International e-Conference on New Horizons And Multidisciplinary Applications In Science And Technology
In Association withInternational Journal of Scientific Research in Science and Technology
Volume 9 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

An Efficient Security Mechanism Using Blockchain Technology

Ms. Geeta N. Brijwani[1], Dr. Prafulla E. Ajmire[2], Ms. Varkha Jewani[3], Ms. Pragati V. Thawani[3]
[1]Assistant Professor, Department of Computer Science, KC College, Churchgate, Mumbai, Maharashtra, India
[2]Head & Associate Professor, Department of Computer Science & Application, G S Science, Arts & Commerce College, Khamgaon, Maharashtra Sant Gadge Baba Amravati University, Maharashtra, India
[3]Assistant Professor, Department of IT, KC College, Churchgate, Mumbai, Maharashtra, India

ABSTRACT

Now a days there is large amount of information is available with the world and is stored in the databases and applications. These databases may be centralized or distributed depending on the need of application but the primary concern here is to store such a large amount of data or information efficiently and effectively. Thus there is also an important aspect that has to be kept in mind while dealing with such a large volume and vast amount of data that is how it can be access whenever that data or information is in a distributed database. However it is also a challenging task that these things can be conveniently done without any hurdles.

There is need to develop necessary operations and applications which can work over this situation. The most important aspect of this scenario which we are going to discuss here is the issue related to the security of such vital and crucial information in terms of the various methods and parameters. Thus the proposed system tries to provide the highest level of security to the very large amount of information with great efficiency in terms of block chain technology.

Keywords: Blockchain framework, information security. Databases.

I. INTRODUCTION

This mechanism discuss here in this context is very successful management and is of greater consumer value of the information which is present in the various types and formats in different kinds of applications.

The information present in the different types of applications can be in the form of structured information, unstructured information or semi structured records. Also these all types of information can be categorized on the basis of various constraints where it can be applied.

Moreover these all sort of information can be after the successful storage can be accessed from several sources and databases using the IOT, Sensors and contact network to network and also from mobile to mobile communication. The primary aspect which is very significant in achieving the highest level of security in perusing the essential sensitive data standards [2].

The data may be from the various domains like it may be from the details relating to hospitals or it may be client data biometric data financial data, confidential information and may be all types and sort of sensitive data. As the data is confidential and sensitive therefore any type of improper access to such type of data may lead to data lost from the application or the trust of any business may also lead to break in case of undetermined modification in the data or the misuse of data.

Therefore there is a great need to provide a high level of security constraints over accessing such a crucial data. In other words there has to be full proof security framework is essential to deal with all situations which tries to hamper the data to a great extent.

Hence in order to achieve all such security features for the information system a new and efficient system is proposed. This research focuses on the blockchain technologies to ensure the all sorts of critical data protection. This system of blockchain that is a sort of distributed database and that is also collection of cryptographic generated block of data. It also contains distributed ledger and consensus system and a proper infrastructure for smart contracts.

This study explains the new framework using the blockchain technology for the implementation of the information security using the various schemes for the retrieval and transfer of confidential data. This paper also discusses the different challenges and constraint specific scenario regarding the various needs specific applications for various parameters.

The blockchain, named the greatest innovation since the invention of the Internet, its success in many ways draws interest. Through its reliable blockchain structure, it has raised the degree of preferably, which poses its differentiation by providing developments in many fields such as health, banking, public and business.

In addition, it has a ground breaking character with the function that excludes the central authority, unlike the classical systems. In terms of perceiving consumer habits, social media, which has become a part of everyday life, offers valuable evidence. Through its insecure framework, social media creates an unstable environment at any moment and can distribute data that can control people. A literature review proposed a solution to this dangerous setting. A blockchain-based architecture was suggested to secure the privacy of users, and the Distributed Partial Ledger Management Technique (DEPLEST) algorithm was used. This algorithm ensures that confidential user information is protected by using fewer resources in the classical blockchain than is necessary.

The paper is organized as follows:

Section I Introduction. Section II discusses Background. Section III discusses previous work. Section IV discusses existing methodologies. Section V discusses attributes and parameters and how these are affected on various architectures. Section VI is proposed method. Section VII is experimental tests carried out. Section VIII is outcome and result. Section IX is conclusion. Finally Section X is future scope of this analytical paper.

II. PREVIOUS WORK DONE

The blockchain framework in the health sector has been stressed, as in almost any sector, and different studies have been carried out. In a study conducted, solutions for protection, privacy and efficiency deficiencies were provided to body sensor networks used to track patient health information. A hybrid blockchain structure was given priority in this report, and openness and usability were taken into account and potential attacks were taken into account.[4]

A blockchain framework was built in another study in which patient health information was stored in a distributed way. A blockchain framework was built in another study in which patient health information was transmitted in a distributed way.[5] While the system presents the advantages of the traditional blockchain, it is seen that the new technology does not meet all the health system specifications.[6]

III. EXISTING METHODOLOGIES

The level of usage of IoT devices is growing day by day with the growth of the internet. With these rising products, the need for energy rises and the wasteful use of these resources is met at the same time. A blockchain-based algorithm using the safe method of sharing of resources (SMER) method was suggested in a study conducted to solve this problem. With its open, autonomous nature and stability, it is anticipated that it will be available in future voting systems.[7]

Blockchain was created with a sequential mining method using Multichain source codes in a study on this subject. Furthermore, by using the blind signature method, the secrecy of the identity of the elector was assured. Although the existing mechanism offers voting and counting protections, in the case of online elections, it will remain open to attacks. [6].

There are, however, certain deficiencies in the blockchain, as in any method. The need for a very large database, high power usage, and the existence of dispute concerns are examples of such shortcomings.

The performance of the blockchain structure has been discussed in this paper and the benefits and drawbacks it provides on the basis of the sector and application have beenexamined.

IV. ANALYSIS AND DISCUSSION

This research discusses different parameters and constraints related to the different scenarios and different aspect of the information security using the blockchain technology. The proposed method also ensures that the different drawback from the previous methods discussed earlier should be overcome using the new advanced technology and framework.

V. PROPOSED METHODOLOGY

There are different methods and parameters discussed in the previously designed methods are discussed here and have many features which are interesting to note their behavior and it is also very significant to note the relationship between the different parameters.

Blockchain technology is graded according to the features used and whether the participation of the network is subject to approval or not. There are 3 forms of blockchain, as can be seen from figure 1.

Users do not require approval from any authority in transparent blockchain schemes. Any method can be transparently tracked in this kind of framework. Examples of transparent blockchains include networks including Ethereum, Bitcoin, Litecoin, Monero.

Unique blockchains are networks approved completely by the authority. Who will engage in the network, mining activities and new transactions are subject to authorization. Although it appears to be contradictory to the logic of the blockchain in this arrangement, the operations conducted are isolated from the classical structures with the function of being viewed in a clear manner by each consumer.

In consortium blockchains, Network membership is not available to all and is based on a system of acceptance. This relates to networks formed between organizations coming together for such purposes.

The method is executed and job specifications are described in a closed manner. Therefore, no mechanisms of reconciliation are required. This helps transfers to be executed more rapidly [4].

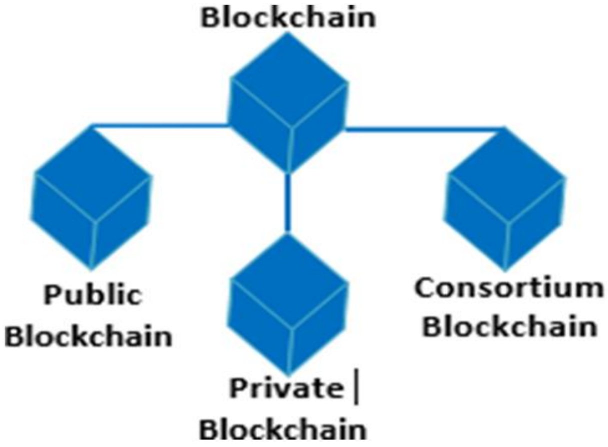

Fig 1: Block chain types

The Hash feature is a feature that takes text as an input and transforms it as an output to a special fixed-length string. These functions are rendered immutable by the uni- directionality of hash functions. In figure, a block diagram explaining this condition is shown.

The node applies to each network unit and has two types. One of them, Light node, is used by keeping block headers to validate the validity of transactions. Even, it is not obliged to obey the laws of consensus. It is the duty of the full node to hold all block information and to enforce the consensus rules.

Encryption is used in case of attack, to protect the blockchain. It is meant to guarantee the secrecy and dignity of the information. For this reason, there are two forms of encryption. There are, respectively, asymmetric and symmetric forms of encryption. A single key is used in symmetric switching, and the same key is used to encrypt and decrypt the data. There are two keys and a logical encryption of these keys in asymmetrical switching. Asymmetric encryption is more efficient than symmetric encryption in this regard.

In the blockchain method, the exchange refers to the movement of digital properties between the parties. The system-approved transactions are registered on the blocks and added to the blockchain. An example block diagram of this approach is given in Figure 2.

