*International Journal of Engineering & Technology*, 7 (2.7) (2018) 825-833

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research Paper***

# Route Map of Privacy Preservation to IOT

**Mr. Pravin N. Kathavate [1]*, Dr. J. Amudhavel [2]**

*[1] Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation*
*[2] Research Supervisor, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation*
**Corresponding author E-mail: pravin.kathavate@gmail.com*

## Abstract

Data anonymization is the main feature of privacy preservation, and it assists in eradicating the privacy hazard in data preparation in various applications including IoT. Pseudonymity and Anonymization are two significant security factors that were adopted when sensitive data are shared. In medical field, data is usually distributed horizontally with diverse regions carrying a similar set of characteristics for various anonymization techniques. Accordingly, this paper intends to formulate a review on privacy preservation in IoT. Here, the literature analyses on diverse techniques associated with data hiding, data preservation and data anonymization along with data restoration properties. It reviews 60 research papers and states the significant analysis. Initially, the analysis depicts the chronological review of the overall contribution of different types of anonymization protocols in diverse applications. Subsequently, the analysis also focuses on various features such as applications, measures, key generation and data preservation in healthcare, etc. Furthermore, this paper provides the detailed performance study regarding data hiding and restoration process in each contribution. Finally, it extends the various research issues which can be useful for the researchers to accomplish further research on data preservation in IoT.

***Keywords***: *IoT, Privacy preservation, Data hiding, Data Restoration, Performance measures*

**Nomen Clature**

| Acronym | Explanation |
|---|---|
| IoT | Internet of Things |
| RFID | Radio Frequency Identification |
| CR | Cloud Requester/Users |
| DBSCAN | Density Based Spatial Clustering of Applications with Noise |
| CABAC | Context-adaptive Binary Arithmetic Coding |
| RDH | Reversible Data Hiding |
| BBE | Binary-Block Embedding |
| PPVG | Pixel-Based Pixel Value Grouping |
| ACS | Ant Colony System |
| N-T-G | Not To be Generated |
| F-T-H | Fail To be Hidden |
| N-T-H | Not To be Hidden |
| GDP | Geometric Data Perturbation |
| P2Q | privacy-preserving query |
| SISO | Single Input Single Output |
| RDH-EI RDH | in Encrypted Images |
| MIMO-OFDM | MIMO-Frequency-Division Multiplexing |
| ROI | Region Of Interest |
| RONI | Region of Non-Interest |
| DWT | Discrete Wavelet Transform |
| DCT | Discrete Cosine Transform |
| EIRDH-P | Encrypted Image-based RDH with Public key cryptography |
| CELS | Collaborative Search Log Sanitization |
| MSE | Mean Square Error |
| SMC | Secure Multi-party Computing |
| TDS | Top-Down Specialization |
| PCA | Principal Component Analysis |
| SSIM | Structural Similarity Index Measure |
| FFT | Fast Fourier Transform |
| TPR | True Positive Rate |
| FPR | False Positive Rate |
| Acc | Accuracy |
| K-A | k-anonymity |
| IL | Execution Information Loss |
| ER | Embedding Rate |
| PSNR | Peak-Signal-to-Noise Ratio |
| QF | Quality Factor |
| Eff | Efficiency |
| Util | Utility |
| Cost | Computational Cost |
| RE | Error Rate |
| GRA | Greedy Algorithm |
| MA | Multi Agent |
| MPC | Multi Party Clustering |

## 1. Introduction

IoT concept has quickly progressed in the previous years in the internet as a group of formulations, intelligent, and objects that are organized in a global and dynamic framework [61] [62]. Objects denote to distinctively smart tools which are usually scattered with actuation and sensing potential and capable of handling partial calculations such as memory, network and CPU capabilities [63] [64]. It can be referred as the summation of numerous communication and technologies solutions like sensors and actuators, and RFID technology [65]. The fundamental idea is the existence of smart devices that are able to monitor, learn, and manage the surroundings [66]. It moreover has the capability to have a significant role in work and home circumstances, like smart home, assisted living and e-health, office, and smart transportation [67]. For example, in medical appliances, small equipments are employed to detain health information like heart rate and blood pressure [68]

**Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.**

[69]. The composed information are subsequently conveyed to doctors for medical recommendation and can be made tenuously applicable to specialist for study. An additional innovative development of IoT application is the smart cities that targets to introduce an effective collaboration and interaction platform utilizing different resources for transforming the cities smarter [70]. Regardless of the current progress in the direction of making IoT an actuality, there prevail numerous open problems that need further development and research efforts for utilizing its entire potential. One of this limitation denotes to the amount of energy utilized at streaming details generated by a huge amount of resource inhibited interrelated strategy that should be processed and offered in a well-organized variety. With the speedy growth of internet and computer knowledge, multimedia data can be exchanged, accessed and copied on the internet at anywhere and anytime [61].

In the meantime, this further makes multimedia data passed on over threat [73] [74]. Hence, the way to convey multimedia data securely has been a demanding problem in the information protection field, and the major protection move towards fingerprinting, encryption, and hiding data [79], which have been extensively studied [62] [71]. Along with them, data hiding is a method that could hide data in an unnoticeable way into multimedia data for content authentication, copyright protection and secret interactions [72]. Data hiding has two associated disciplines, namely, forensics and steganalysis [75]. Conventional data hiding methods typically establish irreversible alteration to multimedia data [76] and hence, they cannot be deployed in certain applications necessitating any stable alteration to the real cover image, such as military and medical image processing [62] [77] [78] [80]. Private information has to be kept private, but privacy conservation is not equivalent to privacy [81]. A huge quantity of data from diverse sources is collected and processed, the IoT process may have an important impact on the privacy of users' [82]. In addition, focusing the extending trend on gathering extra personalized and individual data in IoT, there exists a lot of exertions concerning the impact on privacy of the individuals' from an authorized perspective [83]. The data managing or processing of IoT is significantly impacted by position information and consecutively affects its position privacy [84]. As location information is a foremost constituent in efficient inventory and supply chains, effective context-aware mobile applications, transportation systems, and other numerous IoT systems, harmful consequences and privacy attacks can take place when responsive location information is exposed exclusive of users' approval [85] [86]. This masquerade limitations on IoT privacy and security like head crash, data loss, and power failure, etc. [87] [88]. A huge number of methods have been implemented to represent the privacy conservation problem in location-based services. Some of them are dependent on the cloaking method that utilizes the k-anonymity design to secure user's location privacy [89]. Even though numerous methods are emerging for preserving privacy, it still exists as confront owing to inappropriate privacy concerns on IoT. Therefore, proper study on IoT is necessary that dependent on privacy concerns [90].

This paper contributes a review related to privacy preservation algorithms for promoting secure IoT. As there are few contributions on privacy preservation in IoT, the survey focuses on privacy preservation algorithms in diverse applications that can assist IoT application. Here, the applications, measures, key generation and healthcare applications are focused in this survey. This paper is organized as follows. Section II depicts the related works and reviews done under this topic. Section III discusses the performance study on privacy preservation of data and section IV provides research, gaps and challenges and section V concludes the paper.

