ISSN: 2633-4828 Vol. 6 No.3, September, 2024

International Journal of Applied Engineering & Technology

IMPLEMENTING SECURE MULTI-PARTY COMPUTATION IN BIG DATA ANALYTICS: TECHNIQUES AND CHALLENGES

Priyam Vaghasia and Dhruvitkumar Patel
Mondrian collection, Staten Island Performing Provider System
priyamvaghasia57@gmail.com, pateldhruvit2407@gmail.com

ABSTRACT

One of them is Secure Multi-Party Computation (MPC), which is a critical method in protecting privacy and data confidentiality in big data analysis. This approach allows several different parties to cooperatively compute functions of their data without revealing the data of the other. MPC has been considered as an innovative approach which can solve security issues in the big data context due to the fast-growing data volumes and the requirement for preserving user privacy. There are diverse ways of performing MPC in big data analytics as outlined in this paper: Shamir's Secret Sharing, Homomorphic Encryption, and Garbled Circuits among others. In each technique is evaluated based on its applicability, effectiveness and rigidity in computation large data sets without compromising privacy. On one hand, Shamir's Secret Sharing includes flexibility and proven resistance to attacks, but, on the other hand, maybe lack scalability for big data of more than 2 dimensions. Homomorphic Encryption as the name implies enables the execution of computations on encrypted data but comes with the disadvantage of significant computational cost. Garbled Circuits is a secure approach to asynchronously invoke an evaluation function for any given function but it comes with the inherent challenge of complexity. This paper also examines some of the considerations that come with the use of the algorithm; some are computational complexity or more communication overhead, compatibility with other existing big data platforms. Solving these issues is only possible through improvements in cryptographic style and procedures and optimization methods. The final section of the paper discusses several directions of the future work, as well as the requirement of more efficient and applicable solutions for improving the applicability of MPC in BD. The result of this thesis targets at establishing a clear picture for integrating MPC into big Data systems for enhancing privacy and security over data in the present day's Big Data environment.

Keywords: Secure Multi-Party Computation, Big Data Analytics, Privacy Preservation, Cryptographic Techniques, Computational Efficiency.

1. INTRODUCTION

At the time when data is becoming the key to decision making and innovation, the protection of the privacy and confidentiality of individuals is highly critical. When it comes to big data analysis the major challenge which is experienced by organizations as well as individuals is that of security of data. This has paved way to develop Secure Multi Party Computation (MPC) as an effective solution where multiple parties are able to perform computations on their data in the presence of other parties without the disclosure of the inputs of the parties. Besides protecting people's data, it also allows the information to pass through multiple parties, which may have rival interests.

In other words, the core of MPC is the security of data and its absence of influence from various parties that can work on data-driven tasks simultaneously. Some of the challenges that arise when attempting to achieve data protection in giant data sets include the following -Traditional approaches to data protection prove ineffective in giant data sets; mainly because of the extensive analysis carried out in big data systems. To overcome these limitation, MPC enables the operations to be conducted directly on the encrypted data to reduce the exposure of sensitive data. Hence, it is evident that as big data continues to be a reality, having MPC integrated into data analytical pipelines becomes even more important for privacy and security.

1.1 Techniques of Secure Multi-Party Computation

Shamir's Secret Sharing:

Shamir's Secret Sharing is amongst the most basic methods used in secure multi-party computation. Also known as Shamir's method, this method originated from Adi Shamir in 1979, and requires the splitting of a secret into different shares that are to be given to the shareholders. It is worth underlining that no information about the secret is given through one of the shares; nevertheless, with the combination of all of them, the original data can be reconstructed. This approach also is simple and strong hence it can be applied in many different scenarios and with different parameters. However, its scalability may pose a problem especially when dealing with a high-dimensional data or large data set.

As was already mentioned, Shamir's Secret Sharing is one of the most easy to implement. The scheme makes provision for the number of shares called the threshold for reconstructing the secret. This is an effective approach since it creates a kind of threshold mechanism that serves to enhance security while at the same time providing usability. Although, it becomes somewhat problematic while scaling up for processing sophisticated analyzations or while getting amalgamated in to the existing big data architectures.

This paper also found that Shamir's Secret Sharing has a large overhead when performed repeatedly in an electronic transactions environment. The operations on shares and particularly their management may be complicated which in turn has an effect on the general drive and system utilization. Paradigm improvement is imperative in order to augment the applicability of this method for massive datasets.

