International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 11, Issue 7, July 2020, pp. 629-638, Article ID: IJARET_11_07_063
Available online athttp://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=7
ISSN Print: 0976-6480 and ISSN Online: 0976-6499
DOI: 10.34218/IJARET.11.7.2020.063

LEGAL ISSUES RELATED TO BIG DATA

Preeti Gulia and Hemlata
Department of Computer Science and Applications,
Maharshi Dayanand University, Rohtak, India

ABSTRACT

Big data is concerned with the massive volume of data generated from numerous sources like audio, video, images, social media, sensors, and transactions, etc. The massive volume of big data sets is too complex to be managed and processed. It is a subject of debate among a variety of areas like management and promoting, research, national security, government transparency. Due to this, there are risks of the protection and privacy of big data. Thereby legal problems arise from the contravention of privacy. This paper summarizes the various methods to handle the breach of privacy and legal issues related to the big data field.

Key words: Big Data, Privacy issues, Legal implications.

Cite this Article: Preeti Gulia and Hemlata, Legal Issues Related to Big Data, *International Journal of Advanced Research in Engineering and Technology,* 11(7), 2020, pp. 629-638.
http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=7

1. INTRODUCTION

'Big Data' presents different new manners by which associations, including government and organizations, blend various advanced information sets, thus use insights and various data mining procedures to take out concealed data and stunning relationships. Big data is best comprehended as a new ground-breaking variant of data disclosure in databases or data preparation that has been illustrated as 'the nontrivial extraction of the understood, precursor complex and undoubtedly essential data from data.

Big Data Analytics is managed, putting away and preparing of the risky and massive datasets. As a rule, Big Data is characterized by ten properties [1]. These are:

Volume is worried about broad data and the enormous size of data. A specific data can be considered as big data or not, for the most part, relies on its volume. Along these lines, "Volume" is the crucial parameter that ought to be thought of while managing “Big Data.”

Velocity is the term worried about the data generation speed. The rate at which speed data is delivered and handled to satisfy the needs indicates the genuine capability of data. Big data Velocity decides the speed at which data streams. The progression of data can be monstrous and persistent.

Variety alludes to different sorts of wellsprings of data. It is realized that the data is available in the two structures, i.e., organized and unstructured. Prior datasets were the primary wellsprings of data considered by the more significant part of the application's territory. Data in video records, email, sound documents, word preparing documents, and so forth are additionally being considered in the logical application.

Variability deals with the inconsistency, which can be shown by data and which obstructs the process to handle and manage the data effectively.

Veracity is worried about the provenance or dependability of the data source, its specific situation, and that it is so significant to the examination.

Validity is the term that manages the precision and rightness of data.

Vulnerability concerns with the security highlight of data. A data breaks with big data is a big penetrate.

Volatility is a parameter of Big Data concerning an exact proportion of the scattering for a given arrangement of profits.

Visualization is a present characteristic of big data that manages the representation of data. Changeability in big Data's setting alludes to the irregularity of speed at which the data is put away into our framework.

Value is a fundamental property of big data. It is a tinkle for big data since it is enormous for organizations and foundation frameworks of IT to store a gigantic and enormous measure of qualities in their databases.

Big data analytics helps the individual to make the decisions. While Big Data guarantees essential economic and social advantages, it additionally raises serious privacy issues [2]. Nowadays, the benefits of big data are reversed by privacy and security issues. Big Data privacy is the most important legal challenge of utilizing a massive volume of data.