## 2. Privacy Preservation of Data

### A. State-of-the-art of contributions

In 2017, A. K. Ilavarasi and B. Sathiyabhama [1] presented a privacy design that implanted the anonymization process into a learning algorithm, which alleviated the extra facors that were given to tasks of data mining. It was revealed that categorization precision attained for the majority datasets performs the outcomes acquired with unique dataset. Peipei Sui and Xianxian Li [2] developed a privacy security scheme on the combination of trajectory data and transaction data. It first exhibited a privacy leakage representation occurred by a combination of multimodal datasets, in which integrated data were designed as a tree. At last, experiments were performed on datasets with two synthetic data integration and analyze information and privacy loss under changing factors. Dhasarathan et al. [3] presented the secure design to avoid loss of data in the Cloud. This assisted the CR to believe their data and individual details saved in the cloud. Kim et al. [4] proposed a model for a secure anonymization methods and EMR data cube that was required to attain data privacy. A variety of secure EMR data cubes are evaluated by means of numerous realistic metrics and examined the functioning of all schemes with contemplation for analysis of EMR surroundings. Feng et al. [5] suggested a steganalytic system to identify newly produced content-adaptive binary image data hiding by utilizing the embedding consequence related with the shape pattern-dependent embedding principle. Experimental outcomes have shown that, in spite of the low dimensionality, the implemented steganalytic characteristics can efficiently identify conventional binary image data hiding methods, particularly those pattern-tracing-based techniques. Weng et al. [6] have proposed a two-stage embedding so as to certify the execution of full-enclosed-based calculation. As a substitute of treating individually two stages like in conventional process were treated together to optimize the assortment of embedding bins at a specified embedding capacity. In this manner, the optimal embedding bins can attain highest visual quality. Chen et al. [7] presented a technique for definite data clustering by means of rough entropy technique with DBSCAN clustering technique to develop presentation of k-anonymization technique. Simulation outcomes demonstrated that the suggested algorithm could be further efficient to adjust the effectiveness of computation of anonymization and the mobile social network data. Nan-IWua and Min-Shiang Hwang [8] presented a scheme in which secret position matrix was considered to develop the hiding capability that has the ability for avoiding the slightest alteration depending on the combination hypothesis. The new method has allowed the users to cover more than one bit of secret data by varying at least one pixel in each sub-image. Xu et al. [9] implemented an enhanced method of hiding data in H.264/AVC videos that were partially encrypted by means of CABAC substitution. The encryption of Luma forecast approach was considered besides the encryption that are residual and motion vector encryption so as to develop the structural declining considerably. Experimental results have confirmed that the implemented method can attain improved scrambling presentation and higher embedding capability. Chang et al. [10] have introduced a divisible RDH system for JPEG bit streams that were encrypted. The implemented method was created by means of a alloted room before encoding approach, i.e., real JPEG bitstream was customized with little interruption with the intention by which the content proprietor can preserve sufficient location for upcoming data embedding and after that, the customized JPEG bitstream was encoded. At last, the receiver attained the capability to extract the data that were embedded and recuperated the original JPEG bit stream separately. Agarwal [11] introduced a new RDH method for encoded images. For encryption operation, iimplemented method exploited additive modulo 256 and possessions of average for watermark embedding in the images that are encrypted. Investigational results, on a variety of

benchmark grayscale test descriptions, and evaluation with currently implemented conventional methods demonstrated the dominance of the implemented technique regarding privacy, reversibility, security, computational efficiency and protection. Chung et al. [12] introduced RDH scheme, an intellectual switching scheme to choose the spatial correlation-dependent or the temporal calculation method to exploit the quality development of the marked mosaic videos for fixed embedding capability. The implemented RDH process evidently outperformed the spatial correlation- dependent RDH process. ShuangYi and Yicong Zhou [13] have presented a BBE process for incorporating privacy data in a image that is binary. By means of BBE, an algorithm for RDH. In Encrypted Images BBE-RDHEI was proposed. Comparisons and experiments illustrated that this method has an rate of embedding which was almost double times proportioned than the conventional algorithms. Wenguang He et al. [14] suggested a PPVG through the primitive of embedding varies from block to block pixel and it is filled on pixels to estimate the expected range. Investigational results validated that the implemented method executes better than other conventional techniques. Tai Wu et al. [37] proposed an ACS-dependent technique described as ACS2DT to reduce the influences and improve the presentation of the sanitization method. The results from experiments demonstrated that the implemented ACS2DT technique is better than the GRA and two evolutionary techniques with respective to N-T-G, F-T-H, Database Similarity DS execution time and N-T-H, on both synthetic datasets and real-world. Nayahi [53] suggested an anonymization method depending on clustering and flexible to possible attacks. Experimentation results demonstrate that the F-Measure, accuracy and the execution time on the secure data sets of the classification algorithms created by the implemented clustering techniques are improved than the conventional algorithms. Soohyung Kima and Yon Dohn Chung [54] implemented a novel procedure for the privacy-preserving data collection. Contrast to availing works, this protocol does not limit the kinds of anonymization method and does not necessitate the private channel. Throughout the experiments, the performance of the implemented protocol was revealed.

In 2016, Upadhyay et al. [15] implemented a GDP technique by means of three-dimensional rotations and data partitioning. The experimental estimation demonstrates that the implemented method offered good privacy protection results and data exploitation when compared to the conventional techniques. Yan Li et al. [16] have proposed two distributed secure techniques dependent on a circulated approach. The fundamental concept of this technique was to construct an better design for all combining ability to precisely study the distribution of data. Also, it was revealed that the significant biomarkers, both region-specific and universal and authorized the particular biomarkers by means of the biomedical novel. Wimmer et al. [17] have implemented a MA design along with P2Q methods to guide the sharing of data when maintaining security. Outcomes specify that this flaw was able to overcome the discussed confronts, thus aiding the data sharing for information discovery in applications related to healthcare. Sadhya [18] have presented a security-preserving structure for biometric dependent models by exploiting the common concept of various privacies. Therefore the implemented architecture offers security for biometric users devoid of negotiating its whole performance. Komishani et al. [19] proposed PPTD, a novel technique for maintaining privacy in trajectory data publishing dependent on the theory of modified privacy. The research on both the trajectory datasets proposes that this technique were efficient for maintaining personalized privacy in trajectory data publishing. Jiang et al. [20] presented a better computation and P2Q method over encoded data in big metering to concentrate on this confront.

