
Naeem et al LGURJ CS IT 2020
ISSN: 2521-0122 (Online)
ISSN: 2519-7991 (Print)
LGU R Jounral for
Computer Sciences IT
Vol.4 Issue3, July-Sep 2020

Preservation of Privacy of Big Data Using Efficient Anonymization Technique

[1]Afia Naeem, [2] Dr. Muhammad Rizwan, [3] Dr. Fahad Ahmad
[1]Department of Computer Science, Kinnaird College for Women Lahore, Pakistan
[1]muhammad.rizwan@kinnaird.edu.pk

Abstract

Big data needs to be retained private because of the increase in the amount of data. Data is generated from social networks, organizations and various other ways, which is known as big data. Big data requires large storage as well as high computational power. At every stage, the data needs to be protected. Privacy preservation plays an important role in keeping sensitive information protected and private from any attack. Data anonymization is one of the techniques to anonymize data to keep it private and protected, which includes suppression, generalization, and bucketization. It keeps personal and private data anonymous from being known by others. But when it is implemented on big data, these techniques cause a great loss of information and also fail in defense of the privacy of big data. Moreover, for the scenario of big data, the anonymization should not only focus on hiding but also on other aspects. This paper aims to provide a technique that uses slicing, suppression, and functional encryption together to achieve better privacy of big data with data anonymization.

Keywords: Big Data, Anonymization, slicing, functional encryption, Privacy Preservation

1. INTRODUCTION

Big data can be termed as the study of big datasets generated from multiple sectors e.g. from systems, social media, etc. Data has become the raw material for production, a new source of economics and social value. Big data provides a valuable outcome to all the data analyst so that they could use it again. It has become an important topic for research purposes. Big data can help in the business purpose for the analysis purpose [1]. Data generated can be classified into two ways that are active data generation and passive data

generation. In the active data generation, the owner of data is willingly providing data to the third party while in the passive the data owner is not aware that the data is being accessed by the third party.

Privacy is actually the protection of data from being exposed to the public network. The privacy of personal data is the most concerning aspect which should be achieved. The privacy should focus on the usage of the data rather than a collection of data. Because if the data is not kept secured then it causes many threats. So for that, it should be modified according to the size of data as well as the unexpected use of it. To keep all the personal data and sensitive data private there are many anonymization techniques that help in the preservation of privacy [1]. The main goal of anonymization is actually to perform some masking operations on the data to protect the privacy of the individual with the insurance that it remains useful for researchers. The data contains the information related to the individual, organization, etc. The data contains three types of attributes which are as follows [2]:

Identifiers: These are the attributes that uniquely identify the individual e.g. Person name, CNIC number.

Quasi Identifiers*:* Quasi Identifier (QI) are the attributes that are already known by everyone and when they are taken together they can identify the individual e.g. Date of birth, Zip code, Gender.

Sensitive Attributes: These are the attributes that are not known to anyone and they contain sensitive information about the individual e.g. Salary of Person. They are unknown to the third party. The table below shows examples of these attributes.

TABLE 1. TABLE OF ATTRIBUTES

Name	Gender	Age	Education
Salma	Female	43	PhD
Ali	Male	23	BSc.
Saleem	Male	20	BA
Hafsa	Female	17	FSc
Alina	Female	25	MBA
Afia	Female	23	M.Phil.

Table I shows the example of different types of attributes in data. The Name is the Identifier, Gender and age are Quasi-identifiers and Education is the sensitive attribute.

The information which is disclosed is of various types that are Identity disclosure, Membership disclosure, and Attribute Disclosure. The Identity disclosure is when a particular record that is released has linkage with an individual. Membership Disclosure is when the data which is to be published is extracted out from a large data which is sensitive. It is prevented from the third party from learning that the individual's data is present in the data or not. Attribute disclosure is when the individual's new information is disclosed. The data which is revealed makes it easy to know the characteristics of the individual. These types of information are disclosed when the data publisher publishes the data, therefore all this information needs to be secured.

