iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43752

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Block Chain Based Data Storage with Privacy and Authentication

Navaneetha Krishnan M[1], Vishnu A[2]
[1]*Assitant Professor,* [2]*Student, Department of MCA, Karpagam College of Engineering, Coimbatore, Tamil Nādu ,India*

Abstract— The project is entitled Block Chain Based Data Storage's privacy and ensures that blockchain-based framework integrated with authentication and privacy schemes are enhanced by secure connections to wireless nerve networks. In this set of program programs transmit the information collected to BS. As a result, BS records all key parameters in a distributed blockchain and large data is transferred to the cloud for storage. Damaged certificates for all malicious nodes are removed from the blockchain by Base Station. Although, the performance of WSNs are specific requests in terms of area of interest and method of delivery, but the purpose is to maintain the monitoring, hearing, dissemination and processing of the information collected. However, the amount of information is huge at an extraordinary rate. When an enemy attacks a network and deliberately threatens nodes, network security becomes a threat. Therefore, it is necessary for WSNs to isolate and remove malicious nodes from a network before it can be active. Adjusted outcomes, comparative analysis and security assurance support the height of the proposed solution than existing methods.
Index Terms- wireless sensor, WSN, network security

I. INTRODUCTION

In modern times, Internet of Things (IoTs) is one of the most popular, useful and dominant technologies for wireless communication and information processing. IoTs are the building of 'objects' that are fragile, understandable, manageable, and that can be accessed with the help of the internet. In today's world, virtually every object on the IoT can be connected to the Internet because of its ability to communicate with a computer, which is why even the most efficient and convenient applications can be made. Several node sensors are used for monitoring, hearing and automation purposes on IoT. The collection of these nodes is commonly known as Wireless Networks (WSNs) and forms an integral part of the IoT as these technologies can detect and monitor any objects / activities that are visible in a particular area. The above-mentioned sensors, also known as 'motes', are cheap, small and internally connected and are distributed in certain areas. These sensors node integrate many aspects of hearing, computer and communication using wireless medium and therefore in WSNs, material is monitored and heard in real time. Although, the performance of WSNs are specific requests in terms of area of interest and method of delivery, but the purpose is to maintain the monitoring, hearing, dissemination and processing of the information collected. However, the amount of information is huge at an extraordinary rate too, which needs to be addressed in the current world of technology. As is well known, WSNs are used in a variety of programs such as military, industry, smart home, health care, surveillance, housing monitoring and agriculture to name a few. Sensors node, the core of WSN, has limited resources such as power, integration power, storage, and network bandwidth. Therefore, as the demand for WSNs grows exponentially in IoT, more challenges are encountered in order to make better use of it. In addition, security is another important factor in WSN-enabled IoT. When an enemy attacks a network and deliberately threatens nodes, network security becomes a threat. Therefore, it is necessary for WSNs to isolate and remove malicious nodes from the network before they can be actively active with IoT infrastructure.

II. LITERATURE REVIEW

Aldowah, H.; Rehman, S.U.; Umar, I. Security in Internet of Things: Issues, Challenges and Solutions. In International Conference of Reliable Information and Communication Technology; Springer: Cham, Switzerland, 2018. In the recent past, Internet of Things (IoT) has been a focus of research. With the great potential of IoT, there come many types of issues and challenges. Security is one of the main issues for IoT technologies, applications, and platforms. In order to cover this key aspect of IoT, this paper reviews the research progress of IoT, and found that several security issues and challenges need to be considered and briefly outlines them. Efficient and functional security for IoT is required to ensure data anonymity, confidentiality, integrity, authentication, access control, and ability to identify, as well as heterogeneity, scalability, and availability must be taken into the consideration. Considering these facts, by reviewing some of the latest researches in the IoT domain, new IoT solutions from technical, academic, and industry sides are provided and discussed. Based on the findings of this study, desirable IoT solutions need to be designed and deployed, which can guarantee: anonymity, confidentiality, and integrity in heterogeneous environments.