Homomorphic Encryption:

Homomorphic Encryption is the type of cryptographic technique that would enable the computation of the original data to be performed on the encrypted form of it without necessarily decrypting the said data. This property allows executing data processing securely while at the same time protecting individuals' privacy. By the level of computation allowed, homomorphic encryption schemes can be categorized into partial homomorphic encryption, somewhat homomorphic encryption and fully homomorphic encryption. Arbitrary computation can be performed using Fully Homomorphic Encryption (FHE), but normally, it is highly time-consuming and resource demanding.

The main advantage of Homomorphic Encryption is the operations done on the encrypted data to ensure privacy during computation. This feature is especially worth it in cloud computing and outsourced data mining because the owner of the data does not want others to access and understand the data. However, in certain applications, concerning the computational overhead, FHE can be a major inconvenience, thus reducing it applicability in real-time data analysis.

Besides the performance, challenges are associated with extending the implementation of Homomorphic Encryption to the existing big data analytics platforms. The difficulty levels of both the encryption and decryption process can impacts efficiency of analytical work flows. The aforementioned limitations are being researched to improve homomorphic schemes and to devise application of homomorphic encryption with other privacy-preserving approaches.

Garbled Circuits:

Garbled Circuits is another technique of computing on encrypted data with multiple parties involved which was discovered by Andrew Yao in 1980s. It entails storing in a circuit a function to be computed, and enables other parties in computing the said function. The garbled circuit is constructed in such a way that output of the circuit only is visible while the internal values are concealed. This method provides flexibility in terms of the functions which can be computed securely and therefore is appropriate for a large number of applications.

Another advantage of itself is on computing generic functions with Garbled Circuits. This computation preview supports computation type and complex algorithms and protocols. However, by making use of the garbled circuits, there are a number of implementations that may be deeply entrenched, hence showing a daunting complexity when used in a real sense. One of the significant issues that arise when using this method in analysis of big data is the issue of security and computational power or speed.

However, there are some concerns with these Garbled Circuits to do with communication overhead and scalability. This may hinder the efficiency of the computation process since it may include the requirement of exchanging messages between the two or more parties by encrypting it. Further development is oriented on optimizing the function of garbled circuits and testing mixed models for increasing the applicability of such approach in large scale data processing.

1.2 Challenges in Implementing MPC

Computational Efficiency:

When it comes to the actual performance of Secure Multi-Party Computation, the major issue is to make it as efficient as possible. MPC techniques tend to include transactions that require lots of computational resources such as cryptography. These operations are computationally expensive and may result in negative effects on the actual performance of the data analytical pipelines mainly when dealing with big data sets or in real-time context.

As for the nature of the problem to be dealt with from the point of view of its computational efficiency, it is essential to mention developments in the cryptographic algorithms or optimisation methods. There are different strategies proposed in terms of reducing the amount of computation to be performed in MPC while still achieving the required reliability. For improving the efficiency of the MPC implementations, the possibilities of parallel processing, hardware acceleration, and sorting algorithms are currently under consideration.

However, the most important factor that one should consider while enhancing the computation rate is always the security/ performance ration. Hard sacrifices between the amount of security achieved and the amount of computation used must hence be made. The continuation of work in this field will require search for even more effective solutions for solving MPC problems that would take into account the challenges posed by big data.

Communication Overhead:

Another challenge that persist in Secure Multi-Party Computation is that of communication overhead. This need to exchange encrypted messages during the computation process is disadvantageous in terms of communication transacting costs and response time. There is overhead in using this structure based on the degree of distribution of the system; thus, the overhead can impact the data analysis efficiency especially when dealing with data networks where bandwidth and latency are key parameters.

Communication overhead can therefore be defined as the amount of communication done within a given MPC that is not directly required for computation or other useful operations in the MPC. Minimizing this, entails the optimization of the used communication protocols. To this end, some of the methods that are being considered include cutting down the number of rounds of communication and methods of compressing encrypted messages in an attempt to increase network efficiency. Communication strategies that must be put in place are a major factor that must be considered so as to enable the application of the MPC in the real-time data analysis scenarios.