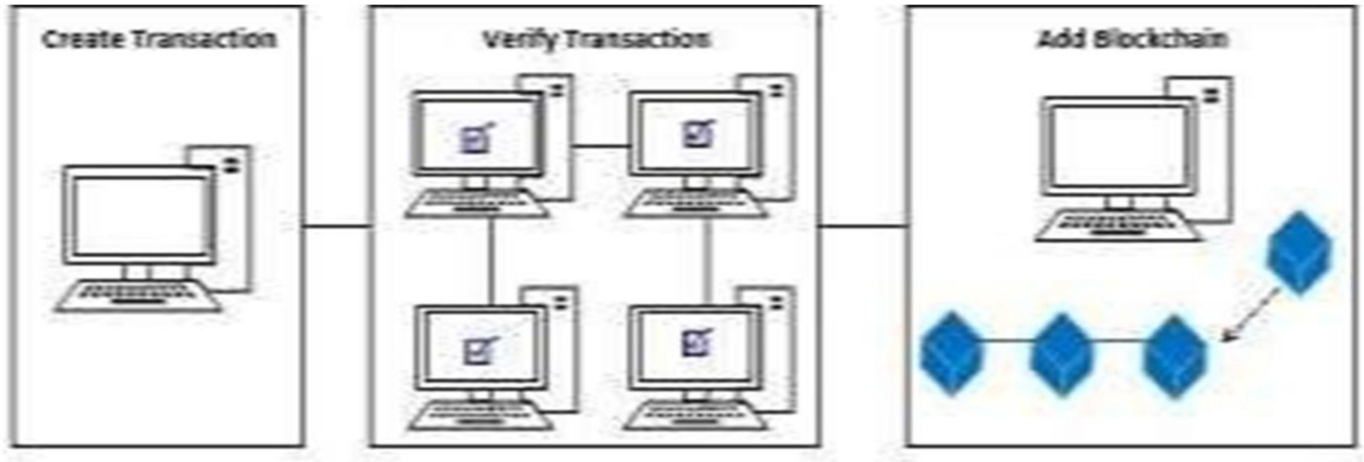

Fig2: Transaction step

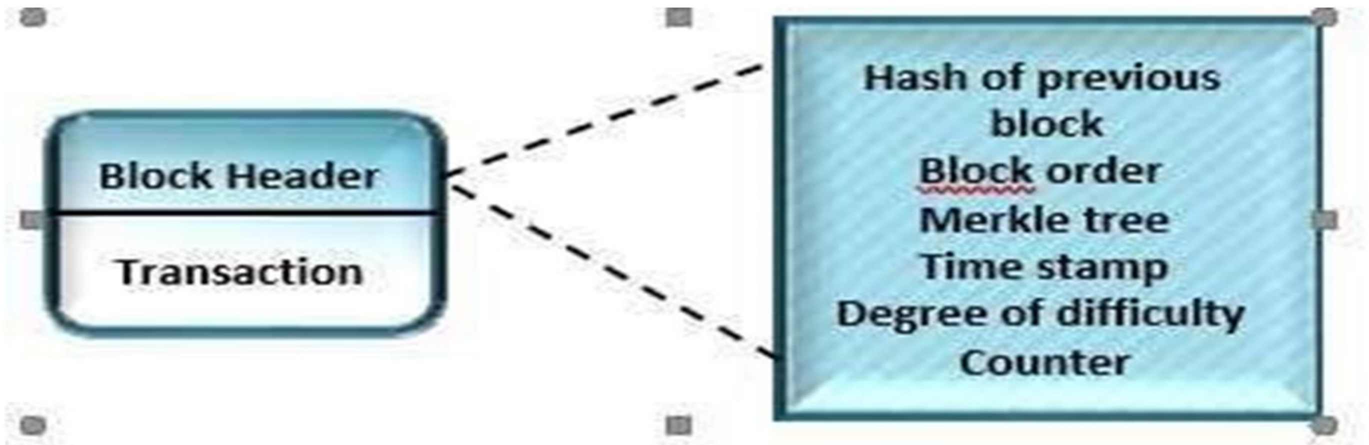

Fig 3: Block chain node

Blockchain is an age that enhances an awesome manner to have huge-undertaking consequences such that it can now not genuinely change financial offerings, but also other commercial business and sectors. Billions of individuals and groups are served and trillions of dollars are transported every day around the previous worldwide financial facility.

Despite the fact that dressed up with a virtual presence, however, closely dependent and dependent on paper, there are different problems with that same age. Primary motivation brought price and delay as well as making it far less difficult to cripple it for theft and fraud. Blockchain and its expected advantages make it worthwhile, considering the monetary employer's aversion to trade. Not like conventional systems, Blockchain is dynamic enough to become a trend setter in a charged business scenario for deployment.

The greatest value it guarantees in a blockchain is that every celebration has a report that is kept in a database that everyone has to use. It is a ledger that is commonly exceeded by special users, thereby providing a shared database that is replicated to certain users and who can get access to it better because they have the correct entry for it.

VI. OUTCOME AND RESULTS

Any bank identified upon that blockchain network would just have to update the registry by exporting encrypted consumer data that allows the user's data to be secured. Each bank will have the same ledger with customer details and recent transactions when registered on this website. DLT would provide the customer with a total accountability model for sending money overseas along with consistent connectivity.

As any node present on the network verifies the transaction and saves the transaction history in the blockchain ledger, this will also minimize the time for the transaction to be processed. The double expense problem present in the centralized method would also disappear from this distributed ledger. On-chain settlement with the negligible cost of a contract is also given by this network.

VII.CONCLUSION

With its innovative features, Blockchain has drawn great interest. With its applicability, protection and versatility in almost every industry, it has undergone a rapid phase of growth. The framework of the blockchain brings foundational characteristics to the fields where they are implemented, such as accuracy, tempo, interoperability and falsifiability. However, daunting challenges, such as the complete replacement of infrastructure by traditional structures, can also be met.

In this research, data on the design of the blockchain is presented and the circumstances found are analyzed on the basis of analysis.

VIII. FUTURE SCOPE

It is expected that the research in this area and continuous development will eventually result in a several of utility of the proposed design. These strategies will also greatly increase the effectiveness and efficiency of the previous designs.

IX. REFERENCES

[1] . L.Ismail and H. Materwala, "A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions, "Symmetry,11(10), vol 1198, 2019.

[2] . Y. Chen , H. Xie, K. Lv, S. Wei and C. Hu," DEPLEST: A Blockchain-based Privacy-preserving Distributed Database toward User Behaviors in Social Networks," Information Sciences,2019

[3] . I. Jawaid, I.U. Arif, N. Amin and W. Abdul, "Efficient and secure attribute- based heterogeneous online/offline signcryption for body sensor networks based on blockchain," International Journal of Distributed Sensor Networks, 2019

[4] . M. Murat, "Blockchain İle Güvenli Elektronik Sağlık Sistemi", İstanbul Technical University, 2018

[5] . Z. Yu, H. Yuxing and W. Jiangtao, "SMER: a secure method of exchanging resources in heterogeneous internet of things," Frontiers of Computer Science, 13.6, pp. 1198- 1209,2019.

[6] . A. E. Muhammed, "Blokzincir Tabanlı Oy Verme Sistemi Öneri," Necmettin Erbakan University, 2018.

[7] . E. D. Serap, "Blockchain Teknolojisinin Finans Sektöründeki Yeri ve Uygulamaları," Marmara University, 2018.

[8] . B. Şeref, "A Blockchain –Based Framework for Customer Loyalty Programs," İstanbul Technical University, 2018.

[9] . G. Güliz, "Blokzincir Teknolojisiyle Gıda Güvenliği Ve Yumurta Sektörü İçin Örnek Bir Uygulama," Marmara University, 2019.

[10] . C. Ç. Salih, "Implementing a Blockchain Protocol and Creating a Digital Asset Transfer Environment",Bahçeşehir University, 2018.

[11] . S. K. İmparator, "Elektronik Ödemelerde Blok Zinciri Sistematiği ve Uygulamaları," Erciyes University, 2017.

[12] . G. Bilal, "Blok zinciri Tabanlı Elektronik Seçim Sistemi Tasarım Ve Kısmi Uygulaması," İstanbul Technical University, 2019.

[13] . Ç. N. Galip, "Blockchain Teknolojisiyle Açık Anahtar Altyapısı Tabanlı Elektronik Sertifika Durum Bilgilerinin Yönetilmesi," Sakarya Uygulamalı Bilimler University, 2019.

[14] . A. Kerem, "Blokzinciri Ve Akıllı Sözleşmeler: Güvenli Bir Dijital Sertifikasyon Uygulaması Geliştirilmesi," Trakya University, 2019.

[15] . Z.Ü. Evrim, "Blockchain's Impact On Solving Supply Chain Mnagement Challenges," Yeditepe University, 2018.

[16] . B.Ç. Doğa, "Blokzincir Tabanlı Elektronik Seçim Sistemi Modellemesi," İstanbul Technical University, 2019.

[17] . O. T. Ali, "Blok Zincir Teknolojisi ve %51 Sorunsalı," Beykent University, 2019.

[18] . K. İsmail," Blokzinciri teknolojisi ve yakın gelecekteki uygulama alanları," Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 9.1, pp. 75-82, 2018.

[19] . S. Hamza,"Gayrimenkul Sektöründe Blok Zincir Teknolojisinin Kullanımı VE Akıllı Kontratların İncelenmesi," İstanbul Technical University, 2019.