Ourad, A.Z.; Belgacem, B.; Salah, K. Using blockchain for IOT access control and authentication management. In International Conference on Internet of Things 2018 June; Springer: Cham, Switzerland, 2018. Securing Access to IOT devices is a challenging task as IoT devices are resource-constrained devices in terms of processing, storage, and networking capacity. Because of their fast spreading and deployment, significant disadvantages are seen in today's authentication and access control schemes. This paper proposes a blockchain-based solution which allows for authentication and secure communication to IOT devices. Our solution benefits greatly from the intrinsic features of blockchain and also builds on existing authentication schemes. Specifically, our proposed blockchain-based solution, architecture, and design allow for accountability, integrity, and traceability with tamper-proof logs. The paper provides overall system design and architecture, and details on testing and implementation of a realistic scenario as a proof of concept.

Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A blockchain-enabled decentralized capability-based access control for iots. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018. The prevalence of Internet of Things (IoTs) allows heterogeneous embedded smart devices to collaboratively provide smart services with or without human intervention. While leveraging the large-scale IoT-based applications like Smart Gird or Smart Cities, IoTs also incur more concerns on privacy and security. Among the top security challenges that IoTs face, access authorization is critical in resource sharing and information protection. One of the weaknesses in today's access control (AC) is the centralized authorization server, which can be the performance bottleneck or the single point of failure. In this paper, BlendCAC, a blockchain-enabled decentralized capability-based AC is proposed for the security of IoTs. The BlendCAC aims at an effective access control processes to devices, services and information in large scale IoT systems. Based on the blockchain network, a capability delegation mechanism is suggested for access permission propagation. A robust identitybased capability token management strategy is proposed, which takes advantage of smart contract for registering, propagation and revocation of the access authorization. In the proposed BlendCAC scheme, IoT devices are their own master to control their resources instead of being supervised by a centralized authority. Implemented and tested on a Raspberry Pi device and on a local private blockchain network, our experimental results demonstrate the feasibility of the proposed BlendCAC approach to offer a decentralized, scalable, lightweight and fine-grained AC solution to IoT systems.

M. Wang and Q. Zhang, "Optimized data storage algorithm of IoT based on cloud computing in distributed system," Computer Communications, vol. 157, pp. 124–131, 2020. In addition to an in-depth review of these threats, we also summarize the corresponding defense strategies. In addition, we discuss future research guidelines on new safety threats, especially those related to in-depth learning based on self-driving vehicles. By providing safety guidelines in this early phase, we aim to promote new strategies and projects related to AVs from both academic and industry, and promote the development of safe driving.

Protecting Shared Learning: Reducing Toxic Attacks through Client Acquisition, L. Zhao et al., "Protecting collaborative learning: Reducing toxic attack through client acquisition", IEEE Trans. Depend. Secure Comput., Apr. 2020. In this article, we introduce a new defense system to get amazing updates on both IID and non-IID settings. Our main focus is to get the opposite side of the client side, where each update is evaluated with the local data of other clients. The server will adjust the weights of the updates based on the test results when performing the integration. In order to accommodate the unequal distribution of data in non-IID settings, the flexible client allocation method is designed to assign the most appropriate clients the diagnostic functions. During the acquisition process, we also protect client-level privacy to prevent malicious clients from being able to participate in other clients, by combining different privacy with our design without compromising adoption performance. Our experimental experiments on three real-world databases show that our system is extremely resilient to two toxic attacks.