Moreover, the interface of MPC with existing big data frameworks also pose the issue of communication needs to be address. It is therefore mandatory for compatibility and communication processes within these frameworks to be enhanced so as to achieve efficiency of data analysis.

Integration with Big Data Frameworks:

There are several difficulties arising from the fact that Integrating Secure Multi-Party Computation with existing big data frameworks. Most of the big data environments require the consumption of complex data processing pipelines as well as different technologies. Integrating MPC into such processes falls into the following general considerations to suit the needs of all the stakeholders involved and to be compatible as well as effective.

One limitation is the ability to show that MPC is feasible for current, popular big data packages such as Hadoop or Spark. The compatibility problems and the low performance have to be solved to allow integration. Scientists are paying efforts to create interfaces and middleware for integration of MPC into the existing data processing environments.

Also, the integration of MPC with big data frameworks has some concerns in terms of data concerns such as storage, management and processing. Another important consideration is to make sure that MPC techniques employed are capable of processing the amount and the type of big data as well as to protect privacy and security of the data. Current work includes the identification of techniques that would enable improvement of the integration of MPC to the big data infrastructure.

2. REVIEW OF WORKS

Secure Multi-Party Computation commonly called MPC or SMPC has emerged as an important tool of privacy-preserving data analytics. With an increasing use of data driven applications, the aspect of securely processing information that has to be shared with others has become very critical. This paper presents an analysis of the state of MPC, which explores several inventions within this approach and the employed methodologies along with the issues that have been reported in numerous fields of application and diverse areas such as genomic analysis, machine learning, finance, and so on. Focusing on the state-of-the-art and the challenges faced by researchers, we try to investigate recent work and systematic review in more detail.

Smith and Johnson (2019) present a detailed survey of the MPC techniques for privacy-preserving collaborative data analysis. They focus on the basic techniques like the Shamir's Secret Sharing and Homomorphic Encryption which are basic in conducting secure computations with different parties. With their review, they note that these techniques are useful in safeguarding data privacy as the data is jointly analyzed. For instance, Shamir's method splits data into shares, whereby no one can access the entire data; Homomorphic Encryption permits computation on encrypted data without decoding it.

Chen et al. (2018) also add to this discussion concerning the employment of MPC in different privacy-preserving data analytics solutions. Their survey inscribes a wide range of methods, explaining how various approaches are used to achieve privacy and performance trade-off. The survey brings out the need of this integration with new technologies in order to cater for scalability in large datasets.

Another great paper reviewed by Brown and Davis (2020) is focused on optimization of MPC methods that are specific to database genomic cooperation. Their study proposes modifications that help to reduce the high computational complexity of genomic data but at the same time ensuring privacy. They show how innovations in MPC methodologies can be employed to enhance the conduct of secure genomics through mitigating on overheads while enhancing efficiency.

Lee and Wang (2021) regional the use of MPC in collaborative machine learning with reference to the difficulties together with solutions related to these methods in the manner of machine learning. They indicate that their work shows that it is possible to apply MPC in order to further privacy in machine learning models, however, they also have acknowledged certain practical issues related to computational complexity and scalability.

Liu et al. (2022) present a critique of MPC methods utilized in cooperative work on financial data processing while focusing on the problem of computational complexity. Their review outline some challenges for instance, the high cost of computations involved in secure computations plus other related areas which can be enhanced to boost the current performances. They gave what they refer to as several strategies for efficiency such as better algorithms, and faster hardware implementations.

Following the same line of thought, Wang & Li (2019) also discuss the issue of computational efficiency when it comes to privacy preserving in collaborative data mining. It is noteworthy that they stress on the idea that increasing computational utility of MPC techniques inevitably results in a lower level of privacy. They also

consider different ways of optimizing these trade-offs so as to enhance the applicability of MPC in large-scale data mining.

While Zhang & Zhang (2020) take a closer look at the ways in which MPC techniques can be incorporated with the IoT data analysis frameworks. They discuss the difficulties associated with the integration of MPC into the mentioned IoT systems, for which the presence of compatibility and the presence of the effective means of communication, etc. As highlighted by their findings, there is need to come up with a hybrid solution that would allow for incorporation of MPC with IoT data analysis architectures.

In their recent work, Li et al. (2021) consider the coupling of MPC with collaborative recommender systems. Among the issues that are mentioned in their study, they focus on data management problems and incompatibility of the system and present solutions. Therefore, integrating MPC with recommender systems is central in ensuring the privacy of users while at the same time providing them with the recommendations they need.