The estimation reveals that the P2Q method can considerably decrease the response time and offer high exploring effectiveness devoid of negotiating on exploration quality. Marwan et al. [21] suggested an inclusive investigation among the DNA-dependent vigenere, play fair, AES ciphers and the RSA, all joined with a DNA screening method. Investigational studies authenticate such excellent performance in contrast with the entire examined combined methods. Qian et al. [22] suggested an enhanced process of RDH-EI. Three parties comprised the implemented system: the remote server, the image owner, and the recipient. Experimental results demonstrated that the implemented method attains a larger payload when compared with the associated works. Chen et al. [23] implemented a hiding equation for the MIMO-OFDM technique and confirmed it by experimental and analysis. After that, the outcome of the OFDM factors, guard interval and FFT length on the hiding capability of data computation was examined. According to the results of experimentation, in the similar circumstances, the accuracy of secret data, BER of carrier data and data hiding capability in the MIMO-OFDM system were superior to those in the OFDM, SISO and MIMO coding channel schemes. Jafar et al. [24] introduced RDH techniques that are dependent on this conception. Efficiently, extraction and data embedding in this techniques are executed in three phases. In addition, this algorithm was of low complexity while computing and do not necessitate interaction of more information. Liu et al. [25] proposed a novel ROI-dependent RDH method in medical images that are encoded. Initially, a owner of content separated a real image into the ROI and the RONI, after that, it encodes the image by means of a key for encryption. Ramalingam [26] presented DWT and DCT coefficients to improve the safety of hidden data and reduces alterations to preserve enhanced quality of video. The results obtained from comparison reveals that the implemented process presents enhanced privacy and reduces interruptions for improved video quality. Jafar et al. [27] suggested a Sharpening-Aware RDH techniques which have the ability to embed certain quantity of data along with improving the image. Investigational outcomes established the capability of SARDH technique in big payload embedding and offering enhanced stego images. Lei Xu et al. [38] presented a paper where the objective was to protect information from unauthorized enclosure when managing data's value. The results of simulation mainly coincided with perception which proved that the game-theoretical investigation was valid. F.Nettleton and JulianSalas [55] presented a complicated synthetic data producer mutually with an anonymization processor with firm secure assurances that considers the neighborhood which is local when anonymizing. Experiments demonstrated the reliability of the process and the development with reduced information loss regarding techniques that fail to consider the context of local neighborhood during anonymizing.

In 2015, M.Prakash and G.Singaravel [28] proposed a personalized anonymization technique that maintains the privacy when the responsive data was available. It also demonstrated that this method achieves better performance over the distinct probabilistic k-diversity measure, l-diversity measure, and k-anonymity with the k-closeness measure. UnilYun and JiwonKim [29] have suggested a fast perturbation technique depending on a tree structure that executes the procedure of database perturbation more rapidly for avoiding responsive information from uncovering. The implemented algorithm promises improved scalability than the most recent ones regarding databases with the features of steadily increasing transactions and attributes. Kokkinos [30] proposed a security-preserving mining of data in huge decentralized positions of data that can construct numerous neural networks for group formation. Experimental model on comparisons and benchmark datasets with other diversity dependent process and various conventional techniques were assuring. Srisungsittisunti et al. [31] proposed the crisis of preserving data based on a prominent security type. Moreover, obtained results demonstrate the effectiveness of the algorithm on practical significance were accessed. Nguyen and Chang [32] suggested a method that permits more private bits into a pair of pixels for embedding when promising the excellent stego-image quality. Moreover, the implemented system has preserved the best quality of the stego-image (i.e., PSNR is greater than 46 dB), that performs several conventional methods. Hong et al. [33]

implemented a method that utilizes a group of key-selected referential pixels to build a 3D Delaunay mesh to attain the forecasting errors. The results obtained from experiment has shown that the implemented method offers improved payload and image quality than the conventional PHS-dependent methods. Qin and Zhang [34] introduced a RDH method in encoded image. The content owner has encrypted the images that are real with the encoded key to achieve security for contents of the image. Simulation results have revealed the efficiency of the implemented scheme. Mao et al. [35] established a novel, RDHmethod that provides improved performances. Results obtained from experiments have illustrated that this method outperforms the existing reversible hiding methods. Shiu et al. [36] have introduced a new EIRDH-P. Also, the technique was analyzed regarding computation and communication. At last, the investigational outcomes demonstrated the efficiency of such system. Zhou et al. [39] introduced an efficient and security-preserving policy, called Privacy-Preserving Dynamic Medical text mining PPDM in health care systems and dynamic medical text mining. At last, the recognized security evidence and extensive performance estimation have revealed that the implemented PPDM attains a higher level of security**.** In 2014, Hong et al. [40] have introduced an effective protocol named as CELS to face the entire security needs. In addition, privacy/security and cost analysis demonstrated the efficiency and utility of the technique with real datasets. Zhu et al. [41] suggested an improved correlated privacy solution by describing the corresponding sensitivity and modeling a data which is correlated by means of liberating process. Experimental outcomes have explained that the implemented solution outperforms conventional differential privacy with respect to MSE on a large set of queries. David Kohlmayer et al. [56] introduced a flexible resolution for distributed data in the semi-honest design. Proceeding to the anonymization process, an encrypted global observation of the dataset was built through a protected multi-party computing SMC protocol. The experimental results demonstrated that this method offers highly competitive computation and provides a flexible and practical resolution for anonymizing distributed biomedical datasets.

In 2013, Zhang et al. [42] established a two-phase TDS technique to process data sets in large-scale by means of Map minimization structure on cloud. Evaluation results obtained from experiments reveals that with this technique, the efficiency and scalability of TDS can be considerably enhanced over conventional approaches. Sanchez et al. [44] introduced a paper that proposed a general-purpose sanitization process which was dependent on detailed conception and utilizes learning bases, hides and detects responsive textual details when maintaining its operations. Results from evaluation demonstrated that this technique outperforms schemes dependent on qualified classifiers concerning the recognition recall. Xiaoyun et al. [45] introduced a paper that targets to discover a realistic way of indicating the secure data network. Simulations have shown that evaluation pointers indicated can sufficiently measure the security. Waqar et al. [49] introduced the chance of making use of the metadata saved in the database of cloud for compromising the security of data items saved by means of a accumulating service of cloud provider's that was simple. RuiChen et al. [50] established a paper to set up local suppression to attain a modified secure design for data anonymization which is trajectory. The implemented local suppression that can considerably develop the data usage in anonymous trajectory data. Zhang et al. [51] suggested an effective quasi-identifier index dependent approach to make sure about the security conservation and attains better data usage over distributed and incremental data sets on the cloud. Results obtained from evaluation revealed that with this technique, the effectiveness of P2Q on extended data groups can be enhanced by conventional methods. R.Vidya Banu and N.Nagaveni [52] proposed a PCA-dependent method that conserves the security of susceptible details in MPC circumstances.

In 2011, Tamir Tassa and Dror J. Cohen [43] presented an algorithm whose objective is to arrive at an observation of the network that are unified and exclusive of revealing some of the data holder's details regarding connections of the nodes which are governed by various holders of data. Yuan et al. [46] proposed a l-diversity anonymity, k-degree design which considers the security of structural information and responsive labels of individuals. Also, extensive experiments were conducted to estimate the efficiency of the implemented technique. Shou et al. [48] implemented a novel anonymization design called (k, P)-anonymity. The implemented methods were estimated in a complete experimental analysis. The results validated the efficiency and effectiveness of this method. Jiuyong Li et al. [57] proposed that data generalization have to be described by the categorization capacity of data instead of the privacy necessity. Experimental results demonstrated that IACk algorithm supported better accurate categorizing models and was quicker than benchmark utility-aware data anonymization technique.

In 2012, L. A. Dunning and R. Kresman [47] presented a method for sharing of personal data between various factors. The method for the shared solution of specific factors for limited areas improved the reliability of the techniques. The implemented PCA-dependent varying process outcome in better protection of privacy and improved computation when evaluated with the conventional Generalized Differential Transform Method GDTMs. Guillermo et al. [58] introduced an approach that guarantees the user's k-anonymity in the query log when maintaining its exploitation. An evaluation of this paper in original query logs was provided, revealing the exploitation in data mining course which were dependent on partitioning. Grigorios Loukides and Aris Gkoulalas-Divanis [59] has suggested a method for processing data in a approach which assures utility of data publishers needs and acquires minimized loss of information. A widespread experimental analysis, by means of medical data and clickstream, revealed that this method allows more precise query is answering several times than the conventional methods when it was compared with them regarding efficiency. Chin et al. [60] established a RDH method which defines if the pixel was not embeddable or embeddable by evaluating the entire variation of its neighboring pixels. Results achieved from experiments and computational comparisons illustrated that the implemented method had improved visual quality and higher hiding capability when compared with the currently proposed techniques.