M. Wang and Q. Zhang, "Optimized data storage algorithm of IoT based on cloud computing in distributed system," Computer Communications, vol. 157, pp. 124–131, 2020 The existing Internet of Things(IoT) uses cloud computing data access storage algorithms, that is, the hash algorithm has defects of low data processing efficiency and low fault tolerance rate. Therefore, HDFS is introduced to optimize cloud computing data access storage algorithms. HDFS is first used to optimize the data access storage architecture according to problems of data access storage architecture in the Internet of Things, in which factors of data access storage distribution in the IoT are fully considered, and hash values are used to optimize the configuration of data access information storage locations, so that data access storage distribution strategy can be optimized. Then, the topology of the IoT is optimized, and data block size is also optimized with effect algorithm. Finally, the design of file storage is optimized. Through simulation experiments, it is proved that the optimized cloud storage method has obvious performance advantages in file read and write speed as well as memory usage. Compared with the traditional hash algorithm, optimization algorithm proposed in the paper greatly improves file upload and download efficiency, data processing efficiency and fault tolerance rate, which fully demonstrates that the proposed cloud computing data access storage optimization algorithm is more superior.

C. Feng, M. Adnan, A. Ahmad, A. Ullah, and H. U. Khan, "Towards Energy-Efficient Framework for IoT Big Data Healthcare Solutions," Scientific Programming, vol. 2020, pp. 1–9, 2020. The aim of the Internet of things (IoT) is to bring every object

(wearable sensors, healthcare sensors, cameras, home appliances, smart phones, etc.) online. These different objects generate huge data which consequently lead to the need of requirements of efficient storage and processing. Cloud computing is an emerging technology to overcome this problem. However, there are some applications (healthcare) which need to process data in real time to improve its performance and require low latency and delay. Fog computing is one of the promising solutions which facilitate healthcare domain in terms of reducing the delay multihop data communication, distributing resource demands, and promoting service flexibility. In this study, a fog-based IoT healthcare framework is proposed in order to minimize the energy consumption of the fog nodes. Experimental results reveal that the performance of the proposed framework is efficient in terms of network delay and energy usage. Furthermore, the authors discussed and suggested important services of big data infrastructure which need to be present in fog devices for the analytics of healthcare big data.

III. EXISTING SYSTEM

In Existing System, One Session cannot fully utilize network capacity due to network root. The second difference is the definition of throughput. In a multi-channel system, all sessions are subject to the same data, and only one block of data can be considered valid while other packets are no longer active. Existing, data transmission is intentionally repeated or delayed by malicious or fraudulent notes. A refusal attack represents a denial or objection and a location tracking attack may occur.

IV. PROPOSED SYSTEM

In the proposed system, a blockchain-based solution for privacy and cloud storage authentication, Base Station provides a certificate for all sensodes nodes, a certificate key for all nodes stored in an immovable key and a large amount of sensitive information stored in the cloud. The proposed system provides promising results in terms of delays and power consumption with the appropriate combination of traffic and processing. The proposed scheme can prevent re-playing, denial attacks and counterfeit attacks. It is necessary for each sensor to constantly transmit information about location, motion speed and information collected. Detection privacy detection ensures that no one was able to disclose the actual data passing through the wireless sensor network..