Big data include Vs (Velocity, Volume, Veracity, and Variety) that are equally important when analyzing the big data. The big data is based on the V-based characterization which has the main motivation of highlighting serious challenges i.e. storage, analysis, cleaning, etc [2]. Figure I shows the Vs of Big Data. The organization collects a variety of data from different data sources so that it is in large volume. This data is streamed at different speeds and they are of different kinds and formats. Storage of these datasets is challenging for the traditional database. So with this reason around big data is stored and shared on the web which requires high security to keep that data private and protected from any harm or loss [3].

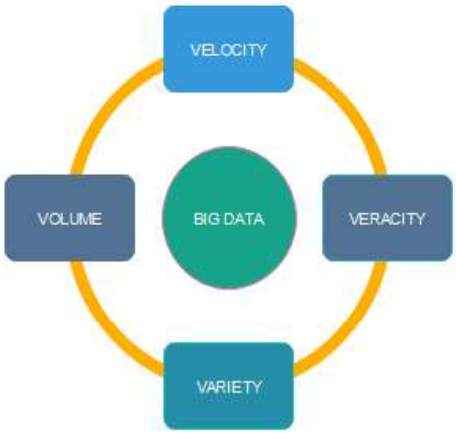

Figure 1: Big Data

A. Types regarding Information disclosure

There are basically two sorts of information disclosure that are Identity disclosure and Attribute disclosure. Identity disclosure is when an individual can be distinguished from the data being published. And Attribute disclosure is when the new information about any of the individual is released [4]. Identity disclosure allows the Attribute disclosure. K-anonymity is a technique that is meant to be a major backbone that helps in the protection of privacy to the data. These techniques also prevent Identity and Attribute disclosure.

B. Preservation of Privacy of Big Data

Big data benefits the industrial as well as research areas. The data nowadays is of different types and huge in volume. Big data have features such as structured, unstructured, semi-structured and heterogeneous [5]. Data generated from different social networks, the Internet, medical application and other sources is the big data that is huge and complex. This huge amount of data needs a way that can preserve the privacy of all the data [6]. Big data privacy is gaining concern as the amount of data is gradually increasing. With this huge amount of data, it is also important to preserve its privacy in the most efficient and reliable way [7]. The usage of data shall be focused rather than only the collection of the data.

Data should be protected before it is published. Unprotected data reveals sensitive attributes as well as identity information [1]. The major challenge is to protect the data from the third party which is in keen on collecting that data. Failure in keeping privacy leads to harm to the data and the individual's personal information.

C. Anonymization of data

Anonymization of data aims at maximizing the benefit by minimizing the individual risk. Anonymization is actually an approach in which the changes are performed on the data in such a way that the sensitive data and the identity of the individual are kept private and secure [8]. Different techniques are used for the anonymization of data that can hide the private data. It is the most important task to hide the identifier attribute. The identification of the key information is protected when anonymization is performed on data. Some details in the data are confidential which needs to be hidden from the third party and all the threats [4]. Data anonymization declares all the information that is used for queries as well as analysis while it maintains the sensitive data to be kept private Demand of Anonymization of data is because of the increasing occurrences of misuse of personal data and privacy issues [8]. Big data privacy is a domain that cannot be neglected at any stage.

The rest of the paper is arranged as follows.

Section II describes different anonymization techniques proposed previously. Moving on to Section III that is the Literature review. Section IV discuss the problem statement of

the selected topic. The proposed solution is described in Section V. The result discussion is presented in Section VI. Finally, Section VII summarizes the paper.

