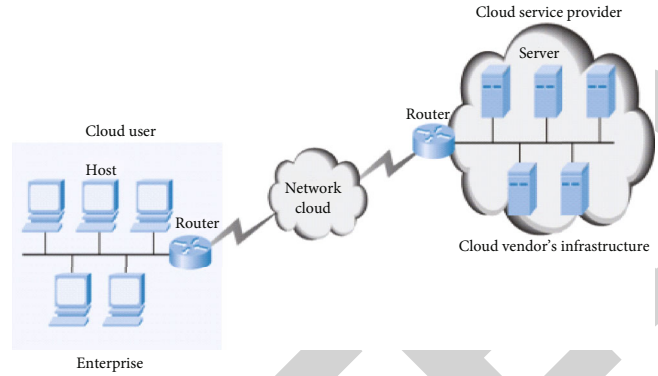

Figure 1: Sample cloud topology.

(i) An attacker can load more website visitors with the intention of sending a large amount of undesirable data, reducing the computer environment's transmission capability and assets

(ii) An attacker can employ a variety of cloud managing requirements and protocols to load a large number of website visitors onto a target beneficial useful resource

(iii) An attacker can generate a large amount of HTTP demand with the intent of preventing it from being processed by a centralized computing instrument

To limit DoS attacks, we can institute congestion largely based on authentication, which allows us to double congestion that is identified as unauthenticated and accepts congestion that is recognized as authenticated. To test this, firewalls might be used to admit or refuse congestion based on access protocols, requirements, IP addresses, and so on.

1.1.2. Injection Attack. In this type of cyberattack, a hostile actor attempts to inject malicious software or a virtual machine (VM) into the cloud. In this type of attack, the malicious actor creates his own nasty help implementation subsystem or VM instance and attempts to install it in a cloud environment.

In the cloud computing framework, utility journeys through the client are taken into account with extreme skill and trustworthiness. So, to defend injection assault and cozy cloud from assaults, we can connect the trustworthiness with infrastructure or rent infrastructure for trust because it is significantly more difficult for an aggressor to break cloud computing offerings.

1.1.3. Validation Attacks. In the cloud computing environment, validation/authentication is a powerless problem that is frequently targeted by malicious actors. Even today, most cloud environments require essential credentials and personal type of data-based total affirmation, but a common scenario is financial institutions that provide numerous

types of auxiliary verification, making it increasingly difficult for well-known social engineering attacks. Authentication attacks include

(i) brute force assault

(ii) dictionary assault

(iii) shoulder surfing

(iv) attacks on replay

(v) phishing

(vi) keyloggers

1.1.4. Man-in-the-Middle Assault. This is a type of cyberattack that involves session hijacking. In this attack, the bad actor joins the transaction concerned between events. He surreptitiously monitors the conversation between the two parties and steals the information from each of them by mimicking them. This type of assault consists of two stages: invading and hijacking. During the invading phase, the attacker infiltrates the communication between the victim and the genuine user. An effective man-in-the-middle operation does not always give up in the first segment. The invader then compromises all beneficial records, such as login credentials from events, in the second step.

The remaining sections of the paper are as follows. Section 2 discusses the literature survey on existing models, Section 3 discusses the proposed methodology to secure the data, Section 4 is the discussion section, Section 5 discuss about the results, and Section 6 concludes the paper.

2. Research Survey

Wang et al. [1] advanced a K-Anonymity architecture that removes linking assaults, but it does now not address basis of facts attack and homogeneity assault, which may be given approximately the use of a database loss of bear in thoughts opportunity. Along those lines, a sparkling method that builds on preceding assaults is needed. As a result of the work with the aid of the usage of Tamas Gal Baltimore et al., a way called L-numerous diversity is presently to be had (2008).

Halabi and Bellaiche [2] studied the issues related with proactive risk detection in the context of cloud computing. The blessings of the cloud computing state of affairs' long-time period transport capacity were lower fees and the advent of commercial enterprise organization outputs. Individuals are in search of to cope with the buildup of safety problems so that it will make cloud computing greater appealing. This evaluation is the premise for the complete cloud computing audit.

Zhang et al. [4] evolved the best enough-anonymity model in reaction to the seize 22 situation in which an information owner desires to evaluate a tough and speedy of person-specific facts without exposing the identification of a person. This motive is performed with the useful resource of the employment of real hypotheses and hiding techniques to guarantee records categorization, in addition to the examination of reidentification assaults.