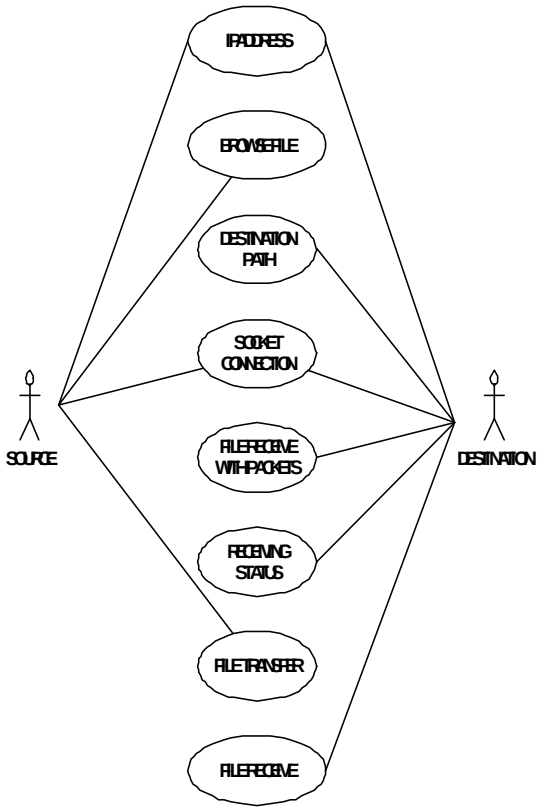


Figure 1: Proposed System

V. METHODOLOGY

Location description is the official description of a system, organized in a way that supports thinking about system structures. It defines system components or building blocks and provides a system in which products can be purchased, as well as advanced systems, that will work together to run the entire system.

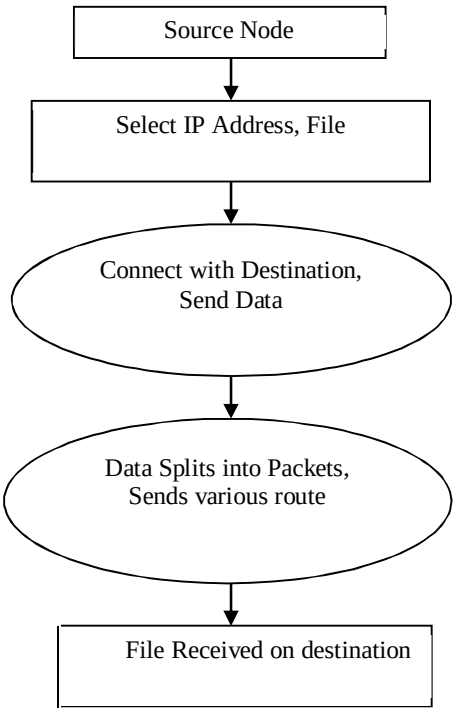


Figure 2: Methodology

VI. TECHNOLOGY USED

A. C#.NET

Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating XML Web services, Microsoft Windows-based applications, and Web solutions. The .NET Framework is a language-neutral platform for writing programs that can easily and securely interoperate. There's no language barrier with .NET: there are numerous languages available to the developer including Managed C++, C#, Visual Basic and Java Script. The .NET framework provides the foundation for components to interact seamlessly, whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate. ".NET" is also the collective name given to various software components built upon the .NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET My Services, and so on).

B. The .Net Framework

The .NET Framework has two main parts:

The Common Language Runtime (CLR)

A hierarchical set of class libraries.

The CLR is described as the "execution engine" of .NET. It provides the environment within which programs run. The most important features are

- Conversion from a low-level assembler-style language, called Intermediate Language (IL), into code native to the platform being executed on.
- Memory management, notably including garbage collection.
- Checking and enforcing security restrictions on the running code.
- Loading and executing programs, with version control and other such features.
- The following features of the .NET framework are also worth description:

1) *Managed Code:* The code that targets .NET, and which contains certain extra Information - "metadata" - to describe itself. Whilst both managed and unmanaged code can run in the runtime, only managed code contains the information that allows the CLR to guarantee, for instance, safe execution and interoperability.

2) *Managed Data:* With Managed Code comes Managed Data. CLR provides memory allocation and Deal location facilities, and garbage collection. Some .NET languages use Managed Data by default, such as C#, Visual Basic.NET and JScript.NET, whereas others, namely C++, do not. Targeting CLR can, depending on the language you're using, impose certain constraints on the features available. As with managed and unmanaged code, one can have both managed and unmanaged data in .NET applications - data that doesn't get garbage collected but instead is looked after by unmanaged code.

3) *Common Type System:* The CLR uses something called the Common Type System (CTS) to strictly enforce type-safety. This ensures that all classes are compatible with each other, by describing types in a common way. CTS define how types work within the runtime, which enables types in one language to interoperate with types in another language, including cross-language exception handling. As well as ensuring that types are only used in appropriate ways, the runtime also ensures that code doesn't attempt to access memory that hasn't been allocated to it.