2. RELATED STUDIES FOR BIG DATA AND PRIVACY ISSUES

Use This section discusses the research work of different researchers in the field of big data analytics focusing on privacy and legal concerns in it. The capability of big data is enormous when it deals with big data analytics. With the data analytics, the businessmen target shoppers precisely and with efficiency by advertising the products and services and offers which support his or her characteristics. Through mobile's geospatial chase, massive information provides the extremely relevant information delivered at the right time and the correct place. The related studies are briefly presented below:

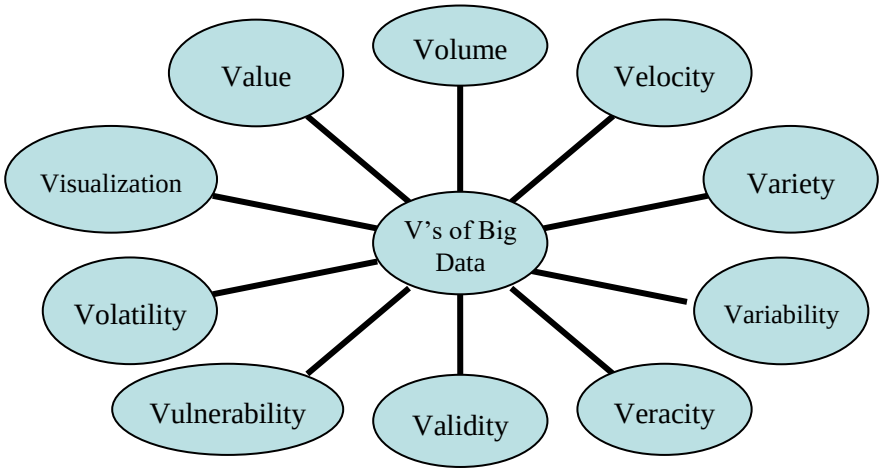

Figure 1 V's of Big Data

2.1. Zhang, "Big Data Security and Privacy Protection" (2018)

The author has discussed that in the existing scenarios of the big data, legal problems occur due to infringement of privacy and security. A number of the steps to save lots of the privacy of the info are bestowed within the paper. However, there are heaps of scope during this field of analysis. Researchers will need to generate a new prototype to keep the data/database secure from others. In this regard, new laws can be developed by the government. Corporations or organizations ought to circulate strict orders to the employees for not revealing personal information to any other party. [3].

Gruschka et al. "Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR" (2018)

The authors have given the suggestions of data protection laws on coping with big data, with the help of two case studies. They stressed that the techniques of privacy-preserving are to be applied. A data protection impact assessment has to be conducted for the technologies coping with sensitive or personal knowledge in the very early stages of the project to determine potential privacy challenges. [4].

Abdullah, "Privacy, security and legal challenges in big data" (2018)

The author in this paper has discussed that big data is a crucial kind of analysis, and can be a part of analysis for an extended time. However, legal problems touching tremendous knowledge mean that the application of getting and exploitation big data will evolve within the next few years. Legal problems associated with immense knowledge do not seem to be regarding solely how data is collected; however, additionally, how it is used. This is one of the first legal problems that conflict with tremendous knowledge. Knowledge assortment sometimes involves a variety of privacy and proper speech act [5].

Fang et al., "A survey of big data security and privacy-preserving" (2017)

The authors have discussed the idea of privacy-preserving of big data, specific challenges and related problems, and some techniques of big data privacy-preserving. They highlighted the laws and regulations' and also unraveled the drawbacks of big data privacy-preserving. They have shown that the existing techniques of privacy-preserving are still not mature. It was specified that the simplest way to solve the problem is to mix the various technological methods, connected policies, and privacy-preserving laws [6].

Rao and Kumar, "Challenges arise of Privacy-Preserving Big Data Mining Techniques" (2017)

The authors in this study examine the significance of big data analytics of information collected from Social Media for increased business intelligence in various businesses. Social Media in the Republic of India and on-line business in India have fully grown exponentially over the last decade and thus gift a chance to seem into the however knowledge collected from these channels may be usefully utilized for any business enhancements. Data processing techniques provide the backbone to harnessing data quickly and expeditiously on immense knowledge. However, this conjointly means that there is a possibility for extracting personal data by compromising user privacy. In this paper, the challenges in Privacy-Preserving Big Data Mining techniques are discussed [7].