1.2 ANONYMIZATION TECHNIQUES

For keeping the data privacy different anonymization techniques are carried out to anonymize the data. The following techniques are used for anonymization and the table below shows data:

TABLE 2. EXAMPLE DATA

Gender	Age	Height	Education
Male	24	5.2	MSCS
Female	21	5.4	BIT
Female	23	5.6	M.Phil. CS
Male	25	5.9	MBA

D. Suppression

Suppression is one of the anonymization technique in which an entire tuple or the attribute value is removed. The tupling is neglected. In the procedure basically, the original data is replaced by some special characters e.g. with (*) in the replacement of the data which is to be kept hidden [9]. The steric represents the data that is not supposed to be disclosed.
This helps the data to be private and preserve from the third party to be known. The suppression technique on the sample data is presented as follows:

TABLE 3. SUPPRESSION

Gender	Age	Height	Education
Male	*	5.2	MSCS
Female	*	5.4	BIT
Female	*	5.6	M.Phil. CS
Male	*	5.9	MBA

E. Generalization

One other anonymization technique is known as Generalization. It can be said as Recoding. In this method, the value of an attribute is replaced by semantically consistent values, but that value is fewer specific ones [10]. Generalization replaces the exact value with some generalized one so that the details of that attribute are mot identifiable. The exact values are changed into a general range of data. The attribute value is generalized so with the help of this technique the third party cannot see the exact value which makes it complex to guess the exact value against something [9]. An example of generalization is as follow:

TABLE 4. GENERALIZATION

Gender	Age	Height	Education
Male	24	[5.2-5.4]	MSCS
Female	21	[5.2-5.4]	BIT
Female	23	[5.6-5.9]	M.Phil. CS
Male	25	[5.6-5.9]	MBA

F. Bucketization

Bucketization is similar to Generalization but the Quasi Identifiers or sensitive attributes are not modified. It divides the records of data into partitions and each partition is given an id which is known as GID. The tuples in the partition have the same value of GID. After that Quasi Identifier Table and Sensitive Table are made. The data which is anonymized have set of buckets that have values of permuted sensitive attributes. The grouping which is made by bucketization is the same as grouping which is made in generalization.

Bucketization has all original values of tuple, while the generalization has generalized values of tuple. The technique of

bucketization work for the anonymization of data with high dimensions [9]. It provides much better utility, unlike generalization. But this technique don't stop the membership

disclosure because values of Quasi Identifier are published in their original form so that is why it is easy to find the record of the individual. Sensitive attribute and Quasi Identifier need separation and it breaks down the correlation between them. The bucketization of the sample data given in Table 1 is as follows:

TABLE 5. QUASI IDENTIFIER

Gender		Age	GID
Female		43	1
Male		23	2
Male		20	3
Female		17	4
Female		25	5
Female		23	6

Table 5 shows the Quasi Identifier where the Gender and Age are Quasi Identifiers and it is assigned GID. Now Table VI shows the Sensitive Attribute Table where Education is the sensitive attribute and they are also assigned GID.

TABLE 6. SENSITIVE ATTRIBUTE

GID	Education
1	PhD
2	BSc.
3	BA
4	FSc
5	MBA
6	M.Phil.

G. Slicing

This technique works on the flaws of the Generalization. Slicing works on data set in two different ways, i.e. vertical portioning of the dataset and horizontal portioning of the dataset [10]. In the vertical partitioning of the dataset, the dataset is grouped in a way that the attributes that are extremely correlated with each other are grouped into one column. Whereas in the horizontal partitioning the dataset is grouped in a way that the tuples are portioned into buckets. In each bucket, the value against each column is sorted for breaking the linkage between the different columns. Every bucket contains a subset of different tuples in it. Each tuple has multiple matching.

Moreover, it provides better utility for the preservation of privacy. Slicing techniques slice the big data so that infrequent attributes break the collaboration among them [11]. This technique reduces the dimensionality of data. Slicing technique works efficiently on big data privacy preservation because it breaks association among the uncorrelated attributes.

The slicing is implemented on the sample data taken. The following example shows the horizontal slicing and vertical slicing is given below:

TABLE 7. SLICING

Gender, Education	Age, Height
Female, BIT	21, 5.4
Male, MSCS	24,5.2
Female, M.Phil. CS	23,5.6
Male, MBA	25, 5.9

These described techniques are kind of anonymization that work on the data for securing it [12]. In big data, anonymization techniques become less effective. It needs to be more than the covering of data as well as generalizing it.

2. LITERATURE REVIEW

For the preservation of the privacy of big data different research has been done previously. In [12] Tiancheng Li, Ninghui Li, Senior Member, IEEE, Jian Zhang, Member, IEEE,

and Ian Molloy introduced a method of Slicing for the Preservation of Privacy. The experiments in this paper show that slicing is an approach better than bucketization and it prevents the disclosure of membership. Later in [1] an efficient approach for privacy preservation of data mining was done that included the use of combined techniques of randomization and anonymization [13]. The proposed technique in this paper protects the sensitive data with less information loss which prevent various types of attack. Later in 2015 Tomislav Krizan, Marko Brakus, Davorin Vukelic came up with in-situ anonymization of big data. A software description is given for the in-suit anonymization of big data which is distributed in cluster form [14]. Moreover, major anonymization techniques were discussed in this paper that includes randomization, generalization. Further, in 2017 Abid Mehmood, Iynkaran Natgunanathan Yong Xiang, Song Guo, Senior Member, IEEE, Guang Hua, Member, IEEE have discussed the anonymization technique that provided privacy to the data which include Generalization, Suppression, Anatomization, Permutation, Perturbation. Later in [3] Nivedita Elanshekhar and Rajashree Shedge gave a solution that uses the Suppression Slicing method. In this paper, this approach was performed on the attributes which have similar values for better privacy and for better utility. The method follows the procedure that the data goes under the MapReduce method and then suppression slicing is implemented. Furthermore, in [15] Brijesh B. Mehta and Udai Pratap Rao used the scalable k-anonymization approach using the MapReduce technique for the privacy preservation of big data. In this paper, an algorithm named as k anonymization using MapReduce was introduced for the privacy preservation of big data publishing. This approach was compared with the existing approaches. In 2018 an approach was proposed which was a scalable approach for big data multidimensional anonymization which was based on the MapReduce.The idea was actually to partition the data set into small data sets using the MapReduce method. Then in [16] the same year 2018 an enhanced privacy preservation auction scheme was used that included an additional verification mechanism.

3. Problem Statement

Conserving the anonymization of big data sets is an important deal to be dealt with. When the data is anonymized, it means that all personal data is eliminated. In the era of big data, the data anonymization techniques tend to fail because of the thousands of data points for the individual. These simple techniques don't fully perform efficiently like up to the mark in preventing from the disclosure of identity. Suppression is easy to implement but the data quality is reduced drastically. Generalization fails when it comes to high dimensional data because of multiple dimensions and the data tends to lose much information [7]. Moreover, big data have a linkage of information that needs to be removed. Data anonymization needs to be much more than just masking the data and generalization of it. The existing models are lacking in managing large datasets. These techniques alone cannot preserve the privacy of the big data, Data anonymization techniques need to be improved in a way that it focuses on the 3Vs of big data i.e. Volume, Velocity, and Variety [1]. It should become more efficient so they can make a positive effect on keeping the big data protected from any loss or attack. There is a need for a new technique that carefully analyzes that the anonymized data is exposed to any harm or not.

4. Proposed Solution

Increasing the growth of data needs a solution that can provide preservation of the privacy of this big data. Many solutions have been implemented to keep the data private but

when it comes to big data privacy those were unable to perform better [14]. The proposed solution in this paper carries three techniques which all together can work in a way that can provide the data privacy to be kept preserve from the third party and hackers. Figure II below shows the steps that are involved in the proposed solution followed by the explanation of these steps:

