IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305473 |

Distributed Intrusion Detection System Using Blockchain Technology

Nikhil kumar M C[1], Anil kumar M U[1], Yashas N[1], Mahendra R[1], M R Suresh[2]

Undergraduate Students, Department of Information Science and Engineering, PES College of Engineering, Mandya, Karnataka, India[1]

Associate Professor, Department of Information Science and Engineering, PES College of Engineering, Mandya, Karnataka, India[2]

ABSTRACT: In the field of network and information security, the term "intrusion detection system" is well recognized It is among the crucial elements of the Network and Infrastructure for Information Security. While Network Intrusion Detection System (NIDS) assists in identifying intrusions and assaults on networks, Host Intrusion Detection System (HIDS) assists in detecting unauthorized use, anomalous, and malicious activity on the host. Numerous researchers have made significant progress in refining various strategies to enhance the IDS performance. But as numerous other technologies advance and new ones emerge, there are always opportunities to give IDS a cutting edge and strengthen its dependability. The creation of a distributed intrusion detection system (DIDS) employing cutting-edge and potentially useful technology is suggested in this study

I. INTRODUCTION

Within the field of network and information security, the term "intrusion detection system" is widely recognized. It is a crucial part of the infrastructure for network and information security. While Network Intrusion Detection Systems (NIDS) assist in detecting intrusions and assaults on networks, Host Intrusion Detection Systems assist in detecting unauthorized use, aberrant, and malicious activity on the host. Numerous researchers are actively pursuing various strategies to enhance the IDS performance, and significant progress has been made in this regard. Nonetheless, advancements in numerous different fields and recently developed methodologies consistently present chances to enhance and fortify intrusion detection systems (IDSs).

A hardware or software program that keeps an eye out for hostile activities or policy breaches on a network or systems is called an intrusion detection system. Typically, a security information and event management (SIEM) system is used to collect data centrally or to communicate any intrusion activities or violations to an administrator.

Attackers are using increasingly sophisticated and sophisticated methods to target the system and evade detection, as has been shown in recent days. Additionally, it's probable that the network administrator's focus will be diverted if an attacker compromises or misconfigures any portion of the network. A significant worry is the legitimacy of the logs and warnings received from each individual IDS because numerous IDS are connected to the centralized server. Therefore, blockchain technology can be effectively employed to maintain privacy.

How quickly the network can identify an attacker is the focus of the intrusion detection application. When an intruder approaches the network region, it can be quickly identified if sensors are put at a high density so that the totality of all detecting ranges covers the entire area. But implementing a high-density deployment strategy like this raises the cost of the network and might even be out of reach for a sizable region. Indeed, in many applications, a network with small, dispersed empty zones will also be able to detect a moving intruder within a specific intrusion distance, negating the need to deploy as many sensors to cover the entire network space.

IDS mainly works on two different approaches:

1. **Anomaly detection**: - In this technique, network traffic or host OS behavior is analyzed based on various parameters and compared with the normal behavior. If the system detects any deviation from normal behavior, it raises an alarm.
2. **Misuse/Signature detection**: - This technique looks for a specific pattern of behavior which is already known as an attack. All the malicious patterns and behaviors which are identified as attacks are stored in the IDS signature

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305473 |

database. These signature databases are continuously updated and used for attack detection. The limitation of this technique is that it will not be able to detect a novel attack, as a signature will not be available. Intrusion.

Detection Systems are broadly classified into two categories:

1. **Network Intrusion Detection System (NIDS):-** It captures the packets from network traffic. The header of the captured packets is analyzed based on various parameters to detect malicious activities. It can be set up in the network backbone, server, switches, and gateways.
2. **Host Intrusion Detection System (HIDS):**- It is installed on the individual system to detect the intrusion or misuse. HIDS analyzes the key system files, process behaviors, unusual resource utilization, unauthorized access, etc.

II. SYSTEM ANALYSIS

1. Distributed intrusion detection :

NIDS and HIDS are based on different methodologies, as was covered in the previous section. There are situations when using both kinds of systems is necessary to obtain complete protection. Many Network Intrusion Detection Systems are installed all over a huge network. The logs and alarm data are shared between these distributed IDS. A distributed intrusion detection system (DIDS) is an organization of several IDS. The administrator configures the kind and quantity of information shared among the distributed IDS; this configuration needs to be adjusted periodically. It makes network monitoring, immediate assault analysis of the entire network, and sophisticated persistent threat analysis easier. It facilitates the administrators' ability to see the network more broadly**.**

Some of the most important jobs include IDS alert analysis and network monitoring. Despite the fact that the security devices and although software can offer sufficient protection, one cannot fully rely on it. Attack patterns are constantly evolving. Attackers are continually coming up with new and inventive ways to avoid detection, therefore security devices need to be adjusted and patched appropriately. The administrators can better comprehend sophisticated assault patterns with the aid of a comprehensive network-wide threat and warning analysis. A signature or collection of guidelines may be produced as a result of the analysis. These can be given to certain IDS to shield the network segment from a future assault of that nature.

2. Incident analysis with DIDS:

The quantity of attacks is rising together with the size of networks. Finding the trespassers and malicious activity at the appropriate moment is the most significant and vital responsibility. It is necessary to understand how the attack started, where it started, what the attacker did, how dangerous it was, and how to stop it.

Regardless of the network segment in which the danger manifests itself, DIDS offers a centralized platform where it may be promptly identified. Although it provides the administrator with a centralized analysis advantage, it also necessitates careful planning and execution. Given that DIDS is the foundation of the entire network infrastructure, it must possess the strength, flexibility, and potential power to identify threats as soon as feasible.

3. Blockchain based intrusion detection:

Attackers are using increasingly sophisticated and sophisticated methods to target the system and evade detection, as evidenced by recent observations. Additionally, it's probable that the network administrator's focus will be diverted if an attacker compromises or misconfigures any part of the network. A significant worry is the legitimacy of the logs and alerts received from each individual IDS because numerous IDS are connected to the centralized server

4. NET Framework

A collection of Microsoft software technologies known as Microsoft.NET allows developers to quickly create and integrate Web solutions, Microsoft Windows-based applications, and XML Web services. A language-neutral platform for creating programs that can communicate with one other safely and readily is the.NET Framework. With.NET, there is no language barrier because developers may work in a variety of languages, such as Managed C++, C#, Visual Basic, and Java Script. The foundation for smooth component interaction, whether locally or remotely on multiple platforms, is provided by the.NET framework. In order to facilitate easy interoperability between components made in different languages, it standardizes common data formats and communications protocols.

Because the.NET Framework and Visual Studio.NET support multiple languages, developers may leverage their current programming knowledge to create a wide range of apps and XML Web services. In addition to several new members of

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305473 |

the family, the.NET framework offers updated versions of Microsoft's long-standing favorites Visual Basic and C++ (as VB.NET and Managed C++).

With numerous new and enhanced capabilities, Visual Basic.NET is now an even more potent object-oriented programming language. These features include overloading, interfaces, and inheritance, to name a few. In addition, multi-threading, custom attributes, and structured exception handling are now supported in Visual Basic. Additionally, Visual Basic.NET is CLS compliant, meaning that the classes, objects, and components you develop in Visual Basic.NET can be used in any language that complies with CLS.

Among the improvements contributed to the C++ language are attributed programming and managed extensions for C++. The process of converting current C++ applications to the new.NET Framework is made easier by managed extensions. Microsoft's new language is called C#. It's a language in the C style, or more accurately, "C++ for Rapid Application Development." Its specification is limited to the language's grammar, unlike other languages. It was built with the goal of leveraging the.NET libraries as its own and does not have a standard library of its own.

Other languages for which .NET compilers are available include

1. FORTRAN
2. COBOL
3. EIFFEL

III. SYSTEM DESIGN

1. Data flow diagram:

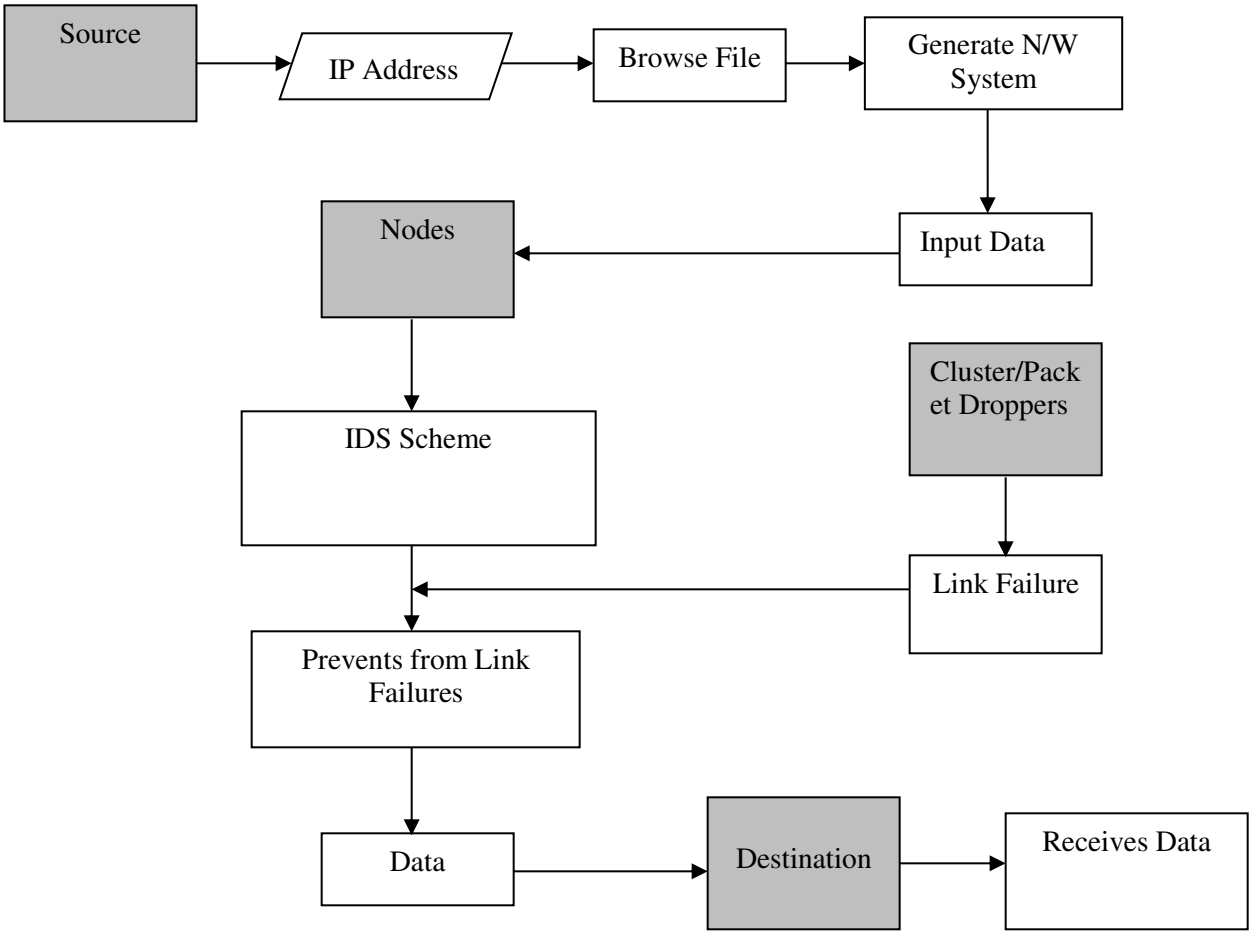

Fig 1:Data flow diagram

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305473 |

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

2. UML Diagrams:

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.
The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.
The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

3.class diagram:

.

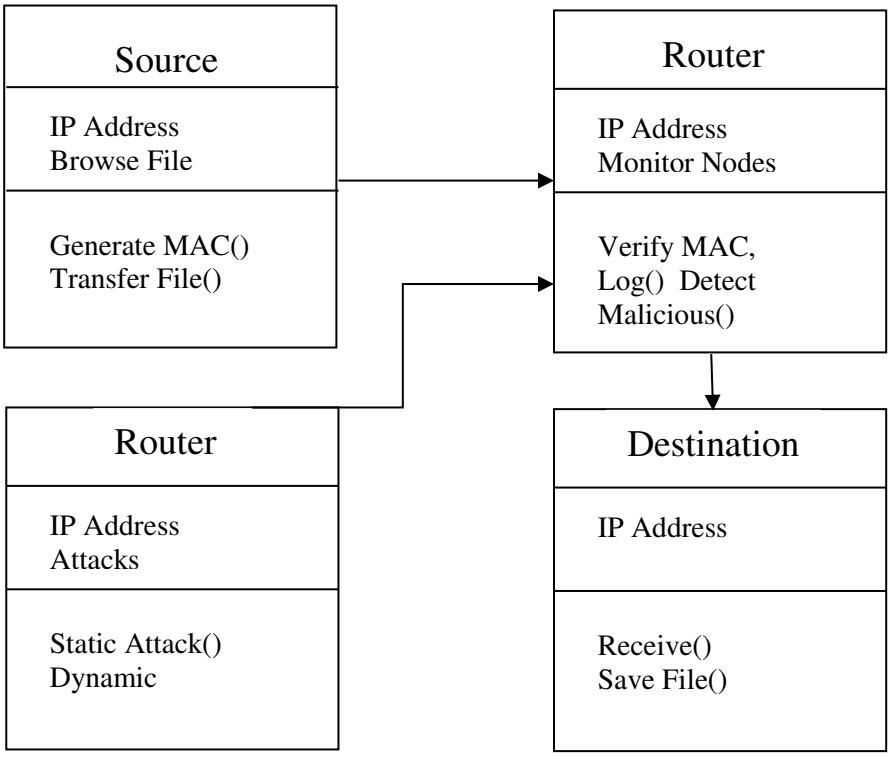

Fig 2:Class Diagram

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305473 |

IV. IMPLEMENTATION

1. Modules:

- Net.work Configuration
- Anomaly detection
- Misuse/Signature detection
- Network Intrusion Detection System (NIDS)
- Constructing Inter-Domain Packet Filters

2. Network Configuration:

In this project we are using Network System. Here we mainly focus on static or quasi-static network. In wireless network we need to send the packet through the node. System is represented as a node. Here every node has communication range. By using this range only we can transmit over packet.

3. Anomaly Detection:

In this technique, network traffic or host OS behavior is analyzed based on various parameters and compared with the normal behavior. If the system detects any deviation from normal behavior, it raises an alarm.

4. Misuse/Signature Detection:

This method searches for a particular behavioral pattern that is previously recognized as an attack. The IDS signature database contains all of the harmful patterns and behaviors that are recognized as attacks. These signature databases are used to detect attacks and are updated on a regular basis. This technique's drawback is that it can't identify a novel attack because there won't be a signature available.

The attacks in incoming traffic from IOT virtual clusters are detected by the fog nodes' intrusion detection system. A collection of IOT devices housed under one fog node is known as an IOT virtual cluster. Based on the training data, the algorithm determines whether the incoming packet is a normal or an attack. With x serving as the IOT traffic parameter and y serving as the output for n observations at each fog node, we are given a network traffic training data set D ={xi, Yi}Ni =1.

The initial parameters of the algorithm, which include the number of hidden layer neurons, the activation function g(x), random input weights wfi, and biases bfi for the hidden nodes, are fed into the training dataset D. These inputs are used to construct the initial hidden layer output matrix, which is then used to determine the initial output weights. The recursive least squares algorithm is used to calculate the most recent values of the hidden layer output matrix and output weight for each successive incoming packet from the Internet of Things traffic.

5.Network Intrusion Detection System (NIDS):

It captures the packets from network traffic. The header of the captured packets is analyzed based on various parameters to detect malicious activities. It can be set up in the network
Backbone,server,switches and gateway.

6. Constructing Inter-Domain Packet Filters:

The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. According port no only we are going to find the path is authorized or Unauthorized.
If the packet is received from other than the port no it will be filtered and discarded. This filter only removes the unauthorized packets and authorized packets send to destination.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305473 |

V. RESULT ANALYSIS

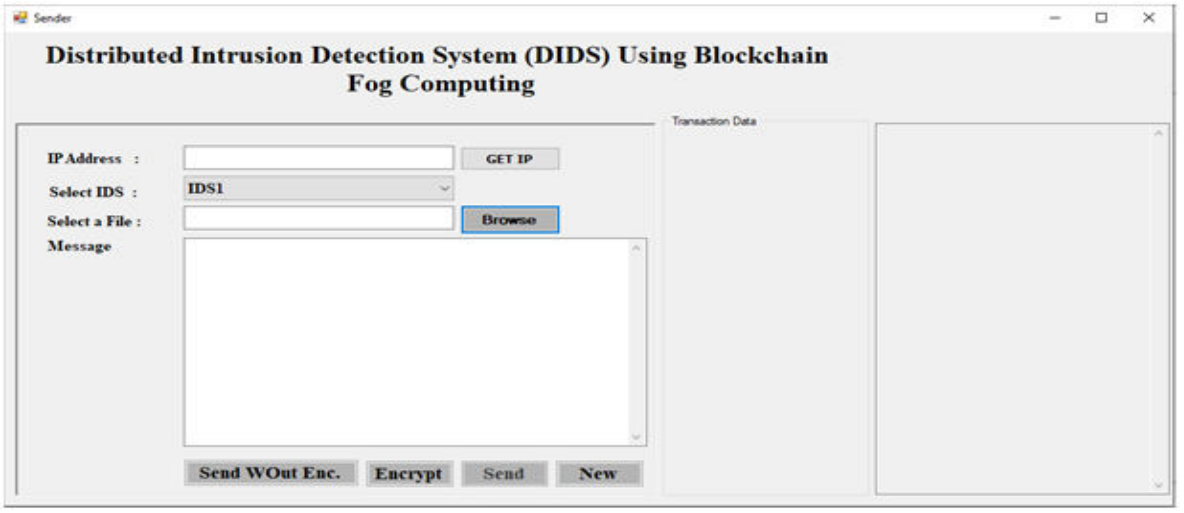

Fig 3:Sender Form

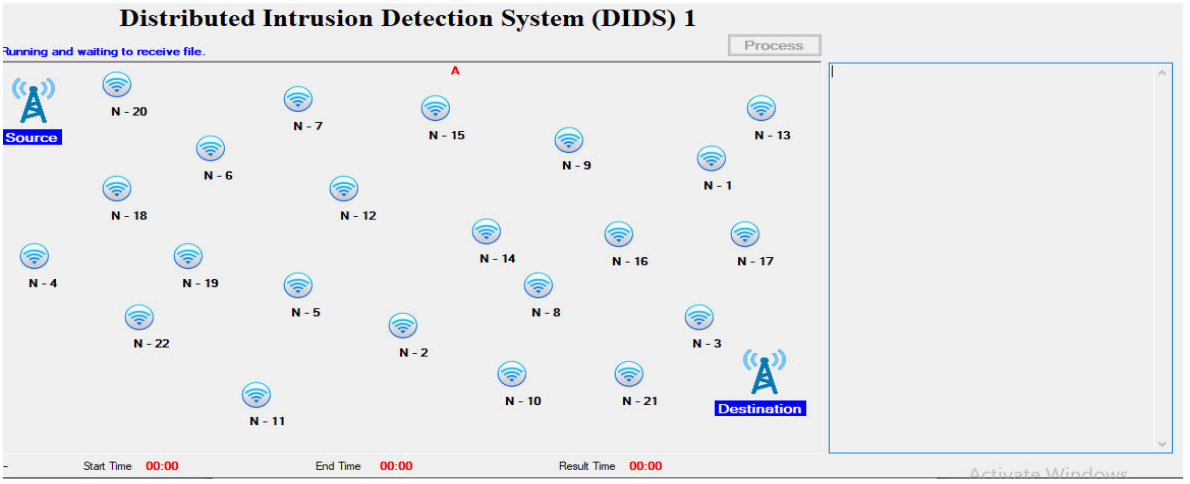

Fig 4:distributed Intrusion detection system

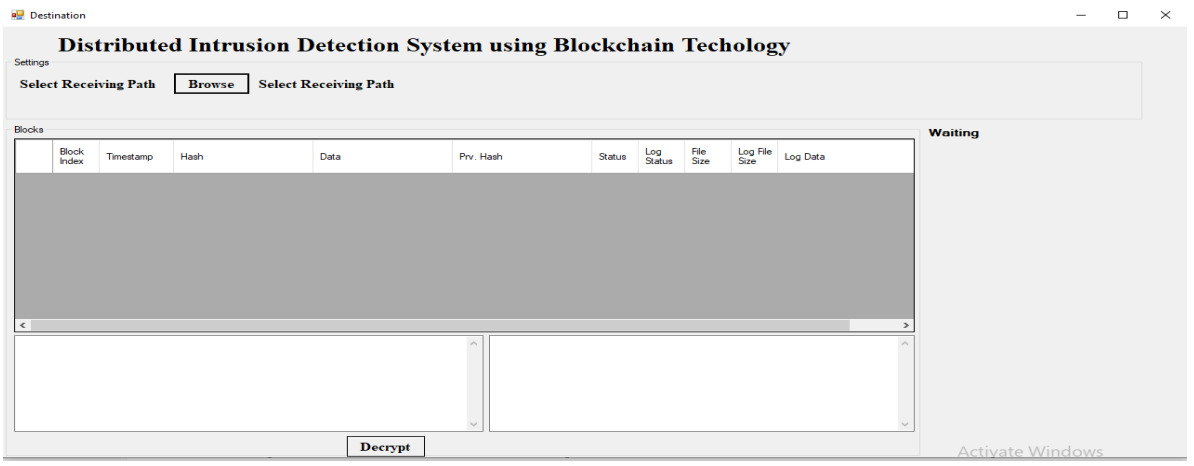

Fig 5: destination form

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305473 |

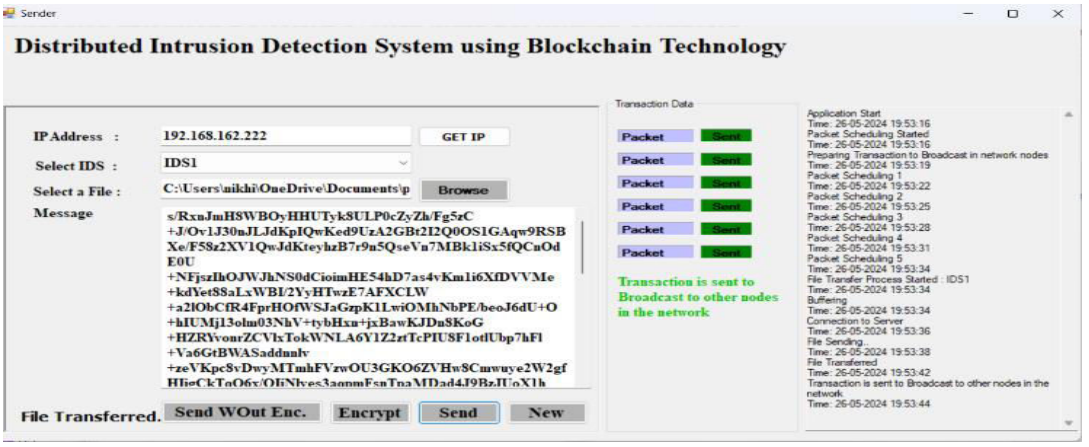

Fig 6:Sending data through IDS1

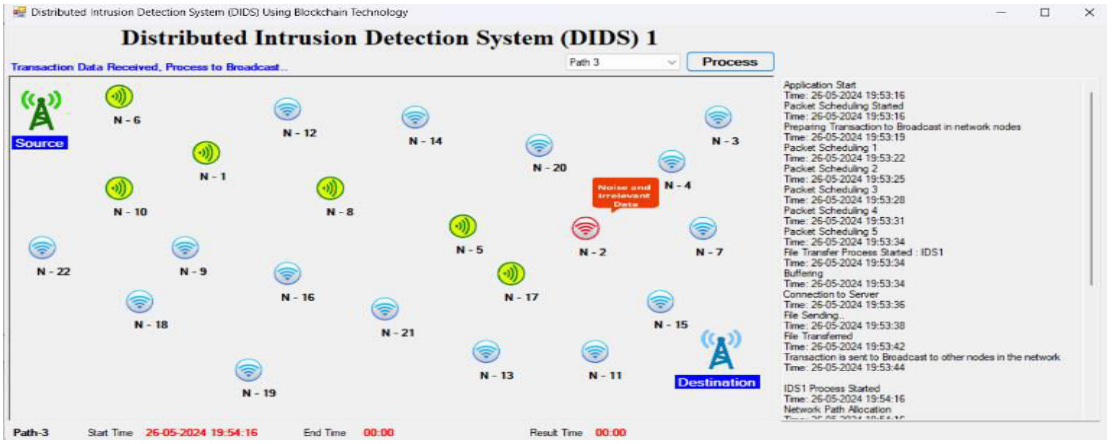

Fig 7: detecting intrusion in the network

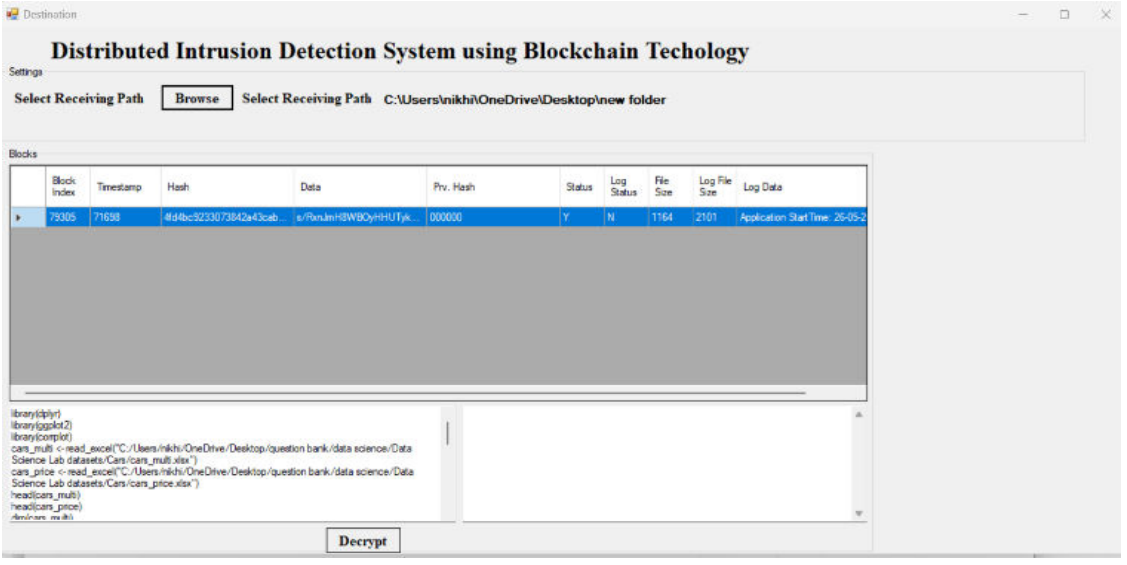

Fig 8:received file stored in Blockchain

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305473 |

VI. CONCLUSION

We have presented the architecture of the Distributed Intrusion Detection System using Cloud Computing Infrastructure and Blockchain. We have shown the performance of the DIDS server with a varying load of data. There are many other issues like communication delay, the overhead of blockchain, cost of implementation, etc.

REFERENCES

1. Titorenko and A. A. Frolov, "Analysis of modern intrusion detection system," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, pp. 142-143.
2. Alexopoulos, Nikolaos & Vasilomanolakis, Emmanouil & Réka Iványkó, Natália & Mühlhäuser, Max. (2018). Towards BlockchainBased Collaborative Intrusion Detection Systems: 12th International Conference, CRITIS 2017, Lucca, Italy, October 8- 13, 2017.
3. Axelsson, Stefan. Intrusion detection systems: A survey and taxonomy. Vol. 99. Technical report, 2000.
4. H. M. Anwer, M. Farouk and A. Abdel-Hamid, "A framework for efficient network anomaly intrusion detection with features selection," 2018 9th International Conference on Information and Communication Systems (ICICS), Irbid, 2018, pp. 157-162.
5. H.Debar, M. Dacier, and A. Wespi, “Towards a taxonomy of Intrusion Detection Systems”, Computer Networks, vol 31, n0. 8, pp. 805-822, 1999.
6. Holtz, Marcelo D. ; Bernardo David ; Sousa Jr., R. T. . Building Scalable Distributed Intrusion Detection Systems Based on the MapReduce Framework. Telecomunicacoes (Santa Rita do Sapucai), v. 13, p. 22-31, 2011.
7. J. Dean and S. Ghemawat, MapReduce: Simplified Data Processing on Large Cluster, USENIX OSDI,2004.
8. J. Yang, C. Shen, Y. Chi, P. Xu and W. Sun, "An extensible Hadoop framework for monitoring performance metrics and events of OpenStack cloud," 2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA), Shanghai, 2018, pp. 222-226.
9. K. Kato and V. Klyuev, "Development of a network intrusion detection system using Apache Hadoop and Spark," 2017 IEEE Conference on Dependable and Secure Computing, Taipei, 2017, pp. 416-423.
10. Konstantin Shvachko, Hairong Kuang, Sanjay Radia, and Robert Chansler, “The Hadoop Distributed File System,” IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST), pp.1-10, 2010.
11. S. Ghribi, A. M. Makhlouf and F. Zarai, "C-DIDS: A Cooperative and Distributed Intrusion Detection System in Cloud environment," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, 2018, pp. 267-272.
12. Suah Kim, Beomjoong Kim, and Hyoung Joong Kim. 2018. Intrusion Detection and Mitigation System Using Blockchain Analysis for Bitcoin Exchange. In Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things (CCIOT 2018). ACM, New York, NY, USA, 40-44.
13. W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," in IEEE Access, vol. 6, pp. 10179-10188, 2018.
14. Yeonhee Lee and Youngseok Lee. 2012. Toward scalable internet traffic measurement and analysis with Hadoop. SIGCOMM Comput. Commun. Rev. 43, 1 (January 2012), 5-13.
15. Zohreh Abtahi Foroushani and Yue Li. 2018. Intrusion Detection System by Using Hybrid Algorithm of Data Mining Technique. In Proceedings of the 2018 7th International Conference on Software and Computer Applications (ICSCA 2018). ACM, New York, NY, USA, 119-123.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details