Wang et al. (2019) provide a literature on the use of MPC in the analysis of joint healthcare data emphasizing on the opportunity it has in boosting privacy in medicine science. In their review, they highlight different AFC techniques and their ability to protect privacy-preserving health data as well as facilitate multi-party computation. It also covers some of the limitations of using MPC particularly in health care sectors including the issue of data complexity and regulatory constraints.

Chen et al. (2022) focus on MPC for collaborative fraud detection explaining a systematic review of the approaches applied to improve the financial security. Their review also highlights on the role of MPC in identifying fraud and malpractices with regard to protection of financial information. They also try to solve the problems related to extension of MPC in the financial area as well as integration with any security means.

In 2021, Huang et al., examine applying MPC in privacy-preserving natural language processing (NLP). They also show that MPC could allow secure applications of NLP tasks including sentiment analysis and text classification without the need to reveal sensitive data. They also talk about the most important issues of applying MPC to NLP such as the hardness due to computational complexity and the data privacy issue.

Yang et al. (2020) consider MPC for collaborative social network analysis, and more specifically – the privacy-preserving approaches to study social dynamics. This is underscored by their own study showing that MPC helps in preserving the user's privacy as well as facilitate teamwork in the analysis of the social network data. Strategies for issues concerning the data merging and the communication burden appear in integrating social network analysis applications.

3. PROPOSED METHODOLOGY

This methodology explains the strategy that will be utilized to study Secure Multi-Party Computation (MPC) methods and how they can be deployed in large datasets processing. The emphasis is on the systematic review of academic literature and the qualitative evaluation of MPC approaches toward the measurement of the strengths, weaknesses, and innovations in privacy-preserving data analytics applications. This type of research is ambitious and non-experimental in that it builds a comprehensive frame of reference for the analysis of MPC from previous studies and theory.

The first step is for the development of the literature review of the recent studies, reviews, and systematic surveys in the field of MPC. Includes: • Journal articles • Conference papers • Technical reports While searching for articles, only sources from peer reviewed, related scientific conferences, and technical reports shall be considered. The literature review will, therefore, detail several MPC techniques like Shamir's Secret Sharing, Homomorphic Encryption, and Garbled Circuits among others and their use in genomic analysis, machine learning, financial analysis, among others. Special attention will be paid to the applications of the described techniques, their effectiveness, and difficulties arising when being used in practice. This review shall therefore assist in laying the right groundwork to foster understanding of the state of the art in MPC.

3.1 Qualitative Analysis

After the literature review, the research study is to employ a qualitative synthesis that will involve integrating findings from the reviewed studies. In this exploration, the various approaches to MPC is going to be presented and the differences between those methods in terms of the efficiency of protecting the privacy of the participants and their ability to work collectively on data will be discussed. Issues like computation complexity, scalability, inter-partition communication cost, and the compatibility with other data planes will be compared. The findings of the studies will be grouped them according to the domains of application and general patterns and similarities will be looked at. In this case, this approach will assist in bringing out the effectiveness of different MPC techniques as well as their use in real-world applications.

3.2 Theoretical Framework

The last one includes creating a theoretical framework based on the findings in the literature review and the qualitative analysis. Bearing this in mind, this framework will define the primary objectives and parameters by which to measure MPC techniques in BD environments. Some of the factors that will be used include policies that respect user's privacy, computational capabilities, and integration with other databases. MPC can be used across different contexts and its feasibility and effectiveness will be evaluated within the scope of the theoretical framework that is going to be developed in the future. It will also assist in learning the shortcomings of the present literature and issues that have not been addressed adequately.

3.3 Synthesis and Recommendations

Thus, conclusions derived from the synthesis of the reviewed literature and the results of qualitative analysis will consist of the recommendations for the further research and utilisation of the MPC in BD analysis. This will involve pointing out approaching that can make MPC techniques more effective, and more scalable, how the integration can be done, and what other areas MPC should be applied to. The recommendations will be made on the understanding of the strengths and weaknesses provided on the MPC techniques and it will involve making recommendations to researchers and practitioners in the area. Such synthesis will help in the improvement of knowledge of MPC and its application in the boost of privacy and security when dealing with analyses of data.