Siadat et al. [6] diagnosed amazing facts privateness challenges for cloud computing and related the tool for comfortable cloud on one of the three degrees. The functionality layer and the information layer have been ranked first and 2nd, respectively. These paintings employ a complete protected question management approach that makes use of every guide decrease and the Hadoop tool. The XACML execution was modified into moreover stated for the Cloud computing state of affairs, which generates the confided in apps.

Luna et al. [8] explored precise cloud risks and assaults, in addition to the safety demanding situations related to cloud computing. Cloud computing is seemed as one of the successful ways for obtaining and utilizing property thru the Internet. The first-rate managing and functionality belongings have been made available on-demand which is an excellent way to lessen prices and increase the usefulness of cloud computing.

Arvind and Manimegalai [9] supplied a way for presenting a large sort of calculations for handling inconsequential whole-place speculations and established that such calculations to carry out in addition to a request for period quicker than in advance calculations on actual databases. de Vaulx et al. [10] endorsed each separate multidimensional version, which presents a similar degree of adaptability that is not specified in single-dimensional strategies.

Sinha and Jana [11] discussed the safety dangers and supply guarantee in cloud computing. The approach for reducing safety difficulties and troubles in cloud computing has become also mentioned. This examination covers the blessings/functions, flaws, and software program domain names. One of the most hard safety troubles is cloud association in an assignment shape. The challenge required proper planning similarly to interest to growing threats, vulnerabilities, and capability countermeasures.

Kim [12] investigated the associated safety challenges inside the transition from single cloud to multimists. They centered at the advancement of multicloud technology, which helps you to lessen security concerns. In phrases of safety necessities, remember Byzantine Protocols and the DepSky System for a multicloud situation. The help of a massive variety of clients led to coping with available degree corruption. They analyzed tremendous studies works at the utilization of the multicloud use technique for the bargain of protection threats.

For file protection, Hasan et al. [13] evolved a chance-free open reviewing apparatus. The Kingdom of the assignment on the identify the time and Visualising them as aunmarried man or woman. They hired an open key primarily based in fact homomorphism authenticator at the side of a commonplace cowl technique and a preprogrammed blocker.

Nakagawa et al. [14] advocated a relaxed cloud storage shape that permits for open evaluation for the protection of customers' information. An impartial examiner might now examine the purchaser's reappropriated info despite the fact that lacking knowledge of the facts content material fabric material. The TPA became granted the proper behavior concurrent inspections of the first-rate clients in an

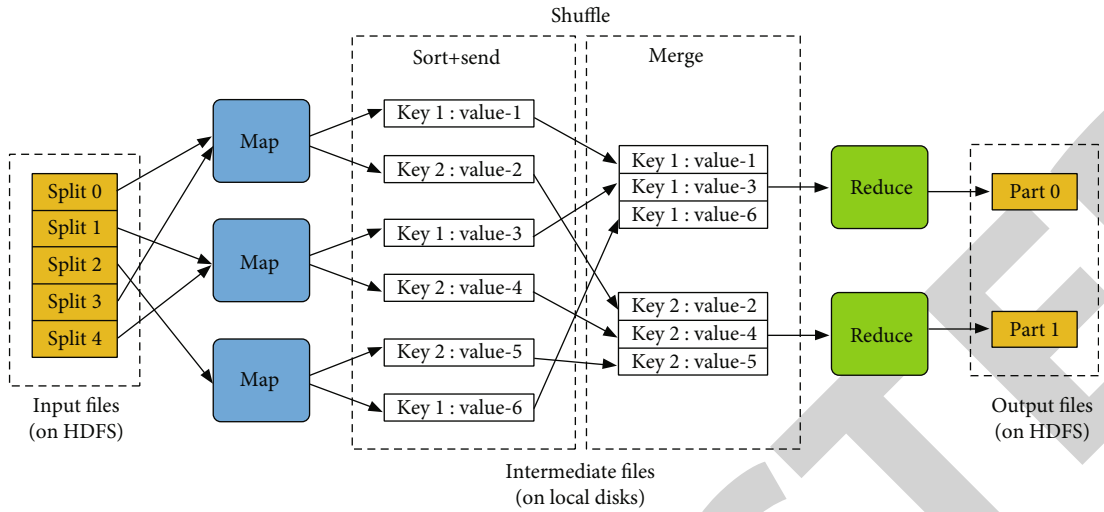

Figure 2: MapReduce inputs and outputs.

environmentally first-class way. The Homomorphic Linear Authenticator (HLA) and arbitrary veiling were employed to make certain that the TPA did no longer come into touch with any information approximately the information saved at the cloud server at any point in the course of the reviewing method.