Cate et al., "The Challenge of "Big Data" for Data Protection" (2012)

The authors have addressed various ways that may be of great significance for improving data protection within the face of immense knowledge. They have concluded that it is vital to work along to spot the principles that should guide our efforts [8].

Wahlstrom et al. "Legal and technical issues of privacy preservation in data mining" (2009)

The authors have concluded that we exist in an associate setting of speedy modification during which technology has an ever-increasing social connectedness. The challenge now could be to implement a way of assessing associate rising technology's social impact at the same time to its analysis, providing the U.S.A. with the capability to use the tools technology provides with wisdom and considerately for our culture and its future. [9]. Table 1 presents the research gap as per the systematic literature review.

Table 1 Research gaps

Authors(s)/Year	Literature Review	Research gaps
Zhang (2018)	The current scenario of the big data, privacy, and security are presented.	Need to develop a new model to keep data secure
Fatma Mohammed Abdullah (2018)	Conventional safety mechanisms, Small-scale static data 5v's of Big Data	In future security techniques for large scale, static data can also be analyzed. Other five v (variety, validity, variability, visualization, volatility) can also be considered for security purposes.
Nils Gruschka (2018)	Discussion on the EU General Data Protection Regulation (GDPR). The sorts of data which can turn into a privacy chance. They utilized privacy-safeguarding methods as indicated by the legal prerequisites. The impact of the strategies on data handling utilizing anonymization.	Their focus is mainly on GDPR using anonymization. Other techniques of Privacy can also be used for the same purpose.
Rao and Kumar (2017)	They explore technical aspects of protecting privacy while processing Big Data. In this paper, they have done this by using Anonymization Techniques, Generalization, Randomization	Other techniques can also be used in various circumstances. They focus on big data generated by social media only.
Ira S. Rubinstein (2013)	This paper presented the consideration of a General Data Protection Regulation of Europe that would replace the aging Data Protection Directive.	New business models can be constructed following the new security and privacy requirements
Fred H. Cate *et al.* (2012)	Primary attention on the data generated from credit and debit cards, checks. Focused on the data that is captured by increasingly sensor networks and saved by more than one party.	Their focus is on protection related to big data collection. However, there can be some protection techniques related to Big data uses.

3. LEGAL ISSUES IN BIG DATA

Big data means the collection of massive data that comes from multiple sources with high speed, variety, and volume. Big Data is produced by everything around us. With such a large scale of collection and usage of user data, privacy, and legal concerns have also raised [10]. This section discusses the number of legal concerns in big data.

Consumer Privacy

As the powerful computers store additional personal data, large sets of knowledge – big data – became obtainable for not solely legitimate uses, however conjointly abuses. Big data has an enormous potential to change our lives with its prognostic power. Imagine a situation in the future in which you recognize how your weather is going to be like with ninety-five % accuracy forty-eight hours before time. However, due to the probability of malignant use, there is a security and privacy threat of vast information you must worry regarding, particularly as you pay longer on the web [11].

Security of personal information

The advent of the time of big data has dramatically promoted the event of the society; however, at a similar time, the explanation for data security drawback has been very anxious. Thus, we tend to desperately like a replacement mechanism to shield personal privacy. The protection of private data security has to be compelled to be worn out in many ways, with the maximum limit to cut back the chance of non-public data outpouring, to raised shield the security of the net data, promote the economic development of our country [12].

Protecting personal data within the age of big data is initiated by those who own the most information. As a result, it raises the importance of the security of personal data [13].

Control over Data

The possession rights to big data give a serious business advantage. The data proprietor has authority over data as the data is additionally utilized and shared. For instance, Twitter offers its day by day tweets to different firms that attempt to extract vile data. The vast majority of the cash extracted from the big data originates from arranging data from altogether various sources. Ownership of data coming about because of the data examination is additionally imperative. Rights to data are once in a while designated inside the privacy approach and TOS for sites, online administrations, and versatile applications. Antiquated consented to arrangements are likewise used in business-to-business transactions [14].