4. RESULTS AND DISCUSSION

The conclusions of the current research are grounded on the theoretical review and qualitative analysis of Secure MPC strategies and their implementation in BDAs. The findings are as follows and are categorised under broad sub headings, which capture various dimensions of MPC as revealed under the research methodology above.

The findings of the literature review indicated that Shamir's Secret Sharing, Homomorphic Encryption as well as Garbled Circuits were the most popular techniques in MPC. Shamir's Secret-Sharing is specifically appreciated for the type of data partitioning it offers where the data set is divided into multiple shares and none holder has an access to the complete dataset. The other type of encryption is Homomorphic Encryption in which computations can be made on encrypted information and retains the privacy even while processing. The feasibility of using Garbled Circuits was established for executing safe function evaluations between parties. All the above methods have unique privacy-presuring benefits but they also consist of different computational complexity and efficiency.

The qualitative analysis reaffirmed the applicability and effectiveness of MPC techniques in contexts aimed at ensuring data privacy across rather sensitive domains including health care, finance, and genomics. All the studies documented in this analysis agreed that MPC techniques can effectively do computations for which they were programmed to do by efficiently computing the results without compromising the raw inputs of the participants. For instance, Brown and Davis (2020) had proven that MPC can effectively address data of genomic type, which is highly sensitive. There are actually, however, growing from the above, some risks of privacy leakage which depend on the used MPC technique and where some techniques seem to be more protective of privacy than others.

However, as the review showed, the computational efficiency is one of the notable issues concerning MPC techniques even if they are sufficiently suitable for privacy preservation. The analysis showed that, although certain optimizations have been implemented, e. g., those described by Liu et al. (2022) for financial analysis, the

addition of MPC still creates a significant burden, in terms of performance loss. Such methods as Homomorphic Encryption in this case are efficient in handling data, but they are usually time-consuming and need a higher computational ability. This challenge is particularly felt more in large data scale scenarios, thereby making the need for real time processing paramount.

Specifically, the findings reveal that the combination of MPC with extant data architectures is not without certain hurdles, most notably in areas such as compatibility and overhead of signaling. Specificly, Zhang and Zhang (2020) pointed out several challenges in integrating MPC into IoT data processing; firstly, the challenges arise from the communication protocols that require addressing the overhead caused by the secure computation. In the same vein, Li et al., (2021) noted that data management in multiple systems in collaborative recommend systems was challenging when considering security measures. Such issues indicate that although MPC provides significant levels of privacy enhancements, the integration of MPC into well-established frameworks needs further analysis and may involve the creation of new medium-advanced approaches.

In other related areas of specialization like the health sector, finance and social network analysis, the use of MPC has been proved to have potential benefits. Wang et al. (2019) discussed that MPC is rather promising for heath care and large datasets where privacy is critical. That is why, for instance, Chen et al. (2022) explored how MPC could improve fraud identification in financial frameworks while preserving the privacy of information. However, the above findings indicate that the effect of MPC is not equal across domains with sectors such as the health sector implementing the technology more because of issues of privacy. For instance, while social network analysis as discussed by Yang et al. (2020) are still in their infancy when it comes to making use of MPC mainly due to the technicalities involved when working MPC on big, dynamic datasets.

Therefore, based on the findings of this study, MPC offers scalability and shown robustness for privacy preservation in different domains, although there is a long way to go before its practical adoption solves the problem of computational overhead for massive integration with the existing data systems.

5. CONCLUSION

Secure Multi Party Computation (MPC) is already gradually becoming the primary approach for Private Information Retrieval especially in the health sector, finance and genomics. Methods like Shamir's Secret Sharing, Homomorphic Encryption as well as Garbled Circuits guarantee the privacy of the computation by making sure that no participant has a full access to the data set being shared. However, as it has been pointed out earlier MPC has certain limitations and that include mainly computational issues and compatibility with current data structures. Some of its major challenges include the high computational overhead accorded to techniques like Homomorphic Encryption and the challenges that exist in integrating MPC into present systems especially within IoT and the collaborative recommender systems. Fields that demand high privacy requirements have adopted MPC, though other domains seem to be discovering its applicability, therefore requiring differentiated approaches. To overcoming these challenges and to stimulate the development of specific domain solutions, involvement will be crucial for the further extension of MPC's applications in different fields and becoming the basis for multiple secure data-driven applications.

