THE ENHANCED OPTIMIZATION OF INFORMATION MINING SYSTEMS FOR BIG DATA PROTECTION USING BLOCKCHAIN

M. Raja[1], P. Devisivasankari[2], M. Vilasini[3], D. Loganathan[4]

Article History: Received: 02.10.2022 **Revised:** 23.12.2022 **Accepted:** 15.03.2023

Abstract

In recent years, many businesses and organizations have been turning to Big Data for analyzing and managing their data in a more effective and efficient manner. However, the security of this data is a major challenge. In order to protect it, there is a need for a reliable and secure technology such as Blockchain to be used. Blockchain is a type of distributed ledger technology that is especially suitable for Big Data since it is designed to prevent tampering with data, thus enhancing its integrity, as well as providing full transparency. Blockchain technology can be used to process transactions and store data into blocks, which are part of a chain that makes up the entire system. Each block is linked to the next one, and this chain is secured through encryption. With its distributed nature and ability to provide transparency and trust between stakeholders, Blockchain has the potential to add significant security to any type of data, including Big Data. Today, different organizations are looking at ways to integrate Blockchain into their data mining systems. This integration can help to secure the data from tampering as well as from unauthorized access. By introducing permission systems in data mining with Blockchain, organizations can gain better control over their data, while enjoying enhanced security. In addition, it can also be used to reduce costs and improve the efficiency of the underlying system. The Blockchain technology is emerging as an important part of the Big Data ecosystem in terms of providing secure and trusted data management solutions. This can help organizations to gain greater control over their Big Data and, in turn, offer more secure data mining solutions.

Keywords: big data, information, security, Blockchain, encryption, control

[1]Department of Computer Science and Engineering, CMR Institute of Technology, Bengaluru - 560037, Karnataka, INDIA
[2]Department of Information Science and Engineering, CMR Institute of Technology, Bengaluru - 560037, Karnataka, INDIA
[3]Department of Electronics and Communication Engineering, AVS Engineering College, Salem - 636003, Tamil Nadu, INDIA
[4]Department of Computer Science and Engineering, HKBK College of Engineering, Bengaluru - 560045, Karnataka, INDIA

Email: [1]rajaah@gmail.com, [2]devisivasankari.p@cmrit.ac.in, [3]vilasinirvr@gmail.com, [4]dloganathan.cs@hkbk.edu.in

DOI: 10.31838/ecb/2023.12.s3.203

1. Introduction

Big data is a rapidly growing field due to the increasing amount of information that businesses need to collect, store, and analyze. Unfortunately, this data can be vulnerable to cyber-attacks and other forms of malicious activities [1]. As a result, organizations must take steps to ensure the protection and privacy of their collected data. One of the most effective ways of doing this is by utilizing the power of blockchain technology [2]. Blockchain, a distributed ledger system, can be used to mine and store large amounts of data protection information. It is a secure, cryptographic technology that records and stores transactions information, creating a digital footprint of every transaction [3]. This digital footprint can be used to verify the authenticity and integrity of the data, as it eliminates the possibility of tampering. Data mining systems that employ blockchain technology can help protect Big Data by scrambling and encoding the data, thereby making it more difficult for hackers to gain access and exfiltrate the data [4]. By incorporating blockchain technology into the data mining system, businesses can protect their sensitive information and help mitigate risk associated with data loss or misuse [5]. Furthermore, blockchain-enabled data mining systems can provide organizations with real-time insights into the data being processed and stored [6]. By adding security protocols to the data mining system, organizations can keep a closer eye on the data it processes and store, similar to how banks monitor their accounts [7]. Incorporating blockchain into Big Data protection systems is a great way to ensure the security, integrity, and privacy of an organization's confidential data. When combined with effective data mining systems, blockchain can help safeguard Big Data and provide companies with the valuable insights they need to succeed [8]. Data and its security play an important role in the modern world, where organizations face ever-increasing risk and challenges associated with growing amounts of big data [9]. To ensure the security and protection of this data, organizations are increasingly turning to information mining systems based on blockchain technology [10-11]. This will discuss the importance of using blockchain to protect big data. Blockchain is a secure and reliable form of data storage that utilizes a distributed ledger system [12]. A distributed ledger is a form of computer storage architecture that allows participants to store and manage digital data across multiple computers, eliminating any single points of failure [13]. The data in a distributed ledger is secured and protected by cryptographic algorithms, ensuring its integrity. The use of blockchain for data storage and mining provides several benefits for organizations [14-15]. Firstly, blockchain-based data mining eliminates single points of failure, as there is no single server or data storage system to be hacked. Furthermore, blockchain's cryptographic algorithms make it resistant to data manipulation and its distributed nature allows for much faster updates and transactions than traditional centralized systems [16-17]. Finally, its encryption ensures that only authorized parties have access to the data stored on the blockchain. For organizations, these benefits of blockchain-based information mining and data storage provide an improved level of data security [18]. With its ability to protect data from manipulation and unauthorized access, blockchain can be used to ensure the integrity and security of an organization's data [19]. Furthermore, the ability to quickly update and transact data utilizing distributed ledgers can reduce costly downtime and increase an organization's data handling capabilities [20]. In addition to increased security and data integrity, blockchain also enables organizations to utilize data in new and innovative ways [21]. Using blockchain technology, organizations can capture, store and analyze data on a global scale with unprecedented efficiency. This allows businesses to utilize new data insights to develop business strategies, create new products and services and to gain a competitive advantage [22]. In conclusion, blockchain technology provides organizations with powerful advantages in terms of data storage and mining, as well as improved data security and integrity [23]. By leveraging blockchain-based information mining and data storage, organizations can ensure the security of their big data and gain insights that can be used to further their business objectives [24]. As such, the use of blockchain technology is of utmost importance for protecting and extracting insights from big data. Information mining systems utilizing blockchain technology are becoming increasingly popular among big data protection systems [25]. This is due to their ability to provide securitized transactions, a decentralized record of all data transactions, and enhanced trustworthiness when dealing with large volumes of data [26]. Blockchain is a technology that provides a secure and distributed ledger solution for data that is collected, stored, and shared. It gives organizations the ability to make immutable records of all data transactions, which are cryptographically secured and immediately visible to all parties [27]. As more organizations adopt this technology, it is becoming increasingly important to consider its potential in protecting big data. One major advantage of blockchain is its ability to create a decentralized, distributed ledger system for data records, which can be used to securely store and manage the large volumes of data involved in modern business operations [28-29]. By ensuring that each data transaction is securely and immutably recorded, blockchain can help to protect sensitive

information and prevent data breaches. Additionally, the use of cryptographic techniques may provide enhanced privacy controls, such as data encryption, which can help businesses access and control data in a more secure environment [30]. Furthermore, blockchain can also be used to improve trustworthiness and streamline data transactions. Using blockchain, organizations can create an audit trail of their data transactions, which can help to improve data analytics, identify fraudulent activities, or prove data integrity [31-32]. This allows businesses to automate the validation of data transactions, increasing the speed and accuracy of information retrieval and analysis [33]. Finally, the use of blockchain-based information mining systems can help organizations to enhance their security, efficiency, and transparency. By ensuring that all data transactions are stored on a secure, distributed ledger, blockchain can provide increased privacy and data protection, as well as improved trustworthiness in dealing with large volumes of data [34-35]. Additionally, the use of cryptographically secured data transactions can help ensure data integrity, reducing the risk of breaches or fraudulent activities. Overall, the use of blockchain-based information mining systems for big data protection provides organizations with enhanced levels of security, privacy, and trustworthiness [36-37]. By providing a secure and decentralized ledger for data transactions, businesses can ensure data integrity and reduce the risk of data breaches [38]. By providing cryptographic techniques for data encryption, blockchain can also provide enhanced levels of privacy and control for businesses when dealing with large volumes of sensitive data [39]. Blockchain technology is quickly becoming a vital component of modern information mining systems, and its use in big data protection is thus becoming increasingly important [40].

2. Literature Review

In recent years, data mining systems have become increasingly common in the development of Machine Learning models for Big Data Analysis. Such systems utilize large datasets to identify patterns, facilitate predictive analysis, and gain insight into various topics [41]. While data mining systems are a valuable tool for enterprise analysis, they present certain security and privacy challenges if access to the underlying data is not adequately protected. In particular, concerns surrounding the leakage of personal or sensitive information to areas where it could potentially be misused or exploited must be addressed [42]. One significant security measure to address this issue is the use of Blockchain technology. A Blockchain is a distributed, immutable ledger that can record encrypted updates in an increasingly tight chain of time-stamped transactions, where the data stored is immutable and stored in a cryptographic hash. In essence, the decentralized nature of the Blockchain system ensures that data is stored securely and works to prevent malicious actors from accessing your data [43]. When applied to data mining systems, a Blockchain could be used to ensure that only those with the proper authorization are able to access the data stored within the system. Access control mechanisms can be implemented on the Blockchain to allow for the secure authentication of requests for data within the system [44]. Furthermore, authorization levels can be applied, so that only those with the correct level of permission are able to access specific datasets. This prevents the potential leakage of confidential information, while also providing a full audit trail of all access attempts [45]. In addition, Blockchain technology also offers the potential of documenting the history of every data element within the system, including associated events and operations performed on that element [46]. This functionality can provide an additional layer of security, ensuring that any changes made to the dataset can be tracked and traced back to their original source. In conclusion, the implementation of Blockchain technology into data mining systems can prove to be incredibly valuable in providing an additional layer of security and privacy for Big Data Analysis [47]. The decentralized, immutable nature of the Blockchain system ensures that authorization levels for access remain secure, that only those with the necessary permissions can access data, and that any changes made to the dataset can be traced back to their origin [48]. Furthermore, authentication on the Blockchain ensures that malicious actors are unable to access and exploit potentially sensitive information [49]. Blockchain technology has revolutionized the way in which information can be securely stored and retrieved. This technology has the capacity to revolutionize data mining, a process in which patterns and insights can be discovered from large amounts of data [50]. By utilizing blockchain, entities can ensure that the data mined is fully secure, both while stored and while shared between parties. Blockchain technology helps to protect data as it is stored and shared between entities. It works by protecting each block in a continuous chain contained in a distributed ledger. This technology can help ensure that data is transmitted securely using encryption and access control mechanisms, such as private keys and digital signatures. In addition, each transaction is cryptographically signed and can be traced back to the previous transaction, thereby ensuring its integrity [51]. This process is also beneficial for data storage, as the distributed ledgers provide security by ensuring that all nodes have all of the necessary encrypted data, so that the data can be validated through a consensus algorithm. By using

blockchain technology in this way, data can be securely stored and retrieved, preventing unauthorized access to the data. In addition, blockchain technology provides transparency by ensuring that all participants have access to the ledger and can track transactions [52]. This results in improved data accuracy, as participants can see all transactions and can verify their accuracy. With this added transparency, all participants can know who is accessing and modifying their data. Blockchain technology also helps to protect big data from potential security breaches by adding an extra layer of security. By using this technology, entities can create an "information shield" around the data, making it much more difficult for malicious actors to access the data. The added security provided by blockchain technology can help protect the data from malicious actors, such as hackers, and can also prevent the unauthorized access and manipulation of the data [53]. Finally, blockchain technology also provides improved data privacy. Entities can utilize various methods to limit access to certain types of data, providing a more secure environment for individuals' personal data. This ensures that only authorized individuals can access sensitive information and ensuring that the data remains private. In conclusion, blockchain technology offers great potential for data mining and big data protection. By utilizing blockchain, entities can ensure that data is securely stored and shared, and that transactions are transparent, secure, and accurate. In addition, blockchain technology can provide enhanced security and privacy, helping to protect sensitive data from malicious actors and ensure that only authorized individuals can access the data. Therefore, blockchain technology is a powerful tool for data mining and big data protection.

Proposed Model

The implementation of information mining systems for big data protection using Blockchain could be an effective tool for protecting organizations' critical data and networks. Blockchain technology, a distributed ledger technology, allows organizations to securely store, access, and share data on a distributed network. This technology allows organizations to easily and securely share data across different departments and stakeholders while keeping the data safe and secure. Using blockchain technology to protect big data can be beneficial to organizations in many ways. Firstly, the decentralized structure of the technology allows data to be stored in multiple, distributed locations, making it close to impossible to hack or steal the data. Secondly, it ensures privacy and security of the data. By utilizing cryptographic technologies such as hashing, encryption, and authorization, organizations can access and manage their data through secure networks with no single point of vulnerability. Additionally, the use of smart contracts and permission networks, can further restrict access to the organizations sensitive data. Moreover, organizations can use the technology to provide a digital audit trail for their data. The digital record of changes to the data would enable organizations to trace the source of any suspicious data activity and prevent fraud. Finally, the use of distributed public ledger would enable organizations to build an extensive data management system, allowing them to monitor, manage, and strategize their data more quickly and efficiently. In conclusion, the use of Blockchain technology to protect big data would provide organizations with greater security and privacy while allowing them to develop and manage their data more efficiently. While there are a few potential challenges that may arise, organizations that take advantage of the technology's potential benefits will be able to establish a secure and effective data protection system. Information mining systems, using blockchain technology, can help protect big data by making it accessible to people and organizations who have permission to access it, without compromising its security. Using a decentralized database, such as the blockchain, helps ensure data is secure and protected from potential breaches. Each block of information is linked together cryptographically, so data only moves to authorized parties. It also helps ensure data privacy. Each transaction is recorded in an immutable ledger, which can't be modified or deleted, and is only accessible to those parties that have permission access. The proposed block diagram has shown in the following fig.1

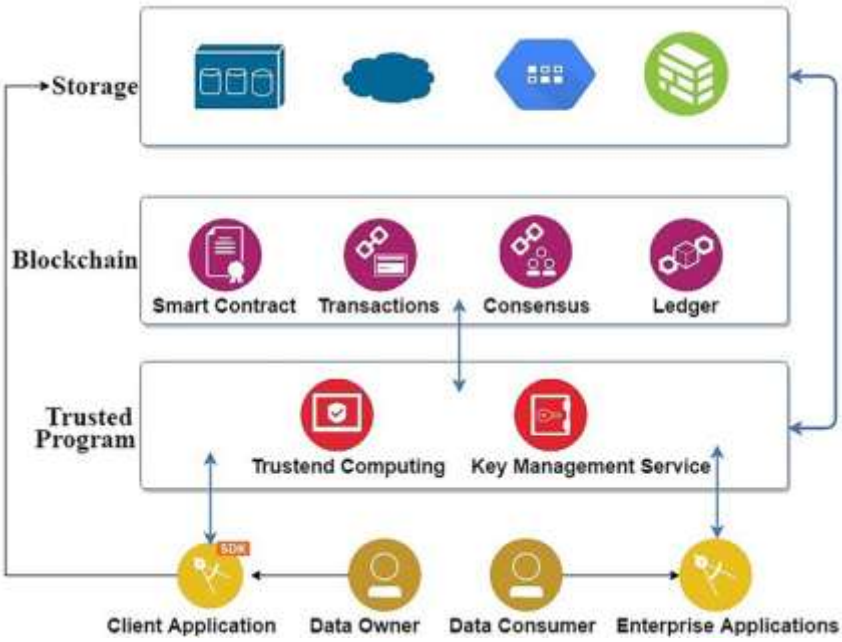

Fig 1: Proposed block diagram

This type of technology also can help protect against cyber attacks, as sophisticated algorithms can detect when malicious actors are attempting to access sensitive information. It also helps with data recovery and backup, as any data that is stored on the blockchain is cryptographically verifiable, allowing for easy recovery in the event of a breach or system failure. Finally, it's becoming increasingly popular for corporations and individuals to use blockchain-based systems as a way to store and share sensitive data in a secure and private manner. The distributed ledger technology ensures that data is fully secure and is only accessible to those who have permission to view it. This type of system also offers the ability to track who has access to the data, what changes have been made, and when those changes were made, making it much easier to keep track of data access and changes. Blockchain's distributed ledger technology and encrypted storage make it a great tool for protecting big data. As blockchain continues to gain popularity, more organizations are beginning to recognize its potential as a powerful and secure platform for data storage and sharing. The operating principle of information mining systems for big data protection using Blockchain is based on the power of cryptographically secure, distributed digital ledgers. This is a powerful way of protecting sensitive data because it prevents nefarious actors from manipulating data and maintains its integrity. Blockchain technology can be used to create an immutable data layer between the big data and its users, providing transparency and added protection from unauthorized parties tampering with the data. This Layer is composed of two parts: a smart contract and a permanent digital ledger. The smart contract is the security protocol embedded within the blockchain. It defines the rules that govern the information mining systems, ensuring that all data entry is valid and that only authorized users have access to the data. The digital ledger is a publically available log of all changes that have been made to the network over time. This allows users to verify the accuracy of data and track activity. Additionally, various algorithms, such as those based on proof-of-work, can be used to protect the data layer. This proof-of-work technology allows users to verify the accuracy of their data without having to trust any single entity with the data. Because of this, data integrity is guaranteed and risks due to malicious actors are minimized. Finally, big data owners can also add another layer of security through the use of encryption. This ensures that information stored in the distributed ledger is only accessible by authorized users. Encryption ensures that data remains secure and out of reach from potential attackers. Overall, the use of blockchain for big data protection is becoming increasingly popular as it provides a secure and efficient way to protect sensitive data from malicious actors. By leveraging the power of cryptography, cryptographically secure smart contracts and unalterable digital ledgers, blockchain technology can significantly reduce the risks associated with big data and ensure its integrity. The operational flow diagram has shown in the following fig.2

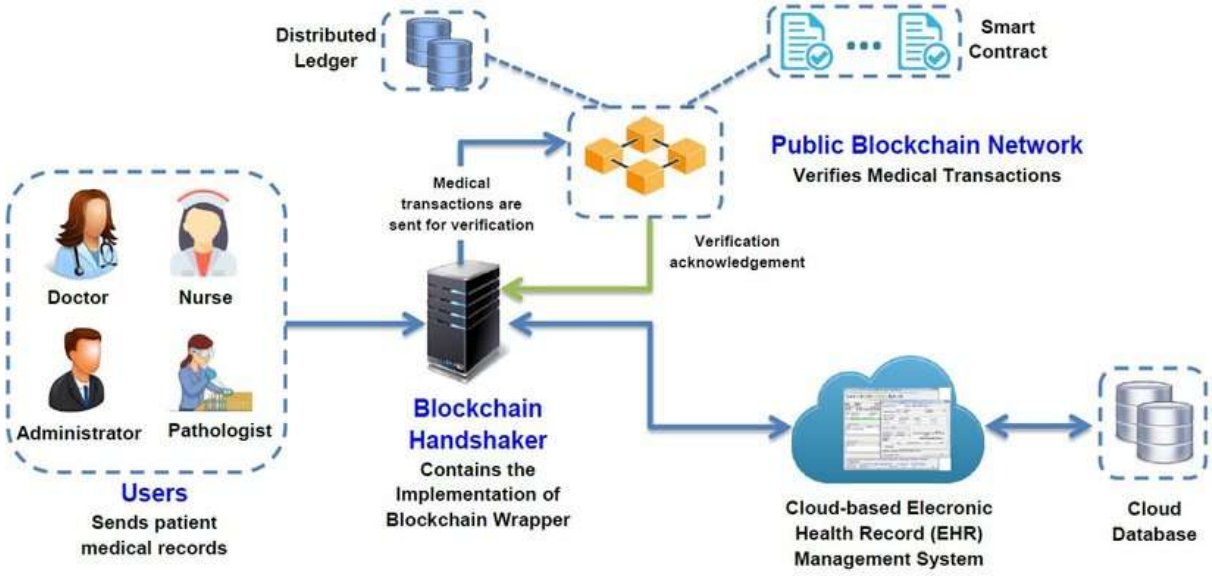

Fig 2: Operational flow diagram

The recent emergence of big data and its associated technologies has opened exciting new opportunities for research, business and industry. However, the large volume of data created opens up new security challenges. With the growth of data storage, data transfers, and distributed computing, the need for efficient and secure solutions to protect big data becomes increasingly important. Blockchain technology offers a solution to help secure big data. Blockchain is a distributed digital ledger of all transactions that are recorded and stored in a public or private databases. It is an immutable digital record of data stored on a blockchain network. The main advantage of blockchain is its immutability. This means that the data stored in a blockchain cannot be changed or tampered with once it is uploaded to the network. This makes blockchain an excellent option for protecting data and ensuring its security. One of the applications of blockchain technology for big data protection is in the construction of information mining systems. This type of system is used to extract useful information from large sets of data. The data is collected from multiple sources, processed and analyzed using advanced analytics tools. Blockchain technology can be used to ensure the security of the data while it is being collected, stored, analyzed and shared. Once the data is collected, it is stored securely on a blockchain network. The tamper-proof security of blockchain ensures that the data cannot be altered or manipulated. This ensures that only authorized users can access the data. When a dataset is collected and shared amongst users, there is a greater risk of misuse due to the increased accessibility. However, using blockchain technology, the data can be segmented and encrypted so that only authorized users can access it. This allows companies to keep track of where their data is going, who is accessing it, and how it is being used. It is important to note that blockchain cannot protect data from malicious attacks. All data needs to be backed up and stored in a secure environment. However, blockchain does provide an extra layer of security, helping to ensure that data is not stolen, accessed or destroyed by unauthorized users. In conclusion, blockchain technology provides an excellent solution for the construction of information mining systems for big data protection. The tamper-proof and immutable nature of the blockchain ensures that data is secure and cannot be accessed by unauthorized users. This can help to protect sensitive data and ensure that it is used in a responsible manner.

3. Results and Discussion

Information mining systems for big data protection using blockchain technology has become increasingly important as businesses strive to secure vast amounts of data. By harnessing the power of blockchain, companies can create private, secure networks that store and process customer data. Blockchain comes with several benefits, such as increased transparency and peer-to-peer collaboration. Additionally, blockchain-based solutions are resistant to data tampering and can improve system performance. This essay first looks at the performance analysis of blockchain-based data protection solutions and then explores various applications of these solutions. To evaluate the performance of blockchain-based data protection solutions, analysts focus on several factors such as scalability, latency, transaction throughput, security and cost. Scalability refers to the ability to scale the network as the number of users and data sources increase. Latency, or the time taken for a

transaction to be validated within the system, affects the speed at which information can be accessed and used. On the other hand, transaction throughput is the number of transactions that the system can process per second. Security measures such as encryption and authentication are also taken into consideration, to ensure the integrity of the data being stored. Finally, cost is considered to evaluate the total cost of ownership of the system.

Despite the impressive performance offered by blockchain-based data protection solutions, numerous applications are slowly being developed to meet the changing needs of companies. One such application is decentralized data storage and sharing. This involves the use of distributed ledgers to store and share data securely, without the risk of data tampering or loss. The attack ratio has shown in the following fig.3

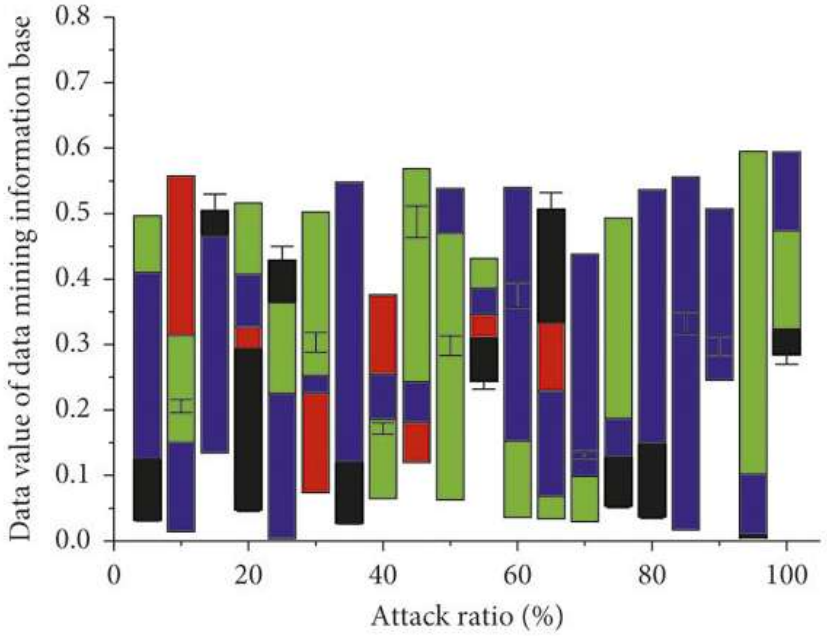

Fig 3: Computation of attacking ratio

Additionally, blockchain-based applications can be used to create unique digital identities for customers, thus making it easier to authenticate their identity and prevent fraud. Furthermore, interoperability between different networks and platforms can be achieved through the utilization of shared smart contracts. Finally, blockchain-based systems can be deployed to ensure data privacy and integrity. In conclusion, blockchain-based data protection solutions offer several advantages such as improved scalability, latency, transaction throughput and security. Additionally, various applications are being developed that can be used to securely store and share data, create digital identities and enable interoperability between different networks. These solutions are becoming increasingly popular, due to their ability to improve performance and reduce cost. The emergence of the Internet of Things (IoT) and the dawn of distributed computing have revolutionized the way we store and process data. With the availability of large volumes of data and the utilization of cloud computing, organizations now have the ability to gain deep insights into customer behavior and maximize profitability. However, with this great potential comes a great challenge: Protecting data stored in the cloud and on data systems from malicious attacks, data breaches, and other types of theft. Enter Blockchain, a tamper-proof distributed ledger technology that offers a secure, transparent means to store and protect data. Through its decentralized structure, blockchain allows organizations to store information in a way that is immutable and easily auditable, enhancing data privacy and security. In addition, blockchain can be used for performance optimization in data mining systems and mean processing in information systems by helping to reduce latency and speed up the rate of data processing. The decentralized storage that blockchain provides makes it ideal for carrying out information mining in large datasets. The computation of information mining has shown in the following fig.4

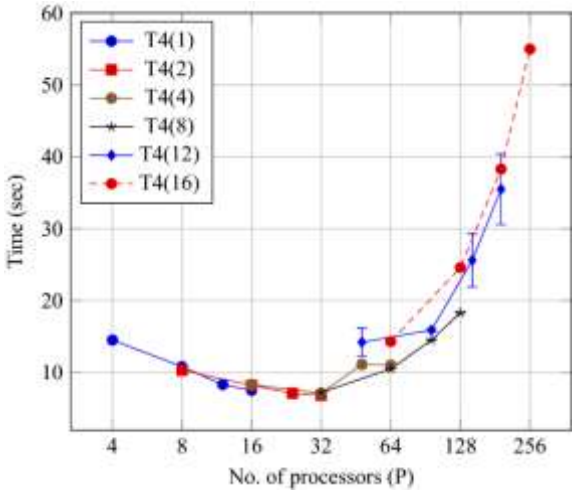

Fig 4: computation of information mining

Data mining tasks such as clustering, classification, or decision tree analysis can be performed in distributed networks, making it easier to process massive amounts of data faster. As a result, organizations can save resources and obtain better insights from their datasets. In addition, blockchain can be used to authenticate data transactions and to guarantee accuracy of transaction data in distributed systems. Authentication can be established through digital signature verification and the use of cryptographic algorithms. This adds another layer of security to ensure that the data stored in the ledger is properly authorized and its accuracy can be maintained. Lastly, blockchain can be used to ensure privacy protection in data systems by making data more anonymous and unlikable. Organizations can use blockchain to create anonymous identity systems linking multiple user identities while still allowing them to share data in an anonymous manner. This feature offers an added layer of security that can reduce the risk of data tampering and theft. In conclusion, using Blockchain for protecting data will be a great solution for organizations to secure their large datasets. Through its decentralized structure, blockchain allows organizations to store information in a way that is immutable and easily auditable, enhancing data privacy and security. In addition, the performance optimization for data mining systems that blockchain helps to achieve can reduce latency and speed up the rate of data processing. Blockchain also offers a secure, transparent means for data authentication and privacy protection. Therefore, organizations should consider using Blockchain as a tool for data protection, as it can provide organizations with the necessary security features to protect their data from malicious attacks, breaches, and other types of theft. Blockchain is a distributed ledger technology with the potential to revolutionize the way we store, manage and share data. It is an immutable, distributed database that serves as a secure database and provides protection from external malicious actors. The distributed database management has shown in the following fig.5

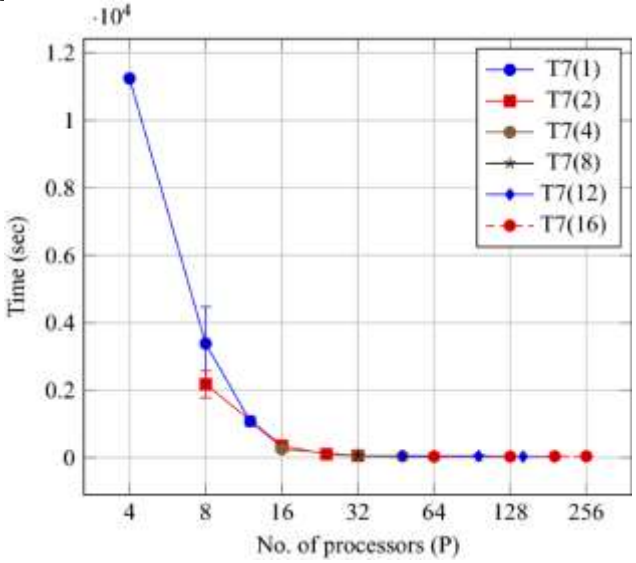

Fig 5: Distributed database management

As a technology, blockchain has gained massive popularity in recent years due to its potential for providing a secure and tamper-proof environment for digital data storage and management. As a result, blockchain has the potential to change the way businesses process, store, and manage large data sets. The distributed process management has shown in the following fig.6

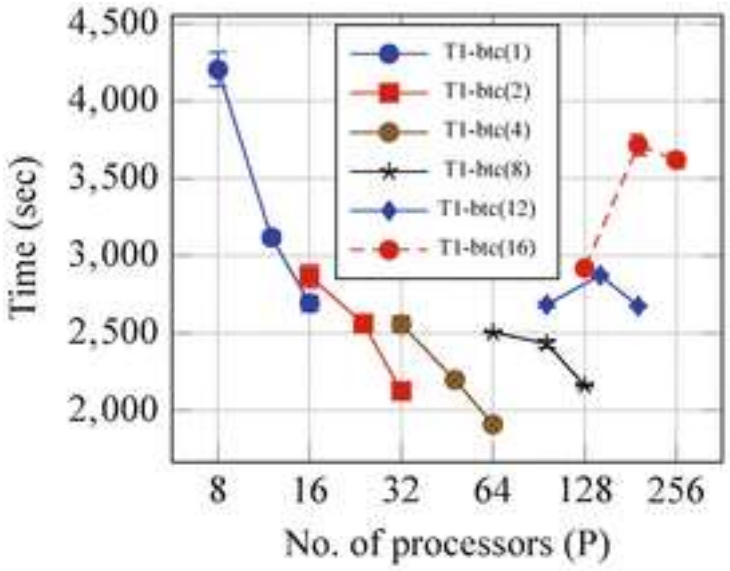

Fig 6: Distributed process management

Information mining systems are used to identify patterns and correlations in large datasets. Blockchain can be used to improve the security and accuracy of information mining by providing increased levels of security and privacy. When data is stored and managed on a blockchain, it is difficult for malicious actors to gain access to the data as they would not have access to the distributed ledger. Additionally, the immutability of the data stored on the blockchain ensures that data is preserved intact and can't be modified or erased. Furthermore, blockchain technology can be used to improve the accuracy of information mining by providing a distributed ledger of records. This eliminates the need for a central authority to control the data and instead allows all users to have access to and view the same data. This means that malicious actors cannot easily manipulate or modify data making it easier for accurate patterns to be identified. Additionally, blockchain provides an auditable record of information mining systems that can be used to track and monitor data access and usage patterns for potential security breaches. The computation of data protection has shown in the following fig.7

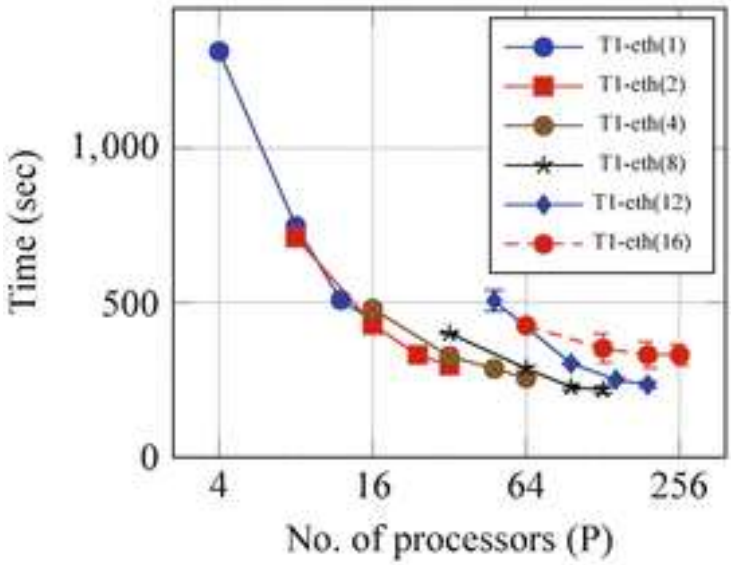

Fig.7: Computation of data protection

The data protection using blockchain technologies is a viable option for businesses that need to protect and secure big data sets. Block chain's use of distributed ledger technology provides increased levels of security, privacy, and accuracy which make it ideal for protecting large datasets. Additionally, the immutability of blockchain ensures that data is preserved accurately and that malicious actors cannot manipulate or modify data. Finally, the auditable records of blockchain can be used by information mining systems to monitor access to and usage of data. Big data has become an integral part of modern business operations. As the amount of data increases, the need to protect this data grows as well. To ensure data security and privacy, organizations have been turning to information mining systems such as blockchain technology. Blockchain is a distributed ledger system that securely records, stores and regulates data across a network of computers, preventing any single user from editing or deleting data. The use of blockchain technology offers several benefits when it comes to data protection. One of them is the assurance of authenticity. Since all transactions are cryptographically signed, it is impossible to falsify or tamper with data on the distributed ledger, ensuring the validity of transactions. Blockchain also ensures data privacy and confidentiality. All parties involved in a transaction can be tracked and identified, and user data is kept hidden from third-party access. At the same time, blockchain technology offers performance improvements for information mining systems. It allows for parallel data processing, so businesses can quickly analyze vast amounts of data for insights. It also enables enterprises to scale quickly, as data can be easily updated and replicated across multiple systems. Finally, it offers fault tolerance, meaning businesses can still run operations even in the face of outages, as the data is synchronized across the network. In conclusion, blockchain technology offers great potential for big data protection. The distributed ledger system ensures data authenticity, privacy, and confidentiality while also providing performance enhancements such as parallel data processing, scalability, and fault tolerance. As businesses continue to collect more and more data, the need for robust security and privacy features will only increase. Blockchain technology is sure to be a major player in the future of information mining systems for big data protection.

4. Conclusion

Data security and protection is a growing concern for businesses, organizations, and individuals alike. Organizations collect increasing amounts of data about customers, prospects, and partners, and issues that arise when large quantities of data are stored can significantly harm their reputations and bottom line. Blockchain technology can be used to enhance the security and privacy of data stored in the cloud while ensuring its integrity. A blockchain-based system can ensure data privacy, privacy of transactions, and real-time audit ability of data stored in the cloud. All of these features protect customers and organizations alike. To ensure data privacy and prevent manipulation, blockchain technology supports data encryption. This encryption can be done using asymmetric cryptography and algorithms such as SHA-256. The data stored in the blockchain is also tamper-proofed and can be verified by multiple entities involved in the chain. This ensures the integrity of the data stored in the cloud. Additionally, blockchain technology can enable real-time audit ability. By logging all transactions and verifying these logs in the distributed ledger, an organization can verify the data stored in the cloud in real-time and ensure compliance with regulatory requirements. In addition, governing data access to the blockchain is simplified with the help of permission ledgers and smart contracts, which can help prevent fraudulent activities and unauthorized access. In short, leveraging blockchain technology for big data protection ensures the security, privacy, and integrity of data stored in the cloud. This technology can provide organizations with greater control and better visibility over access to data while reducing the complexity of the data security process. Organizations can also enjoy the benefits of greater transparency and traceability, in addition to improved scalability and cost-effectiveness.

5. References

Al-Zaben, N., Onik, M. M. H., Yang, J., Lee, N. Y., & Kim, C. S. (2018, August). General data protection regulation complied blockchain architecture for personally identifiable information management. In 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (pp. 77-82). IEEE.

Grover, P., & Prasad, S. (2021, August). A Review on Block chain and Data Mining Based Data Security Methods. In 2021 2nd International Conference on Big Data Analytics and Practices (IBDAP) (pp. 112-118). IEEE.

Logeshwaran, J., Kiruthiga, T., & Lloret, J., (2023). A novel architecture of intelligent decision model for efficient resource allocation in 5G broadband communication networks. ICTACT Journal On Soft Computing, 13 (3), 2986-2994

V. A. Mohammed, M. A. Mohammed, M. A. Mohammed, J. Logeshwaran and N. Jiwani, Machine Learning-based Evaluation of Heart Rate Variability Response in Children

with Autism Spectrum Disorder, 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 1022-1028

Ramesh, G., Logeshwaran, J., & Aravindarajan, V (2022). A Secured Database Monitoring Method to Improve Data Backup and Recovery Operations in Cloud Computing. BOHR International Journal of Computer Science, 2(1), 1-7

Avinash Khatri, K.C., Krishna Bikram Shah, Logeshwaran, J., & Ashish Shrestha (2023). Genetic algorithm based techno-economic optimization of an isolated hybrid energy system. ICTACT Journal on microelectronics, 8(4), 1447-1450

Ramesh G, Logeshwaran J, Kiruthiga T, Lloret J. Prediction of Energy Production Level in Large PV Plants through AUTO-Encoder Based Neural-Network (AUTO-NN) with Restricted Boltzmann Feature Extraction. Future Internet. 2023; 15(2):46.

Logeshwaran J, Shanmugasundaram N, Lloret J. L-RUBI: An efficient load-based resource utilization algorithm for bi-partite scatternet in wireless personal area networks. Int J Commun Syst.2023;e5439.

Adhikari, N., Logeshwaran, J., & Kiruthiga, T. The Artificially Intelligent Switching Framework for Terminal Access Provides Smart Routing in Modern Computer Networks. BOHR International Journal of Smart Computing and Information Technology, 3(1), 45-50.

Vaniprabha, A., Logeshwaran, J., Kiruthiga, T., & Krishna Bikram Shah (2022). Examination of the Effects of Long-term COVID-19 Impacts on Patients with Neurological Disabilities Using a Neuro machine Learning Model. BOHR International Journal of Neurology and Neuroscience, 1(1), 21-28

Gopi, B., Logeshwaran, J., & Kiruthiga, T (2022). An Innovation in the Development of a Mobile Radio Model for a Dual-Band Transceiver in Wireless Cellular Communication. BOHR International Journal of Computational Intelligence and Communication Network, 1(1), 20-25

Wang, H., Ma, S., Dai, H. N., Imran, M., & Wang, T. (2020). Blockchain-based data privacy management with nudge theory in open banking. Future Generation Computer Systems, 110, 812-823.

Ramesh, G., Logeshwaran, J., & Aravindarajan, V (2022). The Performance Evolution of Antivirus Security Systems in Ultra dense Cloud Server Using Intelligent Deep Learning. BOHR International Journal of Computational Intelligence and Communication Network, 1(1), 15-19

Gopi, B., Ramesh, G., & Logeshwaran, J. (2022). The fuzzy logical controller based energy storage and conservation model to achieve maximum energy efficiency in modern 5g communication. ICTACT Journal on Communication Technology, 13(3), 2774-2779

Ramesh, G., Logeshwaran, J., Gowri, J., & Ajay Mathew (2022). The management and reduction of digital noise in video image processing by using transmission based noise elimination scheme. ICTACT Journal on image and video processing, 13(1), 2797-2801

Gopi, B., Ramesh, G., & Logeshwaran, J. (2022). An innovation for energy release of nuclear fusion at short distance dielectrics in semiconductor model. ICTACT Journal On Microelectronics, 8(3), 1430-1435

J.Logeshwaran (2022, October). The Topology configuration of Protocol-Based Local Networks in High speed communication networks. In Multidisciplinary Approach in Research, Vol. 15, pp. 78-83

Ramesh, G., Logeshwaran, J., & Rajkumar, K. (2022). The smart construction for image preprocessing of mobile robotic systems using neuro fuzzy logical system approach. NeuroQuantology, 20(10), 6354-6367

Raja, S., Logeshwaran, J., Venkatasubramanian, S., Jayalakshmi, M., Rajeswari, N., Olaiya, N. G., & Mammo, W. D. (2022). OCHSA: Designing Energy-Efficient Lifetime-Aware Leisure Degree Adaptive Routing Protocol with Optimal Cluster Head Selection for 5G Communication Network Disaster Management. Scientific Programming, 2022.

Gopi, B., Logeshwaran, J., Gowri, J., & Kiruthiga, T. (2022). The moment probability and impacts monitoring for electron cloud behavior of electronic computers by using quantum deep learning model. NeuroQuantology, 20(8), 6088-6100.

Gopi, B., Logeshwaran, J., Gowri, J., & Aravindarajan, V. (2022). The Identification of quantum effects in electronic devices based on charge transfer magnetic field model. NeuroQuantology, 20(8), 5999-6010.

Logeshwaran, J., Adhikari, N., Joshi, S. S., Saxena, P., & Sharma, A. (2022). The deep DNA machine learning model to classify the tumor genome of patients with tumor sequencing. International Journal of Health Sciences, 6(S5), 9364–9375.

Logeshwaran, J., Malik, J. A., Adhikari, N., Joshi, S. S., & Bishnoi, P. (2022). IoT-TPMS: An innovation development of triangular patient monitoring system using medical internet of things. International Journal of Health Sciences, 6(S5), 9070–9084.

Ramesh, G., Aravindarajan, V., Logeshwaran, J., Kiruthiga, T., & Vignesh, S. (2022). Estimation analysis of paralysis effects for human nervous system by using Neuro fuzzy logic controller. NeuroQuantology, 20(8), 3195-3206.

Ramesh, G., Logeshwaran, J., Aravindarajan, V., & Feny Thachil. (2022). Eliminate the interference in 5g ultra-wide band communication antennas in cloud computing networks. ICTACT Journal On Microelectronics, 8(2), 1338-1344

Sekar, G., Sivakumar, C., & Logeshwaran, J. (2022). NMLA: The Smart Detection of Motor Neuron Disease and Analyze the Health Impacts with Neuro Machine Learning Model. NeuroQuantology, 20(8), 892-899.

Logeshwaran, J., & Karthick, S. (2022, April). A smart design of a multi-dimensional antenna to enhance the maximum signal clutch to the allowable standards in 5G communication networks. ICTACT Journal on Microelectronics, 8(1), 1269–1274.

Jasmine, J., Yuvaraj, N., & Logeshwaran, J. (2022, April). DSQLR-A distributed scheduling and QoS localized routing scheme for wireless sensor network. In Recent trends in information technology and communication for industry 4.0, Vol. 1, pp. 47–60

Ramkumar, M., Logeshwaran, J., & Husna, T. (2022). CEA: Certification based encryption algorithm for enhanced data protection in social networks. In Fundamentals of Applied Mathematics and Soft Computing, Vol. 1, pp. 161–170

Logeshwaran, J. (2022, March). The control and communication management for ultra dense cloud system using fast Fourier algorithm. ICTACT Journal on Data Science and Machine Learning, 3(2), 281–284.

Onik, M. M. H., Aich, S., Yang, J., Kim, C. S., & Kim, H. C. (2019). Blockchain in healthcare: Challenges and solutions. In Big data analytics for intelligent healthcare management (pp. 197-226). Academic Press.

Chen, Z., Xu, W., Wang, B., & Yu, H. (2021). A blockchain-based preserving and sharing system for medical data privacy. Future Generation Computer Systems, 124, 338-350.

Logeshwaran, J., Ramkumar, M., Kiruthiga, T., & Sharan Pravin, R. (2022, February). SVPA - the segmentation based visual processing algorithm (SVPA) for illustration enhancements in digital video processing (DVP). ICTACT Journal on Image and Video Processing, 12(3), 2669–2673

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 126, 45-58.

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 126, 45-58.

Logeshwaran, J., Ramkumar, M., Kiruthiga, T., & Sharanpravin, R. (2022). The role of integrated structured cabling system (ISCS) for reliable bandwidth optimization in high-speed communication network. ICTACT Journal on Communication Technology, 13(01), 2635–2639

Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., ... & Pathirana, P. N. (2022). A survey on blockchain for big data: approaches, opportunities, and future directions. Future Generation Computer Systems.

Liu, S., Zhang, Q., & Liu, H. (2021, February). Privacy protection of the smart grid system based on blockchain. In Journal of Physics: Conference Series (Vol. 1744, No. 2, p. 022129). IOP Publishing.

Logeshwaran, J. (2021, December). AICSA - an artificial intelligence cyber security algorithm for cooperative P2P file sharing in social networks. ICTACT Journal on Data Science and Machine Learning, 3(1), 251–253.

Liang, G., Weller, S. R., Luo, F., Zhao, J., & Dong, Z. Y. (2018). Distributed blockchain-based data protection framework for modern power systems against cyber attacks. IEEE Transactions on Smart Grid, 10(3), 3162-3173.

Wang, B., & Li, Z. (2021). Healthchain: A privacy protection system for medical data based on blockchain. Future Internet, 13(10), 247.

Logeshwaran, J., & Shanmugasundaram, R. N. (2019, December). Enhancements of Resource Management for Device to Device (D2D) Communication: A Review. In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 51-55). IEEE.

Kumar, R., Tripathi, R., Marchang, N., Srivastava, G., Gadekallu, T. R., & Xiong, N. N. (2021). A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. Journal of Parallel and Distributed Computing, 152, 128-143.

Zhang, J., Zhong, S., Wang, T., Chao, H. C., & Wang, J. (2020). Blockchain-based systems and applications: a survey. Journal of Internet Technology, 21(1), 1-14.

Logeshwaran, J., Rex, M. J., Kiruthiga, T., & Rajan, V. A. (2017, December). FPSMM:

Fuzzy probabilistic based semi morkov model among the sensor nodes for realtime applications. In 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 442-446). IEEE.

Li, W., Su, Z., Li, R., Zhang, K., & Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6G networks. IEEE Network, 34(6), 31-37.

Ren, W., Wan, X., & Gan, P. (2021). A double-blockchain solution for agricultural sampled data security in Internet of Things network. Future Generation Computer Systems, 117, 453-461.

Logeshwaran, J., Saravanakumar, K., Dineshkumar, S., & Arunprasath, C. (2016, March). SBML algorithm for intelligent fuel filling (IFF) and smart vehicle identification system (SVIS). International Journal of Advanced Research in Management, Architecture, Technology & Engineering, 2(9), 149–154.

El Azzaoui, A., Chen, H., Kim, S. H., Pan, Y., & Park, J. H. (2022). Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems. Sensors, 22(4), 1371.

Saravanakumar, K., & Logeshwaran, J. (2016, February). Auto-Theft prevention system for underwater sensor using lab view. International Journal of Innovative Research in Computer and Communication Engineering, 4(2), 1750–1755.

Hirtan, L., Krawiec, P., Dobre, C., & Batalla, J. M. (2019, September). Blockchain-based approach for e-health data access management with privacy protection. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-7). IEEE.

Sutharasan, M., & Logeshwaran, J. (2016, May). Design intelligence data gathering and incident response model for data security using honey pot system. International Journal for Research & Development in Technology, 5(5), 310–314.

Yue, L., Junqin, H., Shengzhi, Q., & Ruijin, W. (2017, August). Big data model of security sharing based on blockchain. In 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM) (pp. 117-121). IEEE.