Intellectual Property Protection

It follows that it cannot be barred that various actors inside the big data investigation lifecycle can attempt to guarantee holding rights or protection underneath exchange insider facts (portions) of the datasets intended to be utilized. They will so attempt to practice the select rights associated with the holding right included or keep the data mystery. Any nonsensical exercise of rights could smother data sharing and, in this way, advancement through monstrous data, just as inside the vehicle part. This is often, however, in the fundamental due to the innate nature and reason for holding rights and competitive innovations protection, which can at the same time offer a motivating force for partners to interact in data sharing for large data capacities [15].

Terms of Service Agreement (TOS)

Terms of Service Agreement could be a legal understanding that shows the responsibility and limitations for using a site or online assistance. The TOS gives the manners in which that

reduce the opportunity of cases from clients. There is additionally a legal obligation if the data examination gives wrong or no out of line data. Such obligation is planned in the TOS by the vow, disclaimers of guarantees, and confinement of risk arrangements for various contracts. The TOS may build the appropriate use, limitations on activities, disclaimers concerning the substance, repayment, term, and end, copyright and diverse property rights, overseeing law, ward, question goals, and various issues [16].

Notice or Consent

The owner of the data should be given a notice of how his data will be used and who will use it [17-21]. Notice also refers to awareness, i.e., data owners should be aware of his data usage [22]. Organizations should disclose how and for what purpose the data will be used, and owners should be asked to give their consent for it [23-24].

The data owner does not know precisely where his sensitive data is being used and how it is combined with other data to extract more information about the data owner. They are also unaware of the inferences drawn from their private data with the help of Big Data Analytics.

Access or Participation

The concept of participation and access was given by the Fair Credit Reporting Act (FCRA) [25]. The owner of the data himself accesses his data in order to verify that the data is complete and accurate or not. If it is not accurate, he is given the right to correct it [26-27]. In this era of Big Data, this is not feasible, and it is an enormous challenge to follow this concept. The proprietors do not have a direct relationship with the associations which are utilizing their data [28].

DNT and DNC

Another privacy-affected area is “Do Not Track (DNT)” [29]. It means that the data owner’s data should not be tracked for advertising. “Federal Trade Commission (FDC) proscribes the collection of personal information like financial data, health data, likes, and dislikes, etc.”. Collection or tracking of sensitive and private data is a severe violation of privacy. The government should develop laws to forbid this type of practice.

De-identification and Re-identification

De-identification means that the data should not be able to identify the identity of the data owner. Data should be anonymized, i.e., data should be modified in the form that it does not disclose the sensitive data to the users [30-31]. After the Anonymization of data, data should not reveal the identity when combined with any other data. It means that the data should not be of re-identification nature [32].

European data protection laws state that anonymized information must not recognize the personal data when combined with other anonymized data [33-34]. Anonymization should be done in such a way that re-identification is not possible [35]. Several examples show that re-identification can be done. Netflix contest is a famous example of re-identification, which led to a lawsuit against Netflix [36]. Another example of re-identification is that a researcher re-identified Massachusetts governor from a healthcare database combined with the voter records available publicly [37].

4. RESULTS

By analyzing the legal issues presented in the paper, it can be concluded that a single method is not sufficient to ensure the confidentiality of Big Data. For systems handling the massive amounts of data, efficient software systems are required. Testing plays a vital role in ensuring

the quality and reliability of the software system [38-47]. As per the situation or the issue of privacy, a combination of different methods for protecting the privacy of Big Data is used [48]. De-identification or Anonymization of data should be done before using customer data. Methods like notice or consent and Do Not Track or Do Not can be used for protecting the privacy of Big Data. The legal issues, if dealt with timely and efficiently, may have some benefits in preserving the privacy of users. The benefits are summarized in Table 2 below: -