## B. Chronological Review

This survey analyses several papers established in various years. Fig. 1 represents the percentage of contributions for corresponding years. Initially, 8.33% of papers are taken from the year, 2017. Similarly, 5% of the papers are published in the year, 2016. Furthermore, 11.67%, 5% and 16.67% of contributions on privacy preservation are from year 2015, 2014 and 2013, respectively. The number of papers taken for data anonymization in the year 2012 is of 25%. Finally, the percentage of papers taken for data preservation in the year 2011 is about 26.33%.

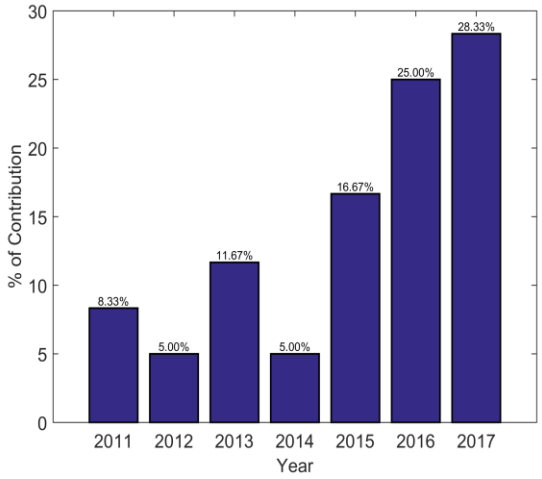



**Fig. 1.** Bar chart representing chronological review

## C. Various Applications

The different data preservation techniques are analyzed from about 60 papers as shown in Table I. From the analysis, it is obtained that the medical application attains about 20% of the entire contribution. Similarly, multimodal data integration and sharing and cloud computing contribute about 1.66% and 10% respectively. Also, image processing, visual communication, and social network applications obtain about 21.6%, 6.67% and 1.66% respectively. Video processing and marketing applications attain about 1.66% and 5% correspondingly. Similarly, traffic management, real-world applications, Geo-marketing and genetic application and location-based advertising contribute about 3.3%, 1.66% and 1.66% correspondingly. MIMO-OFDM system, communication system, machine learning and Web related application acquires about 1.66% respectively. Document sanitization, Multi-party network system along with social network and business analysis attains about 1.66% of the entire contribution. Similarly, location awareness obtains about 3.33%, and economic analysis, partner matching and social community tracking acquire almost 5% of the whole contribution. Moreover, defense, healthcare and finance, IoT application and Query log analysis attains about 1.66% of the entire contribution. Thus the different applications of privacy preservation process are analyzed on diverse data preservation applications.

**Table I:** Data Preservation On Various Applications And Its Citations

| Sl. No | Applications | [Citation] |
|---|---|---|
| 1 | Medical application | [1][4][16][17][22][25] [28] [38][39][54][56][59] |
| 2 | Multimodal data integration and sharing | [2] |
| 3 | Cloud computing | [3][20][42][47][49][51] |
| 4 | Image processing | [5][10][11][13][14][24][26][27][33][34][35][36][60] |
| 5 | Visual communication and image processing | [6] [8][12][32] |
| 6 | Social network applications | [7] |
| 7 | Video processing | [9] |
| 8 | Marketing applications | [15][29][37] |
| 9 | Real world application | [18][41] |
| 10 | Traffic management, Geo-marketing, and location-based advertising | [19] |
| 11 | Genetic application | [21] |
| 12 | MIMO-OFDM system | [23] |
| 13 | Communication system | [30] |
| 14 | Machine learning | [31] |
| 15 | Web related application | [40] |
| 16 | Location-awareness | [43][50] |
| 17 | Document sanitization | [44] |
| 18 | Multiparty network system | [45] |
| 19 | Social network and business analysis | [46] |
| 20 | Financial analysis, social community tracking and partner matching | [48][55][58] |
| 21 | Defense, healthcare, and finance | [52] |
| 22 | IoT application | [53] |
| 23 | Query log analysis | [57] |

## D. Loss and lossless data

In authentication and data preservation process, certain papers refer only the data hiding schemes, while few papers implement both the data hiding and restoration process. The overall analysis of loss and lossless data from entire contributions is shown in Fig. 2. From the performed analysis, it is noted that the data hiding scheme contributes about 66.66% whereas, the data hiding as well as restoration process contributes about 33.3% respectively.

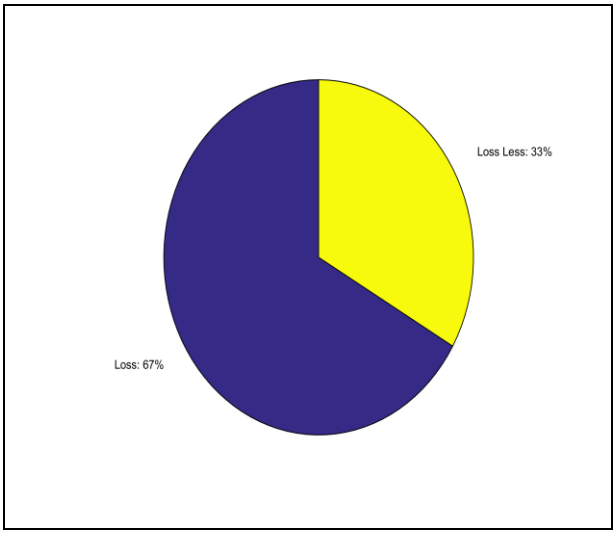



**Fig. 2.** Analysis on loss and lossless data

### E. Key Generation

The key or password serves as a security measure for data preservation and data hiding process. In fact, the data recovery also requires a key for proper authentication. The various contributions use several types of keys or password for authenticating protocols. Fig. 3 shows the data preservation techniques with and without using keys. The papers involved in this study facilitates about 53.3% of the contribution using key or password authentication and 46.7% of the contribution without using key or password.

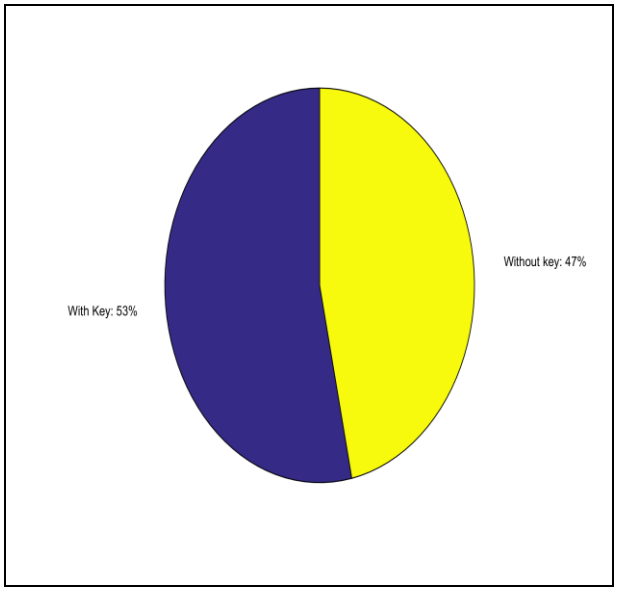



Fig.3. Data preservation with key and without using key

## 3. Performance Study on Privacy Preservation of Data

### A. Performance Measures

The papers taken for analysis on this survey include several measures like accuracy, efficiency, capability, etc. that are described by Table. II (common measures). Initially, accuracy contributes about 15% of the entire papers taken for survey. Similarly, k-anonymity acquires about 11.6% and execution time attains about 20% of the entire contribution. Moreover, execution time, information loss, embedding capacity and PSNR attains about 20%, 10%, 11.6% and 20% of the whole contribution. Quality factor, efficiency, utility and error rate contributes about 8.3%, 16.6%, 21.6% and 6.6% respectively. Similarly, delay, cost, and scalability acquire almost 20%, 8.3% and 8.3% of the entire contribution respectively.

The least measured parameters in the taken papers are analyzed by Table III. Initially, flexibility, probability, SSIM, precision, confidence ratio, threshold and number of iterations acquires about 3.3% of the entire contributions verified in this paper. Similarly, overlap, purity, high fidelity, variance, average AUC, FFT, length effect, guard interval, imperceptibility, block size, TPR, FPR, SPAM analysis, fitness, Attribute analysis, Pearson Correlation analysis contributes about 1.66% of the entire contribution verified by this paper. Data size, entropy, maximum capacity, embedding rate, visual quality, sensitivity, complexity, and hiding capacity involve 5% of the whole contributions considered in this paper. Thus the various measures are considered and verified.

**Table II**: Least used performance measures for understanding the ability of privacy preservation

| Sl.No | Measures | [Citation] |
|---|---|---|
| 1 | Flexibility | [3][8] |
| 2 | Probability | [3][48] |
| 3 | Overlap | [4] |
| 4 | Data size | [4][56] [21] |
| 5 | Purity | [7] |
| 6 | Entropy | [7][45][58] |
| 7 | Maximum capacity | [9][12][15] |
| 8 | SSIM | [9][11] |
| 9 | Embedding rate | [13][25][27] |
| 10 | High-fidelity | [14] |
| 11 | Visual quality | [14][34][32] |
| 12 | Variance | [15] |
| 13 | Average AUC | [16] |
| 14 | Precision | [16][44] |
| 15 | Sensitivity | [16][18][49] |
| 16 | Hiding capacity | [21][60] [23] |
| 17 | FFT length effect | [23] |
| 18 | Guard interval | [23] |
| 19 | Imperceptibility | [26] |
| 20 | Block size | [27] |
| 21 | TPR | [27] |
| 22 | FPR | [27] |
| 23 | Confidence ratio | [30][50] |
| 24 | Payload | [22][24][33][36] |
| 25 | SPAM analysis | [33] |
| 26 | Threshold | [29][37] |
| 27 | Fitness | [37] |
| 28 | Attribute analysis, Pearson Correlation analysis | [41] |
| 29 | Number of iterations | [43][52] |

### B. Data Preservation in health care

The medical applications analyzed in this survey include various diseases which they focus that are described by Table IV. Initially, diabetes is considered by 28% cancer is analyzed by 85.7% of the medical applications. Similarly, Pneumonia, flu, HIV and Gastritis and Duodenal ulcer constitute about 28.5%, 28.5%, 14.2%, 28.5% and 14.2% of the entire medical applications considered in this survey respectively.

**Table III** Preserved Data For Diverse Diseases In Each Contribution

| Sl. No | Disease | [Citation] | Count |
|---|---|---|---|
| 1 | Diabetes | [1][16] | 2 |
| 2 | Cancer | [4][17][25][39][54] | 5 |
| 3 | Pneumonia | [4] [54] | 2 |
| 4 | Flu | [4][54] | 2 |
| 5 | HIV | [38] | 1 |
| 6 | Gastritis | [39] [54] | 2 |
| 7 | Duodenal ulcer | [39] | 1 |

### C. Measures of medical applications

The measures of medical applications are compared with total measures of entire applications.

Definition 1: Familiarity measure: It is defined as the ratio of measures regarding medical applications to the measures regarding a total number of applications.
From the Fig. 4, it is known that the percentage of Acc, K-A, ET, IL, ER, PSNR, QF, Eff, Util, RE and cost are 28.57%, 42.86%, 27.27%, 20%, 11.11%, 9.09%, 25%, 20%, 25%, 25%and 40% respectively existed when compared on measures of entire contributions

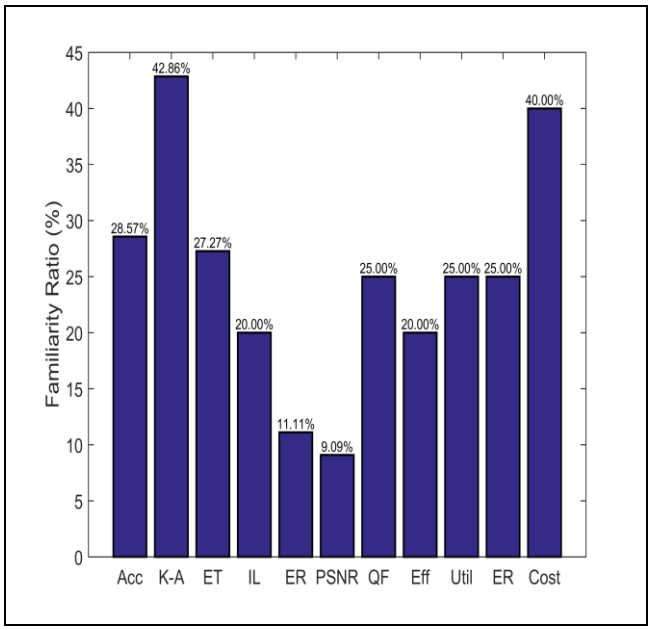



**Fig. 3.** Familiarity ratio of various measures

## 4. Research Gaps and Challenges

Traditionally, security needs are broken down into three main groups, namely: (i) integrity, (ii) confidentiality and (iii) availability that is defined as the CIA-triad. Confidentiality involves employing a set of norms to limit unofficial access to particular information. It is essential for IoT devices since they may manage critical personal information, for instance, medical prescription and records. For example, an unauthorized access to personal health measures may expose personal health information or even directs to life-threatening circumstances. Integrity is also essential for offering a consistent service. The device should make sure that the collected information and received commands are valid. The security issues begin from the data collection phase and persist throughout the gathered data lifecycle passing throughout the transmission, processing, and storage phases. Alternatively, the increasingly dense, invisible, and pervasive processing, collection, and dissemination of data in the middle of people's personal lives give rise to severe privacy distress. The tracking of individual information of activities lifestyle, preferences, and habits would potentially be available for unauthorized or third persons to observe. By means of the machine learning power, researchers investigate and formulate predictions concerning upcoming behaviors of people. The recent private data protection techniques are dependent primarily on security methods like accessing control mechanisms or data encryption. On the other hand, the threats in privacy of IoT outperforms these solutions and aggravate serious challenges like responsibility and accountability, profiling leakage, tracking, and privacy by intended concept. Various research efforts concern on gathering and processing data produced from various connected things. Many others implemented novel communication technologies, architectures, processing, and management schemes. Yet, there are only a few researches done on privacy preservation in IoT. Hence, there is a scope for conducting improved researches on privacy preservation in IoT.

## 5. Conclusion

As discussed in the above sections, data anonymization was a main characteristic of privacy preservation, and it has assisted in eliminating the privacy vulnerabilities in data preparation in various applications including healthcare. In healthcare applications, the data was normally scattered with varied sites handling the same set of properties for different anonymization methods. Anonymization and Pseudonymity were considered as two important privacy factors that were employed when adopting sensitive data. In this paper, the literature analyzed on various characteristics like data hiding, data preservation and data anonymization along with data restoration protocols. In conclusion, Consequently, this paper reviewed about 60 research papers and declared the significant analysis. Initially, the analysis depicted the chronological review of the overall contribution on different types of anonymization protocols.Subsequently, the analysis also focused on various features like applications, measures, key generation in data preservation. In addition, this paper also offered the detailed performance of the study regarding the data hiding and restoration process. At last, this paper has presented various research issues which can be useful for the researchers to accomplish further research on the features of data preservation. In future, further researches can be carried out regarding privacy for enhancing the data preservation technique to an improved level.

## References

[1] A. K. Ilavarasi1 and B. Sathiyabhama, "An evolutionary feature set decomposition based anonymization for classification workloads: Privacy Preserving Data Mining", Cluster Computing, pp 1–11, 30 august 2017.

[2] Peipei Sui, Xianxian Li, “A privacy-preserving approach for multimodal transaction data integrated analysis”, Neurocomputing, vol. 253, pp. 56-64, 30 August 2017.

[3] Dhasarathan Chandramohan, Thirumal Vengattaraman, Ponnurangam Dhavachelvan, “A secure data privacy preservation for on-demand cloud service”, Journal of King Saud University - Engineering Sciences, vol. 29, no. 2, pp. 144-150, April 2017.

[4] Soohyung Kim, Hyukki Lee, Yon Dohn Chung, “Privacy-preserving data cube for electronic medical records: An experimental evaluation”, International Journal of Medical Informatics, vol. 97, pp. 33-42, January 2017.

[5] Bingwen Feng, Jian Weng, Wei Lu, Bei Pei, “Steganalysis of content-adaptive binary image data hiding”, Journal of Visual Communication and Image Representation, vol. 46, pp. 119-127, July 2017.

[6] Shaowei Weng, Guohao Zhang, Jeng-Shyang Pan, Zhili Zhou, “Optimal PPVO-based reversible data hiding”, Journal of Visual Communication and Image Representation, vol. 48, pp. 317-328, October 2017.

[7] Zhi-Guo Chen , Ho-Seok Kang, Shang-Nan Yin and Sung-Ryul Kim, "An efficient privacy protection in mobility social network services with novel clustering-based anonymization", EURASIP journal on Wireless communications and networking, 2016.

[8] Nan-I Wu, Min-Shiang Hwang, “Development of a data hiding scheme based on combination theory for lowering the visual noise in binary images”, Displays, vol. 49, pp. 116-123, September 2017.

[9] Dawen Xu, Rangding Wang, Yani Zhu, “Tunable data hiding in partially encrypted H.264/AVC videos”, Journal of Visual Communication and Image Representation, vol. 45, pp. 34-45, May 2017.

[10] Jen-Chun Chang, Yi-Zhi Lu, Hsin-Lung Wu, “A separable RDHscheme for encrypted JPEG bitstreams”, Signal Processing, vol. 133, pp. 135-143, April 2017.

[11] Smita Agrawal, Manoj Kumar, “Mean value based RDHin encrypted images”, Optik - International Journal for Light and Electron Optics, vol. 130, pp. 922-934, February 2017.

[12] Kuo-Liang Chung, Chih-Yi Chiu, Tzu-Yu Yu, Po-Lin Huang, “Temporal and spatial correlation-based RDHfor RGB CFA videos”, Information Sciences, vol. 420, pp. 386-402, December 2017.

[13] Shuang Yi, Yicong Zhou, “Binary-block embedding for RDHin encrypted images”, Signal Processing, vol. 133, pp. 40-51, April 2017.

[14] Wenguang He, Jie Cai, Gangqiang Xiong, Ke Zhou, “Improved RDHusing pixel-based pixel value grouping”, Optik - International Journal for Light and Electron Optics, 6 September 2017.

[15] Somya Upadhyay, Chetana Sharma, Pravishti Sharma, Prachi Bharadwaj, K.R. Seeja, “Privacy preserving data mining with 3-

D rotation transformation", Journal of King Saud University - Computer and Information Sciences, 28 November 2016.
[16] Yan Li, Changxin Bai, Chandan K. Reddy, "A distributed ensemble approach for mining healthcare data under privacy constraints", Information Sciences, vol. 330, pp. 245-259, 10 February 2016.
[17] HaydenWimmer, Victoria Y. Yoon, Vijayan Sugumaran, "Amulti-agent systemto support evidence based medicine and clinical decision making via data sharing and data privacy", Decision Support Systems, 24 May 2016.
[18] Debanjan Sadhya, Sanjay Kumar Singh, "Privacy preservation for soft biometrics based multimodal recognition system", Computers & Security, vol. 58, pp. 160-179, May 2016.
[19] Elahe Ghasemi Komishani, Mahdi Abadi, Fatemeh Deldar, "PPTD: Preserving personalized privacy in trajectory data publishing by sensitive attribute generalization and trajectory local suppression", Knowledge-Based Systems, vol. 94, pp. 43-59, 15 February 2016.
[20] Rong Jiang, Rongxing Lu, Kim-Kwang Raymond Choo, "Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data", Future Generation Computer Systems, 12 May 2016.
[21] Samiha Marwan, Ahmed Shawish, Khaled Nagaty,"DNA-based cryptographic methods for data hiding in DNA media", Biosystems, vol. 150, pp. 110-118, December 2016.
[22] Zhenxing Qian, Shu Dai, Fei Jiang, Xinpeng Zhang, "Improved joint RDHin encrypted images", Journal of Visual Communication and Image Representation, vol. 40, Part B, pp. 732-738, October 2016.
[23] Liquan Chen, Zijuan Fan, Jie Huang, "Data hiding capacity of spatial domain bit replacement steganography in an MIMO-OFDM coding channel", AEU - International Journal of Electronics and Communications, vol. 70, no. 9, pp. 1295-1303, September 2016.
[24] Iyad F. Jafar, Khalid A. Darabkh, Raed T. Al-Zubi, Ramzi R. Saifan,"An efficient RDHalgorithm using two steganographic images", Signal Processing, vol. 128, pp. 98-109, November 2016.
[25] Yuling Liu, Xinxin Qu, Guojiang Xin, " A ROI-based RDHscheme in encrypted medical images", Journal of Visual Communication and Image Representation, vol. 39, pp. 51-57, August 2016.
[26] Mritha Ramalingam, Nor Ashidi Mat Isa , "A data-hiding technique using scene-change detection for video steganography", Computers & Electrical Engineering, vol. 54, pp. 423-434, August 2016.
[27] Iyad F. Jafar, Khalid A. Darabkh, Ramzi R. Saifan, "SARDH: A novel sharpening-aware RDHalgorithm", Journal of Visual Communication and Image Representation, vol. 39, pp. 239-252, August 2016.
[28] M. Prakash, G. Singaravel, "An approach for prevention of privacy breach and information leakage in sensitive data mining", Computers & Electrical Engineering, vol. 45, pp. 134-140, July 2015.
[29] Unil Yun, Jiwon Kim, "A fast perturbation algorithm using tree structure for privacy preserving utility mining", Expert Systems with Applications, vol. 42, no. 3, pp. 1149-1165, 15 February 2015.
[30] Yiannis Kokkinos, Konstantinos G. Margaritis, "Confidence ratio affinity propagation in ensemble selection of neural network classifiers for distributed privacy-preserving data mining", Neurocomputing, vol. 150, Part B, pp. 513-528, 20 February 2015.
[31] Bowonsak Srisungsittisunti, Juggapong Natwichai,"An incremental privacy-preservation algorithm for the (k, e)-Anonymous model", Computers & Electrical Engineering, vol. 41, pp. 126-141, January 2015.
[32] Thai-Son Nguyen, Chin-Chen Chang, "A RDHscheme based on the Sudoku technique", Displays, vol. 39, pp. 109-116, October 2015.
[33] Wien Hong, Tung-Shou Chen, Jeanne Chen, "RDHusing Delaunay triangulation and selective embedment",Information Sciences, vol. 308, pp. 140-154, 1 July 2015.
[34] Chuan Qin, Xinpeng Zhang, "Effective RDHin encrypted image with privacy protection for image content", Journal of Visual Communication and Image Representation, vol. 31, pp. 154-164, August 2015.
[35] Qian Mao, Fan Li, Chin-Chen Chang, "RDHwith oriented and minimized distortions using cascading trellis coding", Information Sciences, vol. 317, pp. 170-180, 1 October 2015.
[36] Chih-Wei Shiu, Yu-Chi Chen, Wien Hong, "Encrypted image-based RDHwith public key cryptography from difference expansion", Signal Processing: Image Communication, vol. 39, Part A, pp. 226-233, November 2015.
[37] Jimmy Ming-Tai Wu; Justin Zhan; Jerry Chun-Wei Lin, "Ant Colony System Sanitization Approach to Hiding Sensitive Itemsets",IEEE Journals & Magazines, vol. 5, pp. 10024 – 10039, 2017.
[38] Lei Xu; Chunxiao Jiang; Yan Chen; Jian Wang; Yong Ren,"A Framework for Categorizing and Applying Privacy-Preservation Techniques in Big Data Mining", IEEE Journals & Magazines, vol. 49, no. 2, pp. 54-62, 2016.
[39] Jun Zhou; Zhenfu Cao; Xiaolei Dong; Xiaodong Lin,"PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems", IEEE Journals & Magazines, vol. 9, no. 7, pp. 1332 – 1344, 2015.
[40] Yuan Hong; Jaideep Vaidya; Haibing Lu; Panagiotis Karras; Sanjay Goel, "Collaborative Search Log Sanitization: Toward Differential Privacy and Boosted Utility", IEEE Journals & Magazines, vol.12, no. 5, pp. 504 – 518, 2015
[41] Tianqing Zhu; Ping Xiong; Gang Li; Wanlei Zhou, "Correlated Differential Privacy: Hiding Information in Non-IID Data Set", IEEE Journals & Magazines, vol. 10, no. 2, pp. 229 – 242, 2015
[42] Xuyun Zhang; Laurence T. Yang; Chang Liu; Jinjun Chen, "A Scalable Two-Phase Top-Down Specialization Approach for Data Anonymization Using MapReduce on Cloud", IEEE Journals & Magazines, vol. 25, no. 2, pp. 363 – 373, 2014.
[43] Tamir Tassa; Dror J. Cohen, "Anonymization of Centralized and Distributed Social Networks by Sequential Clustering", IEEE Journals & Magazines, vol. 25, no. 2, pp. 311 – 324, 2013.
[44] David Sánchez; Montserrat Batet; Alexandre Viejo,"Automatic General-Purpose Sanitization of Textual Documents", IEEE Journals & Magazines, vol. 8, no. 6, pp. 853 – 862, 2013.
[45] Chen Xiaoyun; Su Yujie; Tang Xiaosheng; Huang Xiaohong; Ma Yan, " On measuring the privacy of anonymized data in multiparty network data sharing", IEEE Journals & Magazines, vol. 10, no. 5, pp. 120 – 127, 2013.
[46] Mingxuan Yuan; Lei Chen; Philip S. Yu; Ting Yu, "Protecting Sensitive Labels in Social Network Data Anonymization", IEEE Journals & Magazines, vol. 25, no. 3, pp. 633 – 647, 2013.
[47] Larry A. Dunning; Ray Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment", IEEE Journals & Magazines, vol. 8, no. 2, pp. 402 – 413, 2013.
[48] Lidan Shou; Xuan Shang; Ke Chen; Gang Chen; Chao Zhang,"Supporting Pattern-Preserving Anonymization for Time-Series Data", IEEE Journals & Magazines, vol. 25, no. 4, pp. 877 – 892, 2013.
[49] Adeela Waqar, Asad Raza, Haider Abbas, Muhammad Khurram Khan,"A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata", Journal of Network and Computer Applications, vol.36, no.1, pp. 235-248, January 2013.
[50] Rui Chen, Benjamin C.M. Fung, Noman Mohammed, Bipin C. Desai, Ke Wang, "Privacy-preserving trajectory data publishing by local suppression", Information Sciences, vol. 231, pp. 83-97, 10 May 2013.
[51] Xuyun Zhang, Chang Liu, Surya Nepal, Jinjun Chen, "An efficient quasi-identifier index based approach for privacy preservation over incremental data sets on cloud", Journal of Computer and System Sciences, vol. 79, no. 5, pp. 542-555, August 2013.
[52] R. Vidya Banu, N. Nagaveni, "Evaluation of a perturbation-based technique for privacy preservation in a multi-party clustering scenario",Information Sciences, vol. 232, pp. 437-448, 20 May 2013.
[53] J. Jesu Vedha Nayahi, V. Kavitha, "Privacy and utility preserving data clustering for data anonymization and distribution on Hadoop",Future Generation Computer Systems, vol. 74, pp. 393-408, September 2017.
[54] Soohyung Kim, Yon Dohn Chung, "An anonymization protocol for continuous and dynamic privacy-preserving data collection", Future Generation Computer Systems, 8 September 2017.
[55] David F. Nettleton, Julián Salas, "A data driven anonymization system for information rich online social network graphs", Expert Systems with Applications, vol. 55, pp. 87-105, 15 August 2016.
[56] Florian Kohlmayer, Fabian Prasser, Claudia Eckert, Klaus A. Kuhn, "A flexible approach to distributed data anonymization", Journal of Biomedical Informatics, vol. 50, pp. 62-76, August 2014.

[57] Jiuyong Li, Jixue Liu, Muzammil Baig, Raymond Chi-Wing Wong, "Information based data anonymization for classification utility", Data & Knowledge Engineering, vol.70, no. 12, pp. 1030-1045, December 2011.

[58] Guillermo Navarro-Arribasa,, Vicenç Torraa, Arnau Erolab, Jordi Castellà-Roca, "User k-anonymity for privacy preserving data mining of query logs", Information Processing and Management, 8 February 2011.

[59] Grigorios Loukides, Aris Gkoulalas-Divanis,"Utility-preserving transaction data anonymization with low information loss", Expert Systems with Applications, vol. 39, pp. 9764-9777, no. 10, August 2012.

[60] Chin-Chen Chang, Ying-Hsuan Huang, Hsin-Yi Tsai, Chuan Qin, "Prediction-based RDHusing the difference of neighbouring pixels", AEU - International Journal of Electronics and Communications, vol. 66, no. 9, pp. 758-766, September 2012.

[61] Fadi Al-Turjman, "Information-centric framework for the Internet of Things (IoT): Traffic modelling & optimization", Future Generation Computer Systems, In press, accepted manuscript, Available online 1 September 2017.

[62] Angel Perles, Eva Pérez-Marín, Ricardo Mercado, J. Damian Segrelles, Fernando J. Garcia-Diego, "An energy-efficient internet of things (IoT) architecture for preventive conservation of cultural heritage", Future Generation Computer Systems, 26 July 2017.

[63] Payton Lin, Dau-Cheng Lyu, Fei Chen, Syu-Siang Wang, Yu Tsao, "Multi-style learning with denoising autoencoders for acoustic modeling in the internet of things (IoT)", Computer Speech & Language, vol. 46, pp. 481-495, November 2017.

[64] Gang Sun, Victor Chang, Muthu Ramachandran, Zhili Sun, Dan Liao, "Efficient location privacy algorithm for Internet of Things (IoT) services and applications" Journal of Network and Computer Applications, vol. 89, pp. 3-13, 1 July 2017.

[65] Koko Friansa, Irsyad Nashirul Haq, Bening Maria Santi, Deddy Kurniadi, Brian Yuliarto,"Development of Battery Monitoring System in Smart Microgrid Based on Internet of Things (IoT)", Procedia Engineering, vol. 170, pp. 482-487, 2017.

[66] Vlad Krotov, "The Internet of Things and new business opportunities", Business Horizons, 12 September 2017.

[67] Oladayo Bello, Sherali Zeadally, Mohamad Badra, "Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT)", Ad Hoc Networks, vol. 57, pp. 52-62, 15 March 2017.

[68] In Lee, Kyoochun Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises",Business Horizons, vol. 58, no. 4, pp. 431-440, July–August 2015.

[69] Maria Ganzha, Marcin Paprzycki, Wiesław Pawłowski, Paweł Szmeja, Katarzyna Wasielewska, " Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective", Journal of Network and Computer Applications, vol. 81, pp. 111-124, 1 March 2017.

[70] Hyung-Jun Yim, Dongmin Seo, Hanmin Jung, Moon-Ki Back, Kyu-Chul Lee, "Description and classification for facilitating interoperability of heterogeneous data/events/services in the Internet of Things", Neurocomputing, vol. 256, pp. 13-22, 20 September 2017.

[71] Wen-Chung Kuo, Chun-Cheng Wang, Hong-Ching Hou, "Signed digit data hiding scheme", Information Processing Letters, vol. 116, no. 2, pp. 183-191, February 2016.

[72] Wen-Chung Kuo, Chun-Cheng Wang, Yu-Chih Huang, "Binary power data hiding scheme", AEU - International Journal of Electronics and Communications, vol. 69, no. 11, pp. 1574-1581, November 2015.

[73] Thai-Son Nguyen, Chin-Chen Chang, Wen-Chi Chang, "High capacity RDHscheme for encrypted images", Signal Processing: Image Communication, vol. 44, pp. 84-91, May 2016.

[74] Shaohui Liu, Seungmin Rho, Worku Jifara, Feng Jiang, Chun Liu, "A hybrid framework of data hiding and encryption in H.264/SVC", Discrete Applied Mathematics, 21 September 2016.

[75] 75. Reza Moradi Rad, KokSheik Wong, Jing-Ming Guo, "RDHby adaptive group modification on histogram of prediction errors", Signal Processing, vol. 125, pp. 315-328, August 2016.

[76] Yunxia Liu, Leiming Ju, Mingsheng Hu, Hongguo Zhao, Zhijuan Jia, "A new data hiding method for H.264 based on secret sharing", Neurocomputing, vol. 188, 5 May 2016, pp. 113-119.

[77] Hai-yang Ding, Yi-xian Yang, "Data hiding in color halftone images based on new conjugate property", Computers & Electrical Engineering, 1 July 2016.

[78] Neethu Thomas, Shiney Thomas, "A Low Distortion RDHTechnique Using Improved PPVO Predictor", Procedia Technology, vol. 24, pp. 1317-1324, 2016.

[79] Heng Yao, Chuan Qin, Zhenjun Tang, Ying Tian, "Guided filtering based color image reversible data hiding", Journal of Visual Communication and Image Representation, vol. 43, pp. 152-163, February 2017.

[80] Hsiang-Cheh Huang, Feng-Cheng Chang, "Hierarchy-based reversible data hiding", Expert Systems with Applications, vol. 40, no. 1, pp. 34-43, January 2013.

[81] Kuan Zhang, Xiaohui Liang, Mrinmoy Baura, Rongxing Lu, Xuemin (Sherman) Shen, "PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs", Information Sciences, vol. 284, pp. 130-141, 10 November 2014.

[82] Raúl Pardo, Musard Balliu, Gerardo Schneider, "Formalising privacy policies in social networks", Journal of Logical and Algebraic Methods in Programming, vol. 90, pp. 125-157, August 2017.

[83] Yuan Chi, Jun Hong, Anna Jurek, Weiru Liu, Dermot O'Reilly, "Privacy preserving record linkage in the presence of missing values", Information Systems, vol. 71, pp. 199-210, November 2017.

[84] Xuyun Zhang, Chang Liu, Surya Nepal, Jinjun Chen, "An efficient quasi-identifier index based approach for privacy preservation over incremental data sets on cloud", Journal of Computer and System Sciences, vol. 79, no. 5, pp. 542-555, August 2013.

[85] Nirali Nanavati, Devesh Jinwala, "Privacy Preservation for Global Cyclic Associations in Distributed Databases", Procedia Technology, vol. 6, pp. 962-969, 2012.

[86] Farzana Rahman, Md Zakirul Alam Bhuiyan, Sheikh Iqbal Ahamed, "A privacy preserving framework for RFID based healthcare systems", Future Generation Computer Systems, vol. 72, pp. 339-352, July 2017.

[87] Alsharif Abuadbba, Ibrahim Khalil, Mohammed Atiquzzaman, "Robust privacy preservation and authenticity of the collected data in cognitive radio network—Walsh–Hadamard based steganographic approach", Pervasive and Mobile Computing, vol. 22, pp. 58-70, September 2015.

[88] Rajen Akalu, "Privacy, consent and vehicular ad hoc networks (VANETs)", Computer Law & Security Review, 3 July 2017.

[89] Kun Xie, Xueping Ning, Xin Wang, Shiming He, Zheng Qin, "An efficient privacy-preserving compressive data gathering scheme in WSNs", Information Sciences, vol. 390, pp. 82-94, June 2017.

[90] José M. de Fuentes, Lorena González-Manzano, Juan Tapiador, Pedro Peris-Lopez, "PRACIS: Privacy-preserving and aggregatable cyber security information sharing", Computers & Security, vol. 69, pp. 127-141, August 2017.