4) *Common Language Specification:* The CLR provides built-in support for language interoperability. To ensure that you can develop managed code that can be fully used by developers using any programming language, a set of language features and rules for using them called the Common Language Specification (CLS) has been defined. Components that follow these rules and expose only CLS features are considered CLS-compliant.

5) *The Class Library:* .NET provides a single-rooted hierarchy of classes, containing over 7000 types. The root of the namespace is called System; this contains basic types like Byte, Double, Boolean, and String, as well as Object. All objects derive from System. Object. As well as objects, there are value types. Value types can be allocated on the stack, which can provide useful flexibility. There are also efficient means of converting value types to object types if and when necessary.
The set of classes is pretty comprehensive, providing collections, file, screen, and network I/O, threading, and so on, as well as XML and database connectivity. The class library is subdivided into a number of sets (or namespaces), each providing distinct areas of functionality, with dependencies between the namespaces kept to a minimum.

6) *Languages Supported By .Net:*

- The multi-language capability of the .NET Framework and Visual Studio .NET enables developers to use their existing programming skills to build all types of applications and XML Web services. The .NET framework supports new versions of Microsoft's old favorites Visual Basic and C++ (as VB.NET and Managed C++), but there are also a number of new additions to the family.
- Visual Basic .NET has been updated to include many new and improved language features that make it a powerful object-oriented programming language. These features include inheritance, interfaces, and overloading, among others. Visual Basic also now supports structured exception handling, custom attributes and also supports multi-threading. Visual Basic .NET is also CLS compliant, which means that any CLS-compliant language can use the classes, objects, and components you create in Visual Basic .NET.
- Managed Extensions for C++ and attributed programming are just some of the enhancements made to the C++ language. Managed Extensions simplify the task of migrating existing C++ applications to the new .NET Framework. C# is Microsoft's new language. It's a C-style language that is essentially "C++ for Rapid Application Development". Unlike other languages, its specification is just the grammar of the language. It has no standard library of its own, and instead has been designed with the intention of using the .NET libraries as its own.
- Microsoft Visual J# .NET provides the easiest transition for Java-language developers into the world of XML Web Services and dramatically improves the interoperability of Java-language programs with existing software written in a variety of other programming languages. Active State has created Visual Perl and Visual Python, which enable .NET-aware applications to be built in either Perl or Python. Both products can be integrated into the Visual Studio .NET environment. Visual Perl includes support for Active State's Perl Dev Kit.

VII. EXPERIMENTAL RESULTS AND DISCUSSION

A. Registration Phase

All node information such as speed, volume, and performance, residual power is registered to the server, to the base station and shared to all other cluster heads available on the network. The Cluster Head maintains all of these parameters and also transmits the parameters to the corresponding sensor nodes. After collecting key information in the cluster head sensor node, each common sensor node stores the information in its memory and uses that information for additional verification purposes.

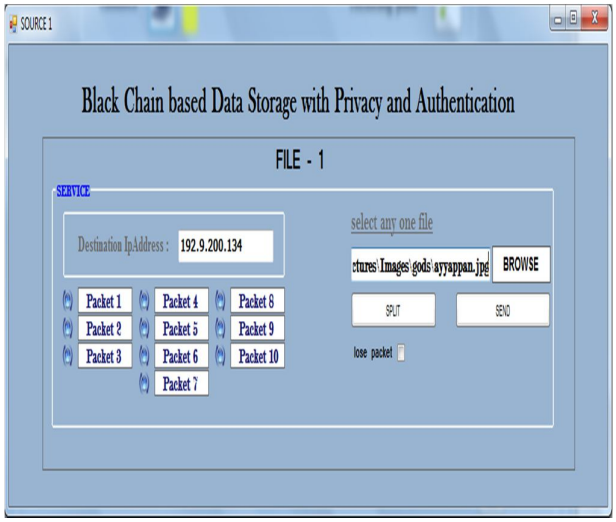


Figure 3: Select file and destination address

B. Packet Signing and Capture

At this stage, the signing and confirmation of the packages is done by the cluster head. The Base station needs to decide whether to deliver the package to its destination at the current time. In that case, the base station needs to select a single sensor area (possibly the source node itself) with a copy of the package at the beginning of the timelot, and set up a radio broadcast to transfer this packet to its destination within the same timelot, using. possible multi-hop transfers. If this happens successfully, we say that the selected sensor node successfully captured the packet location.