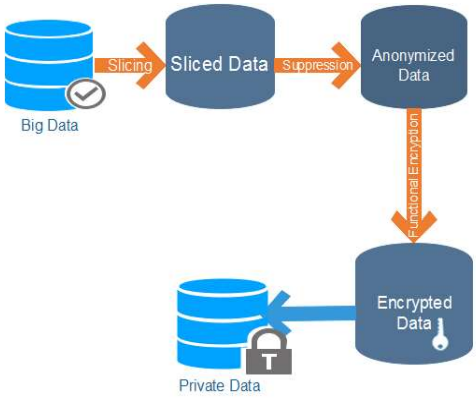

Figure2 : Proposed Solution

4.1 Implementing Slicing on Data

Firstly, the slicing is implemented on the big data where the data is portioned both horizontally and vertically with the preceding procedure as it is discussed before in Section II. Implementing this technique have many advantages that assist in the preservation of the privacy of big data. The technique of slicing provides big data with privacy as it preserves the data utility as compared to the techniques of generalization and also provides the disclosure of attributes. Each tuple in the slicing has more than one matching within so that is why the slicing helped in keeping the privacy of big data [10]. With the help of the slicing of data, the data dimensionality is reduced. The correlation between the attributes is kept maintained. Moreover, it groups the attributes that have much correlation between them.

4.2 Implement Suppression

Secondly, after the data is sliced both vertically and horizontally the sliced data now undergo suppression where the data is kept hidden by replacing the sensitive attribute or sensitive tuple with (*). This helps the confidential attributes to be hidden from the hackers. It will make the data complex to be known. The hackers have to apply guesses in order to know the original data which is hidden under the steric.

4.3 Implement Functional Encryption

4.3.1 Encryption:

Encryption is actually a process that involves encoding some information or any message in a way that the information is only accessed by the authorized parties and no other can access it. It is simply to mystify the information so that it is hidden from the unauthorized parties which have complete or any partial access over the information[19]. The message which has to undergo the encryption is called the plain text and when it is encrypted it is called ciphertext. The ciphertext can only be changed into the plaintext by using the decryption process [15]. For the purpose of encryption and decryption, it makes use of a key that is known only to the sender and the receiver. Encryption helps the data to be hidden from the third party or any attack. The encryption scheme makes use of the encryption key which is generated with an algorithm [20-22]. The key is shared with both the communication parties at both the end i.e receiver end and sender end. For the encryption of data, many different encryption techniques are used. But when it comes to the encryption of big data, which is in huge volume the traditional encryption schemes fail to perform efficiently on it.

4.3.2 Functional Encryption:

Functional Encryption is a type of encryption that works on big data. Functional

Encryption is a type of encryption that helps to keep the privacy of the big data preserve. The traditional encryption techniques only help to encrypt the limited amount of data [17]. When it comes to encrypting the big data, those techniques don't perform up to the mark. But the functional encryption helps to perform better when it comes to big data. Functional Encryption is a type of public-key cryptography It doesn't encrypt any other function than that specific one. This type of encryption differs from the traditional ones in a way that the generated ciphertext of the provided plain text is only decrypted by a specific recipient. While in the functional encryption the group of people can encrypt the message without knowing anyone [18]. Moreover, the traditional encryption encrypted all the data or nothing while in this selected data can be encrypted.

The pictorial representation of functional encryption is shown in Figure III. The technique of functional encryption lets the user to only know any specific functionality without knowing what the rest of the data contains [17].

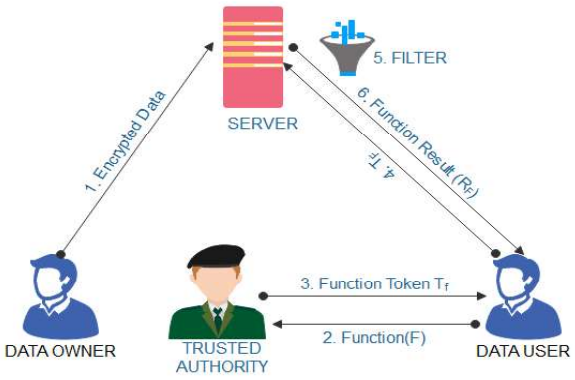

Figure 3: Functional Encryption

In figure III the encrypted data is sent from the data owner to the server. The data user passes the function F to the trusted authority which in return sends the function token to the data owner. The function token is represented by the T_F. The token function is sent from the data owner to the server. As a result, the server filters out important things or needed information. The filter helps in a way that the whole data is not known to the data user. Only a part of a function is known to the data user. The server after filtering send the function result to the data used so that the person can use that data.