Table 2 Legal Issues and Benefits

LEGAL ISSUES	BENEFITS
Consumer Privacy	Use of laws and regulations to protect individuals from privacy loss due to the failure's customer privacy measures. It uses countermeasures like cryptography, access management, intrusion detection, and backups for forestalling information from being broken and falling into the incorrect hands.
"Security of Personal Information"	Personal or private data is secured from misuse.
Control over Data	Ownership rights to big data will offer a serious advantage to the business. The owners have control over data to safeguard their privacy of data.
"Intellectual Property Protection"	Protect one's original creations. It incorporates copyright, database right, secrecy, licenses, right to innovations, and trademarks. It controls access or puts limitations on various kinds of data.
Terms of Service Agreement (TOS)	It a lawful understanding that sets up the commitments and limitations for utilizing a site, portable application, or online assistance. It builds the extent of reasonable use, limitations on exercises, disclaimers concerning the substance, repayment, term, and end, purview, and contest goals.
Notice or Consent	The owner of the data should be given a notice of how his data will be used and who will use it. Organizations should disclose how and for what purpose the data will be used, and owners should be asked to give their consent for it
Access or Participation	The owner of the data himself accesses his data in order to verify that the data is complete and accurate or not If it is not accurate, he is given the right to correct it.
Do Not Collect and Do Not Track	Prohibition of the collection of an individual's personal information which can reveal the sensitive information of the users. The data owner's data should not be tracked for advertising.
De-identification and re-identification	It preserves the identification of information of the data owner. It leads to Anonymization, which states that data should not reveal the identity when combined with any other data.

5. CONCLUSION

Each large organization is battling to search out the approaches to make the data helpful. In any case, this is regularly not a straightforward undertaking. It is problematic to store, oversee, examine, and use the massive amount of information made. The occasion of grouped gigantic information examination apparatuses has encouraged with information taking care of to a reasonable degree. Utilizing and monetizing big data raises monumental legal queries and potential liabilities. Legal problems arising out of the use/misuse of big data are given intimately. The paper presents some of the privacy and legal issues and steps to save the privacy of data. The rights required for significant data protection are unfolded within the paper.

The methods present in the paper should be more investigated by future researchers so that the methods can be more reformed or refined. Future work in this field can be to explore new methods of preserving the privacy of Big Data so that no legal issues arise after that.

REFERENCES

[1] https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx

[2] Rubinstein, I., 2012. "Big data: the end of privacy or a new beginning?". *International Data Privacy Law (2013 Forthcoming)*, pp.12-56.

[3] Zhang, D., 2018, October. "Big data security and privacy protection." *In the 8th International Conference on Management and Computer Science (ICMCS 2018).* Atlantis Press.

[4] Gruschka, N., Mavroeidis, V., Vishi, K., and Jensen, M., 2018, December. "Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR." *In 2018 IEEE International Conference on Big Data (Big Data) (pp. 5027-5033). IEEE.*

[5] Abdullah, F.M., "PRIVACY, SECURITY AND LEGAL CHALLENGES IN BIG DATA," International Journal of Civil Engineering and Technology (IJCIET), 2018.

[6] Fang, W., Wen, X.Z., Zhang, Y. and Zhou, M., 2017. "A survey of big data security and privacy-preserving." IETE Technical Review, 34(5), pp.544-560.

[7] Rao, M.C., and Kumar, A.K., 2017. "Challenges arise from Privacy Preserving Big Data Mining Techniques." International Research Journal of Engineering and Technology (IRJET).

[8] Cate, Fred H.; Kuner, Christopher; Millard, Christopher; and Svantesson, Dan Jerker B., "The Challenge of "Big Data" for Data Protection" (2012). Articles by Maurer Faculty. 2620

[9] Wahlstrom, K., Roddick, J.F., Sarre, R., Estivill-Castro, V., and de Vries, D., 2009. "Legal and technical issues of privacy preservation in data mining" Encyclopedia of Data Warehousing and Mining, Second Edition (pp. 1158-1163). IGI Global.