Figure 4: Splitting File

C. Duplication

With the p packet not delivered successfully, the base station needs to determine whether to duplicate the packet p to other nodes that do not have a packet at the beginning of the timeline. The basic channel also needs to determine which nodes to be transferred to and from, and how. All transmissions can be made to a wireless sensor network or to infrastructural mode.

D. Packet Transmission

Since the p packet was not successfully delivered, the primary channel needs to determine whether to duplicate the packet p to other nodes that do not have the packet at the beginning of the timeline. The primary channel also needs to determine which nodes to transfer or return, and how. All transmissions can be made to a wireless sensor network or to infrastructural mode.

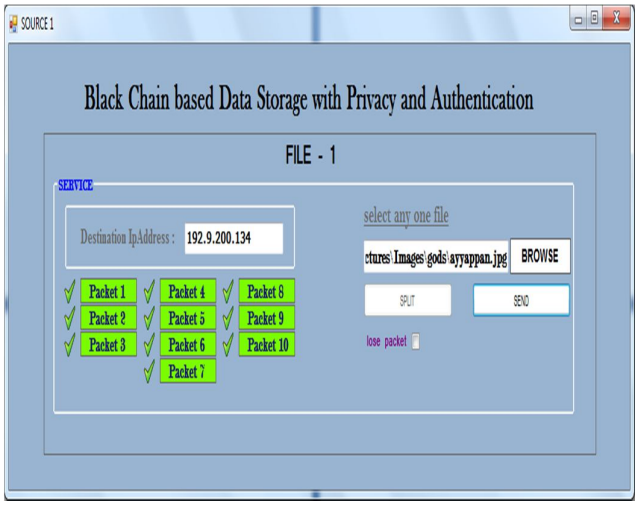


Figure 5: Block Management

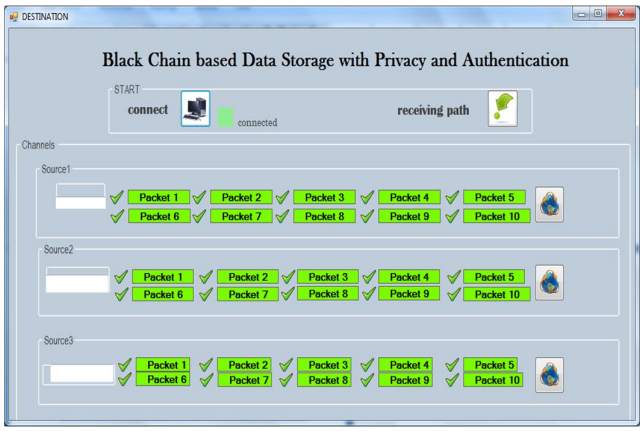


Figure 6: Packets received from source

E. Preventing Packet Modification

Different types of packages in the proposed scheme are cluster head to cluster head packet, cluster head to BS packet, BS to BS packet and key update packet. If the attacker wishes to change or modify packets, they need to get the key from the server, but it is not possible to get such important information. Therefore, the proposed system provides protection against package attacks Simulation or modification. All the sensor nodes are connected to the fake ID and each broadcast packet and skip confirming who you are using the table.