The following box shows the proposed solution algorithm:

These steps of algorithm are carried out step by step on the big data so that it can be preserved and kept private. First, the data is received in slicing function where it is sliced both vertically and horizontally. Then the sliced data is received to the suppression function where the data is suppressed with the steric. In the end, it goes to functional encryption function whether a particular function or whole data is encrypted according to the demand of the user.

In functional encryption function, the pair of master key and public key is generated. Then a secret key (sk) for the value of k with the help of the master secret key using the key generator is generated. After that encrypts the message (m) with the help of the public key. Then the secret key (sk) is used to compute the function F (k, m) from c.

The secret key holds the specification of only

PROPOSED SOLUTION ALGORITHM:

Slicing Function (data)
1: Data Extracted from Database.

2: Anonymity performed to divide the record into two.

3: The sensitive values interchange.

4: Multiple set of values are displayed.

5: Correlation of Attributes and secure data is displayed.
Function End

Suppression Function (data)
6: Sliced Data as input

7: Data replaced by (*)
Function End

Functional Encryption Function (data)
8: (Public key, master secret key) ← SetUp (1^{λ})

9: Secret key ← Keygen (master secret key, k)

10: Ciphertext(c) ← Encryption (public key, message)

11: F (k, m) ← Decryption (SK, c)
Function End

decrypt specific functionality and restricts the decrypting of other data. Encryption and Decryption functions are used to take the input and perform encryption and decryption.

The following Figure IV shows the functional encryption in summarized form.

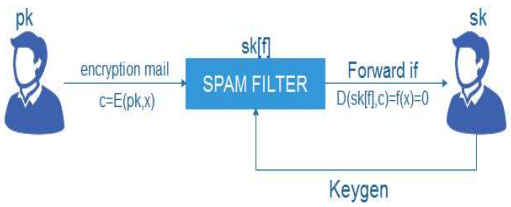

Figure 4: Functional Encryption Summarized

The functional encryption includes four algorithms that include Setup, Encryption, Decryption, and Keygen. The Setup algorithm output the master key. In the Keygen algorithm, the master key is taken as input and also some of the description related to function. Taking them as input the algorithm outputs a key that is only specific to the function which is denoted by the sk[f]. After the data undergo suppression by masking the tuples or attributes with a steric the data is passed through this functional encryption where the big data is encrypted and only a part of ciphertext is revealed to the user. Users cannot know nothing except that portion that is revealed. This helps in keeping the big data privacy to be preserve. With this feature of functional encryption along with anonymization techniques help the data privacy to preserve much better.

This proposed method which is discussed above can help in preventing hackers to hack the data and also from the third party to keep the big data anonymous. Moreover, it can work on big data which the other techniques fail to perform up to mark. Previously only the anonymization techniques were implemented for privacy reasons. But this solution can provide improved and better results and also in an efficient way.

5. Result Discussion

The proposed solution has been implemented on the big data, can result in a better privacy preservation. The data first is portioned in the vertical form or horizontal form. It assembles the attributes having a correlation with each other. Then the data is suppressed by hiding confidential attributes or tuples. After that, the functional encryption is applied that encrypts the function that is to be kept private with the help of the key. All the data is not encrypted but only a specific portion is hidden from the hackers. This all procedure result is privacy that is complex to be harmed and in each step of the big data lifecycle, it can preserve privacy. This proposed solution can perform

better than the traditional anonymization alone can perform and can be automated with the increasing (volume, velocity, and volume) in the big data.

6. CONCLUSION

Big data is growing every day and it contains private information which needs to be preserved. It is a term that is used for the data which is complex and of huge volume. It is used in the analysis and for decision purposes. At every stage of the big data life cycle, it requires high privacy. So, privacy is a major concern that needs to be focused. Privacy is a factor that needs not to be compromised because the disclosure of private information leads to harm of data and threats. For the privacy of this big data, the anonymization techniques were being used that include generalization suppression, etc. The technique of generalization or suppression alone was not able to handle when it comes to big data that is also the high dimensional data. One of the anonymization techniques is the slicing which is best for big data as it provides the portioning. Applying suppression and functional encryption it can give results up to the mark. If functional encryption is implemented properly then it can reduce the privacy challenges that big data may face. The preservation of the privacy of big data is a major emerging field that cannot be ignored because with the gradual increase in data it is becoming more complex.

REFERENCES

[1] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, "Protection of Big Data Privacy," *IEEE Access,* vol. 4, pp. 1821-1834, 2016.

[2] M. Dave and J. Kamal, "Identifying big data dimensions and structure," in *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, Solan, India, 2018.

[3] N. Elanshekhar and R. Shedge, "An effective anonymization technique of big data using suppression slicing method," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, 2017.

[4] P. C. Kaur, T. Ghorpade and V. Mane, "Analysis of data security by using anonymization techniques," in *2016 6th International Conference - Cloud System and Big Data Engineering (Confluence)*, Noida, India, 2016.

[5] M. D. A. Praveena and B. Bharathi, "A survey paper on big data analytics," in *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, India, 2017.

[6] S. Singh and N. Singh, "Big Data analytics," in *2012 International Conference on Communication, Information & Computing Technology (ICCICT)*, Mumbai, India, 2012.

[7] Q. Tan and F. Pivot, "Big Data Privacy: Changing Perception of Privacy," in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, Chengdu, China, 2015.

[8] A. Kumar, M. Gyanchandani and P. Jain, "A comparative review of privacy preservation techniques in data publishing," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2018.

[9] T. Karle and D. Vora, "PRIVACY preservation in big data using anonymization techniques," in *2017 International Conference on Data Management, Analytics and Innovation (ICDMAI)*, Pune, India, 2017.

[10] P. Goswami and S. Madan, "Privacy preserving data publishing and data anonymization approaches: A review," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, Greater Noida, India, 2017.

[11] P. C. Kaur, T. Ghorpade and V. Mane, "Analysis of data security by using anonymization techniques," in *2016 6th International Conference - Cloud System and Big Data Engineering (Confluence)*, Noida, India, 2016.

[12] T. Li, N. Li, J. Zhang and I. Molloy, "Slicing: A New Approach for Privacy Preserving Data Publishing," *IEEE Transactions on Knowledge and Data Engineering ,* vol. Volume 24, no. Issue 3, pp. 561 - 574, 2010.

[13] M. Sharma, A. Chaudhary, M. Mathuria, S. Chaudhary and S. Kumar, "An efficient approach for privacy preserving in data mining," in *2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014)*, Ajmer, India, 2014.

[14] T. Križan, M. Brakus and D. Vukelić, "In-situ anonymization of big data," in *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2015.

[15] B. a. U.P.Rao, "Privacy preserving big data publishing: a scalablek-anonymization approach using MapReduce," *IET Software,* vol. 11, no. 5, pp. 271-276, 2017.

[16] W. F. W. a. C. W.Gao, "Privacy-Preserving Auction for Big Data Trading Using Homomorphic Encryption," in *IEEE Transactions on Network Science and Engineering*, 2018.

[17] K.Takashima, "Recent Topics on Practical Functional Encryption," in *Second International Symposium on Computing and Networking*, Shizuoka,Japan, 2014.

[18] A. Boneh, "Functional Encryption:A New Vision for Public Cryptography," vol. 55, pp. 56-64.

[21] P. S. a. D. K. Kaur, "Database Security Using Encryption," in *015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*, Noida, India, 2015.

[22] C. Matt and U. Maurer, "A Definitional Framework for Functional Encryption," in *2015 IEEE 28th Computer Security Foundations Symposium*, Verona, Italy, 2015.