Kumar and Nayak [15] verified a tool-based really sure look for awesome anonymization. When the rate of okay is low, this method works properly. They investigated the method's applicability through project assignment analyses on actual worldwide evaluation records. The lower level to Uplevel approaching works nicely for brief finding the proper solition for little good enough esteems and as accepted grows. So does on the foot time of a hypothesis plan.

A version is proposed that separates key manipulation from cloud employer facilitating statistics, ensuing in a partition affiliation. The key isolation shields both the cloud company and the patron from clashes by way of manner of preventing them from handing over information due to a valid order. Person and get right of entry to the section, which includes individual provisioning/nonprovisioning, validation, enterprise, approval, and patron profile the phase, are the final and maximum crucial interest.

Stergiou et al. [16] emphasized the cloud degree, as visible through the usage of making use of every internal and outer safety and protection concerns, which encompass media disappointments, programming flaws, malware, government mistakes, and malevolent insiders. Humans and their efforts generate a massive range of facts that need to be stored and used, together with messages, character-associated records, image collections, fee statistics, coin-related transactions, and so forth. Because of the cloud's extended adaptability and fee-information, they were compelled to re-adapt their locally difficult information the board frameworks.

An et al. [17] addressed protection issues in SaaS which incorporate information protection, organized protection, data place allocation, facts respectability, records isolation, records get proper of entry to, affirmation and approval,

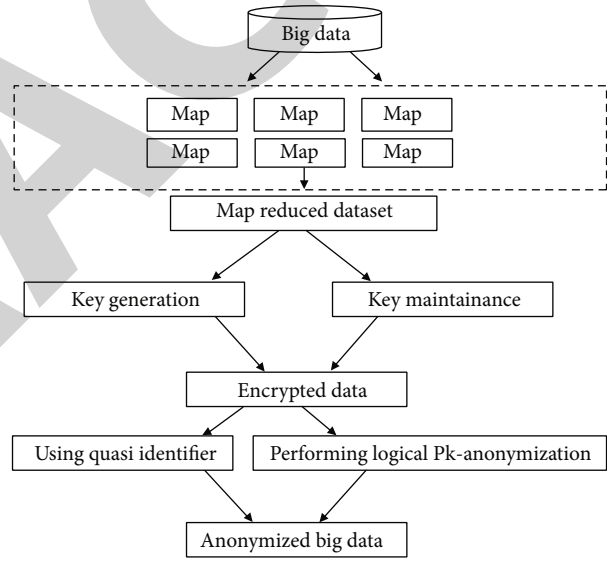

Figure 3: Block diagram of Logical Pk-Anonymity.

information secrecy, internet software safety, records loss, virtualization powerlessness, accessibility, reinforcement, person executives, and sign-on method.

Namasudra and Roy [19] defined "Anonymization with the valuable resource of Local Recoding in Data with Attribute Hierarchical Taxonomies." Because this framework is regularly geared at character safety, the informational collection is not always a legitimate de-ID. Deidentifiable proof strategies take away the need for an educational collection to differentiate amongst proof and facts.

The treasured idea supplied by Singh, V.K. and Singh, T. [20] is "software program software-based totally completely anonymous community recoding." Use the neighborhood recoding perception in this concept since it depicts the worldwide recoding complicated conditions as it must. This method demonstrates international recoding by way of mapping the regions; those regions are crafted from semi-

Input: Data sets - DS

Step-1Load the dataset DS into cloud environment.

Step-2Calculate the opportunity imply value of each file T(c1) − T(cn), h <=th <= Max, h is starting report cost, th is threshold and Max is the final document set.

Step-3Probability Mean= T'(th)(Max − h) ∗ DS(r1..Rn)

Step-4For each cluster of parameter type

(i) For each data record do

(ii) Calculate Intrusion posteriori distributions

(iii) IPd = exp {Rth, N, r}/vexp {comp(cn, th)} ∗ Mean.

(iv) until R(i)==0

(v) end for

(vi) end for

Step-5 To Parameter P_x generate cluster set CS_i

(i) do

(ii) $CS_x(P) = P_x$;

(iii) $P_x=P_x++$;

(iv) ` done

Step -6 Update cluster CS_x.

(i) $M_x(CS) = CS_x$;

Algorithm 1

identifier talents. With the use of the identification function, in particular quasi, global recoding has altered the tendencies or summed up the information.

"Productive good enough-Anonymization Using Clustering Techniques," in line with Mahmud et al. [21], is a protection conservation method. This technique is supposed to counteract the good enough-anonymization technique. This approach necessitates anonymized statistics at the same time as also proscribing records loss; This strategy needs anonymized statistics while also limiting record loss. On this framework, the clustering technique is hired to place into effect the adequate-anonymization approach. The immoderate fee of this framework is quite information adorable.

3. Proposed Work

The cautionary Logical Pk-Anonymization method differs from the winning Pk-Anonymization method in that it has a high rate of data loss and takes a lengthy time to complete the statistical conversion process. Inside current Pk-Anonymization, it is a systematic augmentation of K-Anonymity within the role of the safeguarding borders. There is no need for any parametric assumptions. It is crucial to compare the deterministic and probabilistic microstatistics calculations' safety steps. The Big Statistics are subjected to map discounting techniques first. In the statistics it contains, there are no duplicates. In addition, honest data is directed using a Pk-anonymization method. MapReduce uses three different approaches. It entails mapping, reorganizing, and minimizing the number of different statistics. To overcome the risks of the proposed approach, the map's following affiliation is subjected to Logical Pk-Anonymization, which improves the map's typical overall performance phases.

To avoid the unpredictability of anonymization, the most extreme estimate of k should obtain completely well worth [19]. It is significantly more difficult to anonymize the dataset if it comes higher than that [20]. When it comes to data gathering, the concept of Logical Pk-Anonymity is appealing since K statistics are indeterminate to the quantity and semi-identifier is concerned. A semi-identifier may be extremely closely related to an element that has multiple semi identifiers [22]. In Figure 3, the proposed device's mechanism is depicted.

Changing the first esteem in a report in order to preserve the data may be necessary for anonymization. Excellent anonymity necessitates restraint. In addition, there is less of a lack of information in the proposed method.

Logical Pk-Anonymization yields the following statistical data: $1G(v) = E(T[v]) - \sum_c (|T[c]|/|T[v]|)\, E(T[c])$, where v is the index of every document, T is the time instance, and c is the cluster set.

3.1. Functionalities of Cluster Computing and Need. Cluster analysis is a technique for categorizing data entry devices into several groups. Each agency may also have records devices that are similar to but unique from one another when compared to records devices from other groupings. It constantly separates the data items according on their degree of similarity and dissimilarity. Even if it indicates that the untagged facts are organically clustered among them, clustering is quite important. It is a significant difficulty in investigative and analytical data extraction, as well as a popular technique for measurable data study, used in a variety of fields such as AI and image processing.

A cluster is a grouping of factual items that have similar trends [23]. Cluster evaluation begins with the distribution of data to agencies based on data relevance, followed by the distribution of data to groups [21]. Clustering over arrangement has the significant benefit of being adaptable to changes and assisting singles with applicable talents that comprehend a variety of firms. Threshold value refers to a value or set of values that can be used to determine the quality level attained for a specific criterion and, as a result, the degree to which better environmental status has been achieved. The proposed model considers the threshold value

Algorithm: Pk-Anonymization
Start
DS - Input Big data set
I - Quasi identifier
r - Initial level
Pk - Original probability value to perform anonymization
DS∗ - Anonymized Big dataset
Begin
Step-1 Input large statistics set DS to simplify
Step-2 Specify the quasi identifier I(r)
Step- three If DS(r) have duplicate cost
Step- four Call map reduce()
Step- five DS∗(r)=sigma(DS(r))∗I(r)
Step-6 else
Step-7 Pk=max(pr, pmax)
Step- eight end if
Step- nine Change the r fee to k fee
Step-10 DS∗(r(I))=DS(r(ok))
Step-11 Maintain a cluster DS∗ which contains anonymized Data.
End
Stop

Algorithm 2: The proposed calculation to use the Pk-Anonymization method is portrayed beneath.

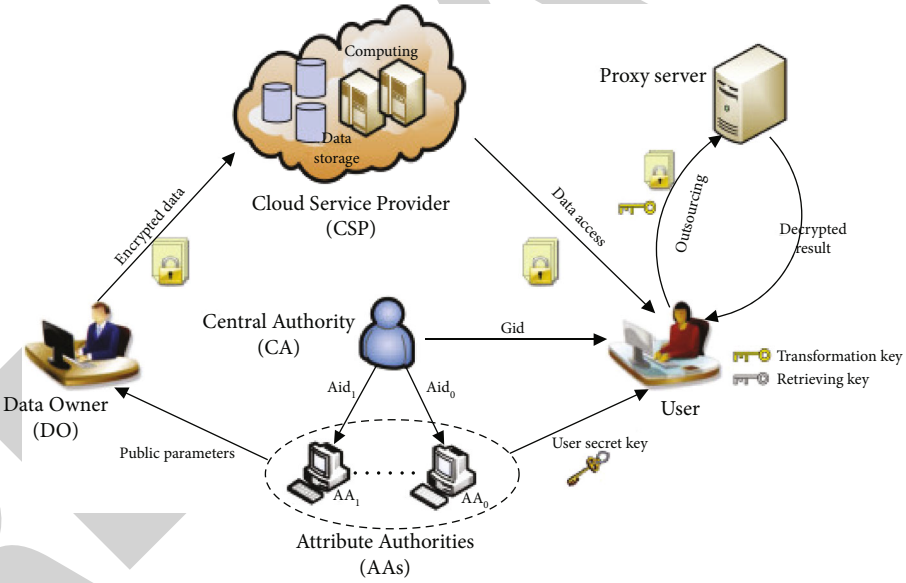

Figure 4: Key usage process.

as the number of registered users divided by the VM groups. Clustering is done using an Enhanced Probability Clustering Method (EPCM) in the suggested artworks. For acting clustering, the EPCM set of rules is employed.

To begin, the program takes into account a dataset that has been encrypted with a cryptographic mechanism. Pk-Anonymization is then generated the use of these data. A quasi identifier *I* is used while there are a massive amount of records. Cluster devices are built using the Pk-Anonymization software program tool. The data clusters are saved inside the cloud after Pk-Anonymization that is extra comfortable and stops unauthorized customers from gaining access to the statistics.

3.2. Key Generation Technique. For one-to-many encryption, attribute-based encryption (ABE) is used. The public key for encrypting information is created by using the man or woman strings. There are three main aspects in ABE: authority, data owner, and information user, for example. Each entertainer's activity is printed inside the Figure 4. The picture shows that the authority's primary responsibility is to generate keys for the data owner (DO) and fact customers to use in encrypting or decoding statistics [23]. The public key is generated by the authority, while the secret key is generated by the tendencies. The generated keys are kept in a safe place for future access. If another records

```
Algorithm Encryption
{
SD = Secret Date, K = Key, Pid = Public ID Encrypt ()
Begin
string[] = SD [] = to convert ASCII String2 (SD)
Split(String2,10) until the duration is reached (String2)[]=DeciConv String2 (String2)
Until String[SD]10 split(String2)String2[SD]∗Pid Cipher=Cipher[] should be returned.
Return 1[] String
End
}
Algorithm DecryptionE
{
public static String decrypt(String algorithm, String cipherText, SecretKey key)
            Cipher cipher = Cipher.getInstance(key);
          cipher.init(Cipher.DECRYPT_MODE, key);
          byte[] plainText = cipher.doFinal(Base64.getDecoder()
            .decode(cipherText));
          return new String(plainText);
}
```

Algorithm 3: The following diagram depicts the ASCII encryption and decryption method.

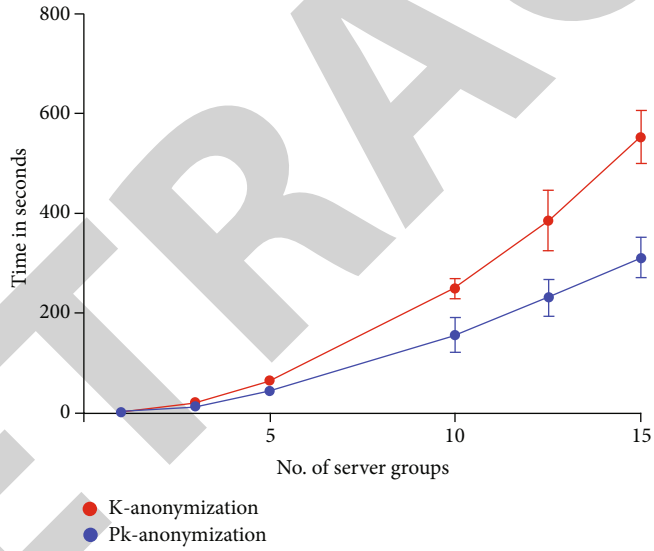

Figure 5: Difference of establishment time.

customer enters the framework without the predefined trends, the position will reconsider the developments and retrieve the public key and thriller key [21]. The DO's number one obligations consist of encrypting statistics and the usage of a public key and arranging housing.

The data owner is working hard to keep the information up to date so that it can be shared. The data owner first enrolls their information in the cloud server, then receives access by approving the information on the cloud server. The record's proprietors have the authority to regulate or assemble it. They also can develop an information database to decide facts approximately asset owners. The purpose of the data consumer is to decrypt the encoded cloth with the use of the personal key provided by using the way of the trusted authority [24, 25]. While decrypting the information, the dispositions of the statistics consumer's nonpublic key, similar to the homes within the encrypted statistics, need to be synchronized.

The proposed AES calculation verifies the message's appearance. The encryption key is generated using keys such as the public key and the personal key [26]. The plaintext is encoded, and the content is introduced as the end result when a new encryption secret is produced.

4. Discussions

The idea of storing data on the cloud has recently gained traction among technologists. Customers are increasingly storing their most essential data on cloud servers, without even keeping a duplicate on their own devices. In such cases,

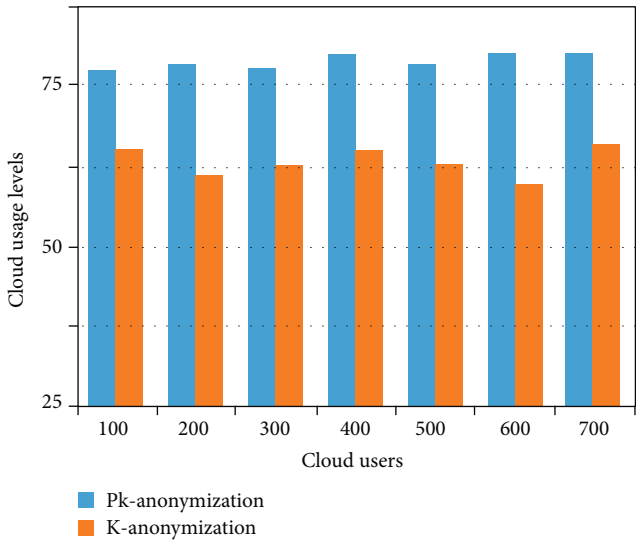

Figure 6: Server usage levels.

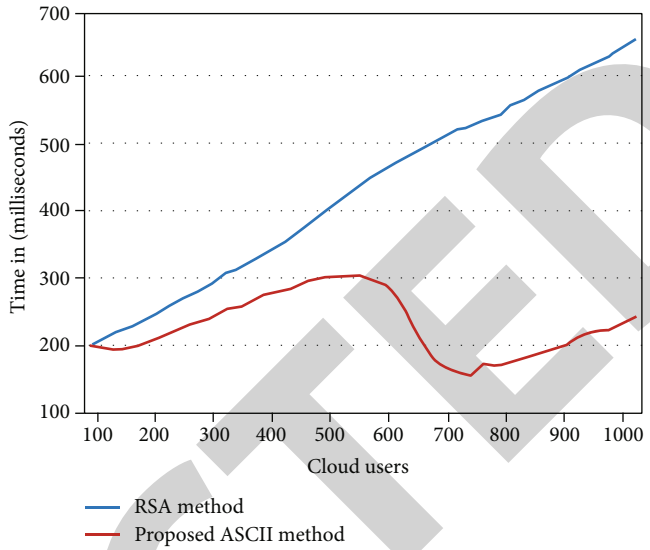

Figure 7: Data encryption accuracy time.

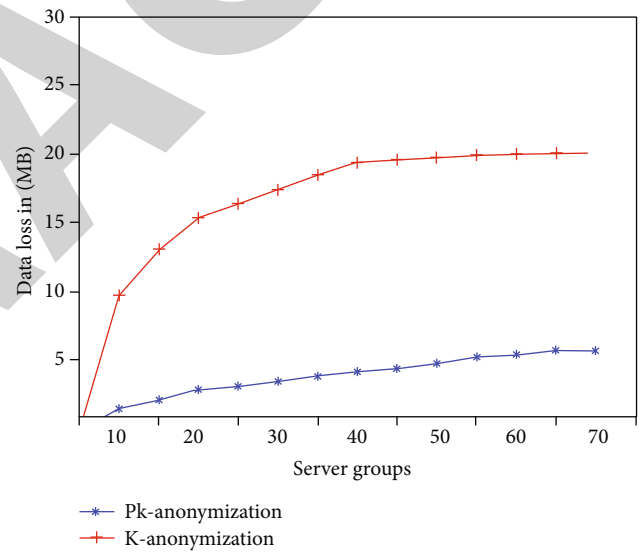

Figure 8: Data lost rate.

the clients must make sure that personal data is not lost or tampered with. Remote data integrity checking procedures have been developed throughout the years to ensure that stored data is accurate. These approaches, on the other hand, verify the authenticity of encrypted or plain text. After encryption, the complexity of doing calculations on encrypted data is a significant concern. Data can be anonymized instead than encrypted to protect privacy. Changes are made to data that will be utilized or disclosed so that crucial information cannot be identified. Data that has been anonymized can be stored and processed in the cloud without fear of unauthorized access.

Organizations can employ data anonymization to comply with severe data privacy rules that mandate the protection of personal information (PII), such as health records, contact information, and financial information.

Anonymization can be reversed, even if the identifiers have been removed, by using deanonymization techniques. Deanonymization procedures cross-reference sources can expose personal information because data often flows through multiple sources, many of which are publicly accessible.

Organizations can employ data anonymization to comply with severe data privacy rules that mandate the protection of personally identifiable (PII), such as health records, contact information, and financial data.

Deanonymization techniques can be used to retrace the process of data anonymization, despite the fact that the data of identifiers has been erased. De-anonymization procedures will cross-reference information and expose personal information because data often travels through multiple sources, some of which are exposed to the public.

5. Results

The proposed is written in Java, and the dataset for financial sports activities is sourced from the https://relational.Healthy.Cvut.Cz/dataset/Financial repository, where the statistics must be efficiently delivered in the cloud with the capability of implementing the given techniques. Following the implementation of the encryption method, the proposed Pk-Anonymization methodology is applied to the dataset. The structure for configuring order time is depicted in Figure 5

The proposed approach gives at ease records storage surroundings for storing records and having access to records, and the proposed method's cloud utilization stages are represented in Figure 6.

The proposed information encryption approach is more accurate, and the time it takes to encrypt the statistics that comes from the cloud is shorter than the time it takes to encrypt the data that comes from exclusive strategies. Figure 7 shows that the proposed method had better consequences.

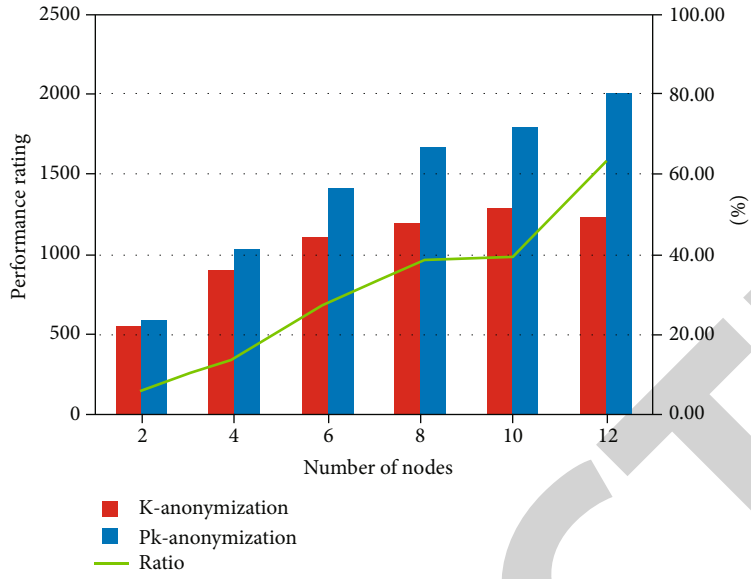

Figure 9: Performance rating report.

After encryption, the statistics could be Pk-Anonymized, and the facts can be lost for the duration of the procedure, at which point they may be collected as a cluster. Figure 8 depicts the charge for missing information.

The advised method's average accuracy is in assessment to the prevailing current day approaches, and the results display that the proposed approach's accuracy is accurate in evaluation to provide strategies. Figure 9 depicts the overall general performance ranges.

6. Conclusion

PK-Anonymization outperforms K-Anonymity in terms of statistics software and data loss. Using Pk-Anonymization, valuable information can be protected in a cloud context without risking its integrity. It is quite difficult to maintain the amount of obscurity required for anonymization to work properly. It offers an adaptable, flexible, dynamic, and logical security approach based on the cloud. Users with low security levels are more likely to lose data when they choose for anonymity, according to the study's findings. Additionally, the size of the datasets and their cardinalities affect how long it takes to anonymize data. Data that has already been encrypted to a tolerable level of security can be anonymized using the Logical Pk-Anonymization secrecy technique. This strategy is superior even when compared to conventional methods. The proposed model can handle the users with available resources; however, horizontal scalability is not supported in the model that needs to be enhanced in future to improve the performance levels.

Data Availability

The data used to support the findings of this study are included within the article. Should further data or information be required, these are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors thank the Vels Institute of Science, Technology & Advanced Studies, Chennai, for providing characterization supports to complete this research work.

References

[1] Q. Wang, D. Chen, N. Zhang, Z. Ding, and Z. Qin, "PCP: a privacy-preserving content-based publish–subscribe scheme with differential privacy in fog computing," *IEEE Access*, vol. 5, pp. 17962–17974, 2017.

[2] T. Halabi and M. Bellaiche, "Towards quantification and evaluation of security of cloud service providers," *Journal of Information Security and Applications*, vol. 33, pp. 55–65, 2017.

[3] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: supporting reputation-based trust management for cloud services," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 367–380, 2016.

[4] W. Zhang, Y. Lin, S. Xiao, J. Wu, and S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1566–1577, 2016.

[5] Y. Yang, X. Peng, and D. Fu, "A framework of cloud service selection based on trust mechanism," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 25, no. 3, pp. 109–119, 2017.

[6] S. Siadat, A. M. Rahmani, and H. Navid, "Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model," *The Journal of Supercomputing*, vol. 73, no. 6, pp. 2682–2704, 2017.

[7] X. Li, J. He, B. Zhao, J. Fang, Y. Zhang, and H. Liang, "A method for trust quantification in cloud computing

environments," *International Journal of Distributed Sensor Networks*, vol. 12, no. 2, 2016.

[8] J. Luna, A. Taha, R. Trapero, and N. Suri, "Quantitative reasoning about cloud security using service level agreements," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 457–471, 2017.

[9] K. Arvind and R. Manimegalai, "Secure data classification using superior naive classifier in agent based mobile cloud computing," *Cluster Computing*, vol. 20, no. 2, pp. 1535–1542, 2017.

[10] F. J. de Vaulx, E. D. Simmon, and R. B. Bohn, *Cloud Computing Service Metrics Description*, National Institute of Standards and Technology, Standard, 2018.

[11] A. Sinha and P. K. Jana, "A hybrid MapReduce-based k-means clustering using genetic algorithm for distributed datasets," *The Journal of Supercomputing*, vol. 74, no. 4, pp. 1562–1579, 2018.

[12] H. Kim, "Enhancing trusted cloud computing platform for infrastructure as a service," *Advances in Electrical and Computer Engineering*, vol. 17, no. 1, pp. 9–14, 2017.

[13] A. S. M. T. Hasan, Q. Jiang, J. Luo, C. Li, and L. Chen, "An effective value swapping method for privacy preserving data publishing," *Security and Communication Networks*, vol. 9, 3228 pages, 2016.

[14] T. Nakagawa, H. Arai, and H. Nakagawa, "Personalized anonymization for set-valued data by partial suppression," *Transactions on Data Privacy*, vol. 11, pp. 219–237, 2018.

[15] S. Kumar and C. Nayak, "An approach to detect malicious feedback rating for measuring web service reputation," *International Journal of Grid and Distributed Computing*, vol. 9, no. 3, pp. 109–116, 2016.

[16] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Generation Computer Systems*, vol. 78, pp. 964–975, 2018.

[17] Y. Z. An, Z. F. Zaaba, and N. F. Samsudin, "Reviews on security issues and challenges in cloud computing," *IOP Conference Series: Materials Science and Engineering*, vol. 160, no. 1, p. 012106, 2016.

[18] P. Jain, M. Gyanchandani, and N. Khare, "Big data privacy: a technological perspective and review," *Journal of Big Data*, vol. 3, no. 1, p. 25, 2016.

[19] S. Namasudra and P. Roy, "Secure and efficient data access control in cloud computing environment: a survey," *Multiagent and Grid Systems*, vol. 12, no. 2, pp. 69–90, 2016.

[20] V. K. Singh and T. Singh, "Present data security issues and their resolving technique in cloud computing," *International Journal of Science & Technoledge*, vol. 1, pp. 1–6, 2016.

[21] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: a taxonomy, survey and future directions," in *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*, B. Martino, K. C. Li, L. T. Yang, and A. Esposito, Eds., pp. 103–130, Springer, Singapore, 2018.

[22] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016.

[23] Y. Yu, L. Xue, M. H. Au et al., "Cloud data integrity checking with an identity-based auditing mechanism from RSA," *Future Generation Computer Systems*, vol. 62, pp. 85–91, 2016.

[24] S. Goryczka, L. Xiong, and B. C. M. Fung, "m-Privacy for collaborative data publishing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 10, pp. 2520–2533, 2014.

[25] J. Soria-Comas, J. Domingo-Ferrer, D. Sanchez, and S. Martinez, "T-closeness through microaggregation: strict privacy with enhanced utility preservation," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 11, pp. 3098–3110, 2015.

[26] X. Zhang, L. T. Yang, C. Liu, and J. Chen, "A scalable two-phase top-down specialization approach for data anonymization using MapReduce on cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 363–373, 2014.