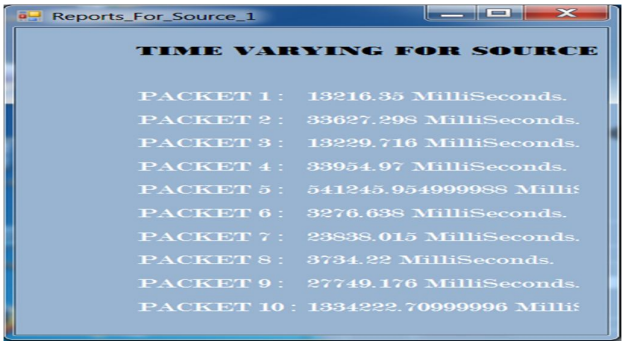


Figure 7: Find converge cost delay

VIII. CONCLUSION

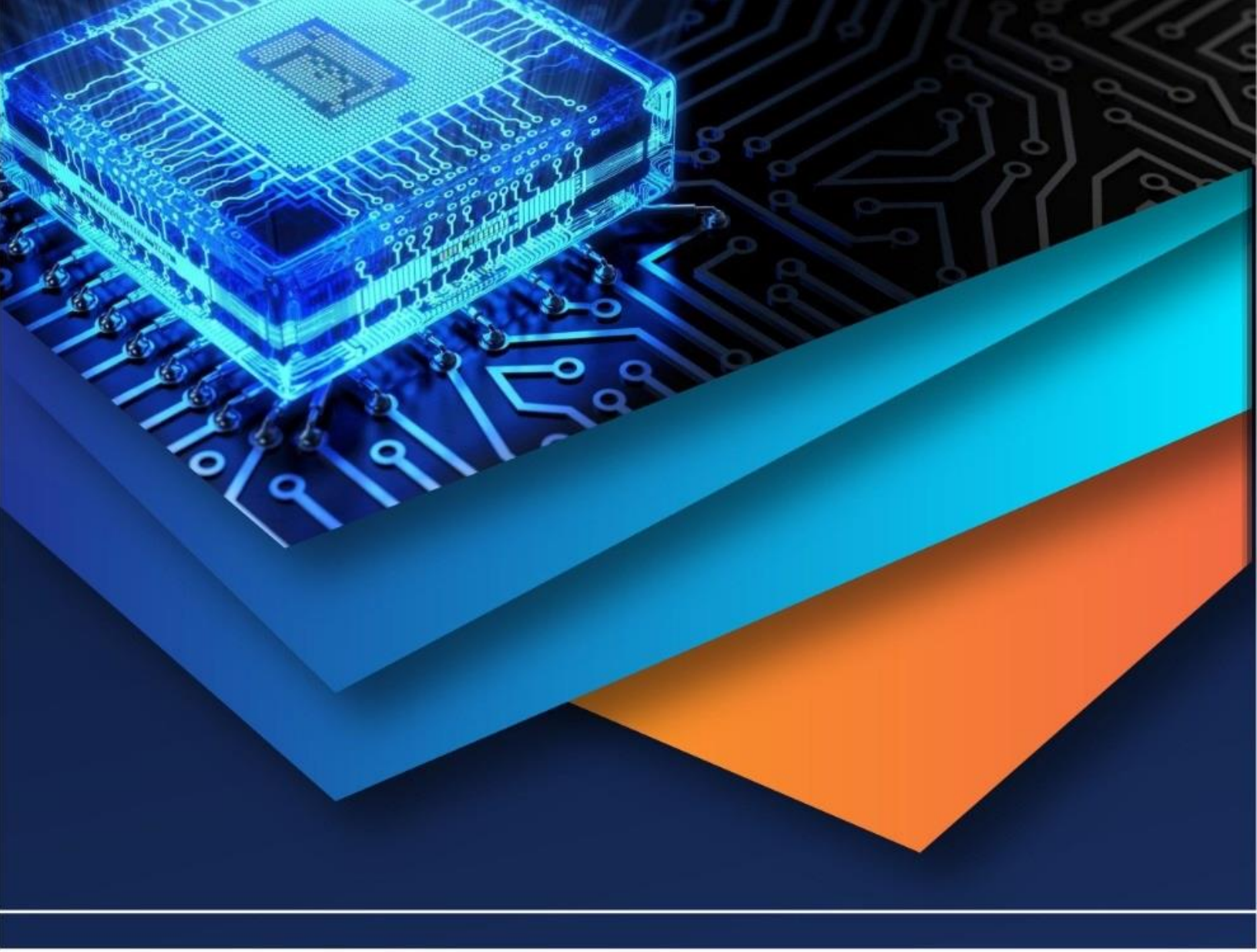
A blockchain-based security verification system for data sharing and storage is successfully implemented on WSN. A large amount of audible data is then shared with the clouds to maintain reliable and efficient data. Key parameters are also recorded in emerging blockchain technology to improve the consistency and transparency of the acquired data. A blockchain-based information storage system is used. Important information about all the sensor nodes is stored in the blockchain which is very difficult to break the attacker. Sharing a large amount of information in cloud storage ensures the reliability and efficiency of the proposed system.