[10] https://rroyselaw.com/technology-transactions/agtech/legal-issues-big-data-2017/#_ftn6

[11] http://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798

[12] Consent of Customer to Use Personal Data: http://www.ftc.gov/reports/privacy3/

[13] Zou, H., 2016, December. "Protection of personal information security in the age of big data." *In 2016 12th International Conference on Computational Intelligence and Security (CIS) (pp. 586-589). IEEE*

[14] "The Internet of Things is Driving Smart Agriculture," http://royselawblog.com/the-internet-of-things-is-driving-smart agriculture/.

[15] Yang, M., 2019, April. "Research on Intellectual Property Protection from the Perspective of Big Data." *In 1st International Symposium on Education, Culture and Social Sciences (ECSS 2019).* Atlantis Press.

[16] Mohanty, H., and Vaddi, S., 2015. "Big Data Service Agreement. In Big Data" (pp. 137-160). Springer, New Delhi

[17] Chahal, Hemlata. (2018). "Comprehensive Analysis of Data Mining Classifiers using WEKA." International Journal of Advanced Computer Research. 9. 10.26483/ijarcs.v9i2.5900.

[18] Munir, A.B., Yasin, M., Hajar, S., and Muhammad-Sukki, F., 2015. "Big data: big challenges to privacy and data protection." *International Scholarly and Scientific Research & Innovation*, *9*(1).

[19] https://www.geeksforgeeks.org/5-vs-of-big-data/

[20] https://www.dummies.com/careers/find-a-job/the-4-vs-of-big-data/.

[21] https://www.ibmbigdatahub.com/infographic/four-vs-big-data.

[22] https://www.zarantech.com/blog/the-4-vs-of-big-data/

[23] Hemlata, Gulia P. (2018) "DCI3 Model for Privacy-Preserving in Big Data". In: Aggarwal V., Bhatnagar V., Mishra D. (eds) Big Data Analytics. Advances in Intelligent Systems and Computing, vol 654. Springer, Singapore

[24] Tene, Omer, Polonetsky, Jules: "Big data for all: Privacy and user control in the age of analytics," 11 NW. J. Tech. Intell. Prop. 239, 240–242 (2013)

[25] Big Data and Data Protection, ICO Informations Commissioner's Office

[26] Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681, et. Seq

[27] Hemlata, Gulia, P. (2017). "Novel Algorithm for PPDM of Vertically Partitioned Data." International Journal of Applied Engineering Research, 12(12), 3090- 3096.

[28] Fang, W., Wen, X.Z., Zhang, Y. and Zhou, M., 2017. "A survey of big data security and privacy-preserving." IETE Technical Review, 34(5), pp.544-560.

[29] Young, M.: "The technical writer's handbook-protecting consumer privacy in an era of rapid change." University Science, Mill Valley, CA (1989)

[30] http://www.infolawgroup.com/2012/03/articles/data-privacy-law-or-regulation/ftc-looks-tolink-donottrack-big-data-privacy-concerns-seeks-solutions/

[31] Godard, B., Schmidtke, J., Cassiman, J.J., and Aymé, S., 2003. "Data storage and DNA banking for biomedical research: informed consent, confidentiality, quality issues, ownership, the return of benefits." A professional perspective. *European Journal of Human Genetics*, *11*(2), pp. S88-S122.

[32] Hemlata & Gulia, Preeti. (2018). "Big data mining application in fasteners manufacturing market by using apache mahout." International Journal of Engineering Research and Technology. 11. 881-896.

[33] De-identification of Customer Data: http://en.wikipedia.org/wiki/De-identification

[34] Anonymised and De-identification of Information: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

[35] European Union Directive 95/46/EC

[36] Robust De-anonymization of Large Data Sets: How to break the anonymity of the Netflix prize data set. http://arxiv.org/PS_cache/cs/pdf/0610/0610105v2.pdf

[37] Example of Anonymous Data: http://www.wired.com/images_blogs/threatlevel/2009/12/doev-netflix.pdf.

[38] O. Dahiya and K. Solanki, "Comprehensive cognizance of Regression Test Case Prioritization Techniques," International journal of emerging trends in engineering research, Vol. 7 No. 11, pp. 638-646, 2019.

[39] O. Dahiya and K. Solanki, S. Dalal, A. Dhankhar, "Regression Testing: Analysis of its Techniques for Test Effectiveness," International Journal of advanced trends in computer science and engineering, Vol. 9, No. 1, pp. 737-744, 2020.

[40] O. Dahiya and K. Solanki, S. Dalal, A. Dhankhar, "An Exploratory Retrospective Assessment on the Usage of Bio-Inspired Computing Algorithms for Optimization," International journal of emerging trends in engineering research, Vol. 8 No. 2, pp. 414-434, 2020.

[41] O. Dahiya and K. Solanki, and A. Dhankhar, "Risk-Based Testing: Identifying, Assessing, Mitigating & Managing Risks Efficiently In Software Testing," International Journal of advanced research in engineering and technology, Vol. 11, Issue 3, pp. 192-203, 2020.

[42] Solanki, K., Singh, Y. and Dalal, S., "A Comparative Evaluation of "m-ACO" Technique for Test Suite Prioritization". *Indian Journal of science and technology*, *9*(30), pp.1-10, 2016.

[43] O. Dahiya, and K. Solanki, "A systematic literature study of regression test case prioritization approaches." International Journal of Engineering & Technology, 7(4), pp.2184-2191, 2018.

[44] O. Dahiya, K. Solanki and S. dalal, "Comparative Analysis of Regression Test Case Prioritization Techniques," International Journal of advanced trends in computer science and engineering, Vol. 8 No. 4, pp. 1521-1531, 2019.

[45] Solanki, K., Singh, Y. and Dalal, S., Experimental analysis of m-ACO technique for regression testing. *Indian Journal of Science and Technology*, *9*(30), pp.1-7, 2016.

[46] P. Gulia and Palak, "Nature-inspired soft computing based software testing techniques for reusable software components" Journal of Theoretical & Applied Information Technology, *95*(24), 2017.

[47] P. Gulia, and Palak, "Hybrid swarm and GA based approach for software test case selection." International Journal of Electrical & Computer Engineering, pp. 2088-8708, Issue-9, 2019.

[48] R. Ratra, and P. Gulia, "Big Data Tools and Techniques: A Roadmap for Predictive Analytics.", International Journal of Engineering and Advanced Technology (IJEAT), Vol. 9, Issue-2, pp. 4986-4992, 2019.

[49] S. Nagarjuna Reddy, Y. Vijaya Bhaskara Reddy, S. Sai Sathyanaryana Reddy. A Dynamic Programming Approach to Data Discovery and Analysis of Big Data. International Journal of Civil Engineering and Technology,8(12), 2017, pp. 718-722

[50] Dr. Anjali Mathur, V Vaishnavi, K Jigeesha, K S V A G Sudheer, A Framework Using Big Data Analysis on Human Activity Patterns for Health Prediction, International Journal of Mechanical Engineering and Technology, 8(12), 2017, pp. 775–787

[51] K. Vikram, Ch.Aparna, Harshitha.B and Ishpreet Kaur, A Secure and Certifiable Access Mechanism System Designed for Big Data Storage in Clouds. International Journal of Computer Engineering & Technology, 9(2), 2018, pp. 86–90.

[52] Azhagammal Alagarsamy and Dr. K. Ruba Soundar, A Survey Paper on Deep Belief Network for Big Data. International Journal of Computer Engineering and Technology, 9(5), 2018, pp. 161-166