REFERENCES

[1]. Smith, J., & Johnson, A. (2019). Secure Multi-Party Computation for PrivacyPreserving Collaborative Data Analysis. Journal of Privacy and Security, 15(2), 123- 145.

[2]. Brown, M., & Davis, R. (2020). Efficient Secure Multi-Party Computation for Collaborative Genomic Analysis. Journal of Bioinformatics and Computational Biology, 18(3), 235-257.

[3]. Lee, H., & Wang, S. (2021). Secure Multi-Party Computation for Collaborative Machine Learning: Challenges and Solutions. IEEE Transactions on Knowledge and Data Engineering, 33(8), 1234-1256.

[4]. Chen, L., et al. (2018). Privacy-Preserving Data Analytics using Secure Multi-Party Computation: A Survey. ACM Computing Surveys, 51(3), 1-35.

[5]. Liu, X., et al. (2022). Secure Multi-Party Computation for Collaborative Financial Analysis: A Systematic Review. Journal of Financial Data Science, 2(1), 45-68.

[6]. Wang, Y., & Li, Q. (2019). Privacy-Preserving Collaborative Data Mining using Secure Multi-Party Computation. Data Mining and Knowledge Discovery, 33(4), 789-813.

[7]. Zhang, W., & Zhang, L. (2020). Secure Multi-Party Computation for Collaborative Internet of Things Data Analysis. IEEE Internet of Things Journal, 7(5), 3789-3807.

[8]. Li, X., et al. (2021). Efficient Secure Multi-Party Computation for Collaborative Recommender Systems. ACM Transactions on Information Systems, 39(4), 1-28.

[9]. Wang, L., et al. (2019). Secure Multi-Party Computation for Collaborative Healthcare Data Analysis: A Review. Journal of Biomedical Informatics, 92, 103148.

[10]. Yang, C., et al. (2020). Privacy-Preserving Collaborative Social Network Analysis using Secure Multi-Party Computation. Social Network Analysis and Mining, 10(1), 1- 22.

[11]. Chen, Z., et al. (2022). Secure Multi-Party Computation for Collaborative Fraud Detection: A Systematic Review. Journal of Financial Crime, 29(2), 345-367.

[12]. Huang, Y., et al. (2021). Privacy-Preserving Collaborative Natural Language Processing using Secure Multi-Party Computation. Journal of Artificial Intelligence Research, 70, 965-988.

[13]. Zhou, Q., & Chen, Y. (2019). Secure Multi-Party Computation for Collaborative Traffic Analysis: Challenges and Solutions. Transportation Research Part C: Emerging Technologies, 104, 301-320.

[14]. Xu, Y., et al. (2020). Efficient Secure Multi-Party Computation for Collaborative Energy Consumption Analysis. IEEE Transactions on Smart Grid, 11(4), 3000-3012.

[15]. Liu, Z., et al. (2021). Secure Multi-Party Computation for Collaborative Video Surveillance Analysis. IEEE Transactions on Circuits and Systems for Video Technology, 31(8), 3146-3159.

[16]. Banerjee, S., & Mondal, A. C. (2023). An intelligent approach to reducing plant disease and enhancing productivity using machine learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 250-262. doi:10.17762/ijritcc.v11i3.6344

[17]. Al-Rawe, Y. H. A., & Naimi, S. (2023). Project construction risk estimation in iraq based on delphi, RII, spearman's rank correlation coefficient (DRS) using machine learning. International Journal of Intelligent Systems and Applications in Engineering, 11(5s), 335-342. Retrieved from www.scopus.com

[18]. Esposito, M., Kowalska, A., Hansen, A., Rodríguez, M., & Santos, M. Optimizing Resource Allocation in Engineering Management with Machine Learning. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/115

[19]. Ahammad, D. S. H. ., & Yathiraju, D. . (2021). Maternity Risk Prediction Using IOT Module with Wearable Sensor and Deep Learning Based Feature Extraction and Classification Technique. Research Journal of Computer Systems and Engineering, 2(1), 40:45. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/19

[20]. Mondal , D. (2021). Green Channel Roi Estimation in The Ovarian Diseases Classification with The Machine Learning Model . Machine Learning Applications in Engineering Education and Management, 1(1), 07–12.