IX. FUTURE ENHANCEMENT

In the future, we will strive to improve data management and framework resources for effective outcomes. We would like to point out that, similar to the unicast case, our one-sided travel models reach greater capacity than the two-sided models under the multi-channel traffic pattern. The advantage of low dimensional mobility is that it is simple and predictable, thus increasing the level of communication between. Although nodes are limited in motion only horizontally or vertically, the range of motion in their rotation lines is not limited. We plan to study the power enhancements that this hybrid dimensional model will bring in the future.

REFERENCES

[1] Y. A. Abdulrahman, M. Kamalrudin, S. Sidek, and M. A. Hassan,"Internet of things: Issues and challenges," Journal of Theoretical andApplied Information Technology, vol. 94, no. 1, pp. 52–60, 2016.
[2] SK Lo, Y Liu, SY Chia, X Xu, Q Lu, L Zhu, H Ning, Analysis of blockchain solutions for IoT: A systematic literature review, IEEE Access, vol. 7, 2019, pp. 58822-58835.
[3] R. V Kulkarni, S. Member, A. F¨orster, and G. K. Venayagamoorthy, "Computational Intelligence in Wireless Sensor Networks: A Survey," Communications Surveys & Tutorials, IEEE, vol. 13, no. 1, pp. 68–96, 2011.
[4] A. H. Bagdadee, M. Z. Hoque, and L. Zhang, "IoT Based Wireless Sensor Network for Power Quality Control in Smart Grid," Procedia Computer Science, vol. 167, pp. 1148–1160, 2020.
[5] J. Wang, Y. Cao, B. Li, H. jin Kim, and S. Lee, "Particle swarm optimization based clustering algorithm with mobile sink for WSNs," Future Generation Computer Systems, vol. 76, pp. 452–457, 2017.
[6] Z. Song-Juan and Y. Jian, "Distributed data storage strategy in wireless sensor networks," International Journal of Online Engineering, vol. 12, no. 11, pp. 52–57, 2016.
[7] L. Buttyan, D. Gessner, A. Hessler, and P. Langendoerfer, "Application of wireless sensor networks in critical infrastructure protection: challenges and design options Security and Privacy in Emerging Wireless Networks," IEEE Wireless Communications, vol. 17, no. 5, pp. 44–49,2010.
[8] R. Singh, D. K. Singh, and L. Kumar, "A review on security issues in wireless sensor network," vol. 2, no. 7, pp. 28–34, 2010.
[9] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 75–87, 2017.
[10] M. Wang and Q. Zhang, "Optimized data storage algorithm of IoT based on cloud computing in distributed system," Computer Communications, vol. 157, pp. 124–131, 2020.
[11] C. Feng, M. Adnan, A. Ahmad, A. Ullah, and H. U. Khan, "Towards Energy-Efficient Framework for IoT Big Data Healthcare Solutions," Scientific Programming, vol. 2020, pp. 1–9, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY