International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain-Enabled Decentralized Edge Computing in Cyber Security for Intrusion Detection

[1]Prof. Priyanka Patel, [2]Dr. Ruby Bhatt, [3]Prof. Manish Joshi, [4]Prof. Govinda Patil, [5]Dr. Hemant Pal, [6]Dr. Abdul Razzak Khan Qureshi

Submitted: 25/11/2023 **Revised**: 05/01/2024 **Accepted**: 15/01/2024

Abstract: The foundation of our modern society is an ever-expanding digital ecosystem; nevertheless, this ecosystem is also one that is continuously vulnerable to the threats posed by cyberattacks. The fact that intrusion detection is tasked with identifying and stopping unauthorised access to computer networks and systems has made it abundantly obvious that it is one of the most important aspects of cybersecurity in its entirety. On the other hand, due to the centralised architecture of old intrusion detection systems (IDS), it may be difficult for these systems to respond quickly and effectively to the complex nature of modern cyber threats because of the nature of the design itself. This unique technique makes an attempt to resolve some of the pressing problems that plague traditional intrusion detection systems. These problems include vulnerabilities caused by a single point of failure, data integrity concerns, and scalability concerns. This study presents a brand-new distributed intrusion detection system (IDS) that makes use of fog computing in order to recognise DDoS assaults against mining pools in blockchain-enabled IoT networks. Finding answers to the problems that were discussed before is the reason for doing this research in the first place. Random Forest (RF) and an updated gradient tree boosting approach (XG Boost) are used in order to conduct the performance evaluation of distributed fog nodes. On the basis of the use case of video analytics at the edge, an experimental configuration for an Internet of Things edge solution using the Hyperledger Sawtooth Blockchain has been constructed.

***Keywords**: Blockchain, Edge Computing, Cybersecurity, Intrusion Detection, Decentralization.*

1. Introduction

The present digital world is characterised by an extremely large volume of data as well as an increasing dependence on devices that are connected via networks. Due to the fact that the information on which our modern civilization is growing an increasing amount more dependent is becoming an increasing amount more vulnerable to the continual risk posed by cyberattacks, it has become absolutely essential to defend these precious digital assets. Intrusion detection is an essential part of cybersecurity since it allows for the identification and prevention of unauthorised access to computer networks and systems. This can only be accomplished by being vigilant and watching out for dubious behaviours. On the other hand, traditional intrusion detection systems (also known as IDS) often struggle to keep up with the constantly morphing and more sophisticated nature of modern cyberthreats. The deficiencies of traditional IDS may be attributable to the fact that their design is largely centralised, which results in a variety of problems that are inherent to the system. These limitations include concerns with scalability, latency, and single points of failure, all of which may be exploited by malicious attackers. Single points of failure are particularly dangerous since they allow for just one point of failure. At the intersection of blockchain technology and decentralised edge computing, a creative solution to these vulnerabilities as well as a method to reinforce our cyber defences have emerged as feasible responses to the questions that have been raised. This cutting-edge combo promises to revolutionise the intrusion detection sector of the cybersecurity industry by simultaneously lowering the dangers presented by centralised systems and enhancing the area's resilience, scalability, and efficacy [1].

This in-depth study analyses the paradigm shift in cybersecurity brought about by blockchain technology, which enables decentralised edge computing. A significant focus of the investigation is placed on the use of this technology in the detection of intrusions. This approach represents a big step forward in the continuing fight against cyberthreats since it takes use of the

[1]*Assistant Professor, Department of Computer Science and Engineering, Medi-Caps University, Indore, MP, India, 453331 priyanka.patel@medicaps.ac.in*
[2]*Assistant Professor, Department of Computer Science, Medi-Caps University, Indore, MP, India, profrubybhatt15@gmail.com*
[3]*Assistant Professor, Department of Computer Science, Medi-Caps University, Indore, MP, India, manish_riya@Yahoo.co.in*
[4]*Assistant Professor, Department of Computer Science, Medi-Caps University, Indore, MP, India, patil.govinda1976@gmail.com*
[5]*Assistant Professor, Department of Computer Science, Medi-Caps University, Indore, MP, India, hemantpal.scs@gmail.com*
[6]*Assistant Professor, Department of Computer Science, Medi-Caps University, Indore, MP, India, dr.arqureshi786@gmail.com*

distributed ledger capabilities offered by blockchain technology as well as the computational power offered by edge devices. In the following pages, we will make an effort to analyse any potential advantages that blockchain-enabled decentralised edge computing may have over more conventional approaches, as well as explain the fundamental concepts that underpin them. We are going to conduct an in-depth analysis of the inner workings of the new paradigm, dissect its essential components, and investigate how it improves intrusion detection systems. In addition to this, we will evaluate the current state of research and development, explore the implications of this convergence for the development of cybersecurity, and demonstrate real-world applications that illustrate how effective cutting-edge fusion may be. In a time when the digital world is transforming at a rate that has never been seen before, decentralised edge computing combined with blockchain technology is a glimmer of hope that points the way to a brighter future. This combination of technologies is an indication of the way forward. This combination may safeguard our interconnected world in ways that were not feasible in the past and may alter the boundaries of intrusion detection. Our never-ending mission to keep the digital world secure enters a new phase with this exploration of the convergence of blockchain technology, decentralised edge computing, and cybersecurity [2].

The statement "provides an IT service environment and cloud-computing capabilities at the edge of the mobile network, within the Radio Access Network (RAN), and in close proximity to mobile subscribers" is used to describe the technology known as mobile edge computing (MEC). This idiom refers to modern technological advancements. The lightning-fast pace at which technology has advanced has led to the emergence of a new paradigm. As a result of this shift in paradigm, the capabilities of computing and the services that were before provided by the cloud are now moved to locations that are closer to the "edge" of the mobile network. As a result of the meteoric growth in the number of mobile devices, conventional forms of centralised cloud computing are no longer able to provide the quality of service (QoS) that a great number of applications need. The processing and storage resources for the internet's edge base station, which is located in close proximity to end devices, are provided by MEC in the form of cloudlets, fog nodes, or tiny data centres. This edge base station is located at the internet's edge. This makes it easier for the system to prevent hiccups and other kinds of faults. Reducing network latency, improving network efficiency, and guaranteeing consistent service delivery are the primary objectives with the final aim of providing customers with an improved experience overall. In order for users of delay-sensitive applications like virtual reality (VR) and augmented reality (AR) to satisfy the stringent delay requirements of their apps, they may quickly connect to the edge network of the cloud service that is located closest to them. Moving resources closer to the edge of the network provides a number of benefits, including a reduction in latency, an increase in mobility, and a heightened awareness of position. MEC is required in order to enable the growing deployment of new applications by the Internet of Things (IoT), the tactile internet, and the next generation of cellular networks (5G). It satisfies the stringent needs of 5G and the Internet of Things by improving scalability, lowering latency, boosting automation, and increasing throughput. It paves the way for multiple new use cases, business possibilities, and value chains in a wide variety of different sectors of the economy [3].

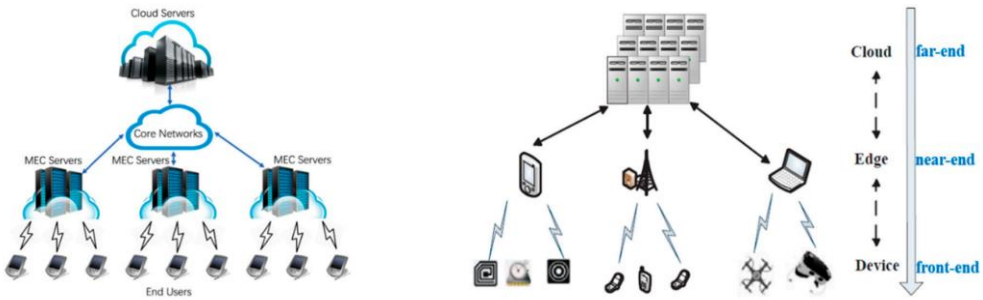

Fig 1: (A) BASIC EDGE COMPUTING ARCHITECTURE AND (B) TYPICAL ARCHITECTURE OF EDGE COMPUTING NETWORK.

The structure of edge computing is shown in Figure 2a; in contrast to cloud servers, edge servers are located in locations that are more physically accessible to end users. Its architecture may be roughly broken down into three levels: the front end, which is made up of end devices; the near end, which is made up of edge servers; and the far end, which is made up of the core cloud. Each level has its own distinct set of components. Figure 2b depicts a hierarchical structure that provides a rapid sense of how the different levels' computing talents compare to one another and shows how they differ from one another. It is the responsibility of the front end to install end devices

such as actuators and sensors in order to improve the level of responsiveness and engagement offered to end users. Devices that work at this level must send queries to the edge servers in order to satisfy demand because of the restricted capacity of the devices themselves. Edge servers, which are positioned as gateways on the near end, are responsible for the duty of transmitting and distributing the traffic that goes over the networks. Edge servers are located on the near end. The edge servers could also be able to provide the resources required for real-time data processing, data caching, and offloading computation. The bulk of the processing and storing tasks will be shifted closer to the near end of the facility in order to optimise speed and maximise the capacity of the available storage space. Cloud servers have more powerful processing and storage capacity, despite the fact that they are physically farther away from end users. However, because of their geographical isolation, cloud servers are subject to a significant degree of transmission latency. At this level, many different approaches to processing data may be used. Some examples of these approaches include massively parallel processing, machine learning, big data mining and management, to mention just a few. While edge server applications synchronise the data with the main cloud for long-term storage, the primary emphasis of this architectural design is on the execution of mission-critical, computationally costly, and delay-sensitive operations for customers at the edge. In other words, the execution of these tasks at the edge is where the action [4].

2. Review of Literature

Fog computing is increasingly becoming popular as an extension of cloud computing and as a major component of the Internet of Things (IoT) due to its capacity to tackle various troublesome problems such network congestion, latency, and local autonomy. These issues are only some of the issues that fog computing can handle. This is due to the fact that fog computing might assist to alleviate some of these issues. The performance of fog computing is, however, being hampered by worries over the users' privacy as well as the resulting inefficiencies. When discussing cases of poisoning, the vast majority of the works that are now available on the market almost always take into consideration a fair equilibrium between them. We propose a cutting-edge approach that we term blockchain-enabled federated learning (FL-Block), with the goal of bridging the knowledge gap and overcoming the difficulties outlined above. FL-Block enables local learning updates of end device exchanges by using a global learning model that is constructed on a blockchain and validated by miners. By using the proof-of-work (PoW) consensus technique that the blockchain provides, the FL-Block makes it possible for autonomous machine learning to be employed without the requirement for a centralised authority to coordinate and maintain the global model. This is made possible by the FL-Block. In addition, we investigate the latency performance of FL-Block and determine the optimal rate at which blocks are created by taking into consideration the delays that are associated with communication, consensus, and processing. The analysis of FL-Block's performance demonstrates that it performs very well in terms of protecting the privacy of its users, maximising the efficiency of its operations, and withstanding the attempts of those who would poison it [5].

With the assistance of the Internet of Things (IoT), a brand-new technology, developers are now working on the development of a variety of important applications. On the other hand, these applications continue to depend on centralised storage architecture and are confronted with a number of serious challenges, the most evident of which are concerns about the users' privacy and security. In recent years, the growth of applications for the Internet of Things (IoT) has been helped along by the use of block chain technology. The establishment of a block chain may be able to overcome the issues of privacy, security, and having a single point of failure that are associated with the dependency of Internet of Things applications on third parties. There is a possibility that individuals as well as society as a whole might benefit from the marriage of blockchain technology with the internet of things. On the other hand, a Distributed Denial of Service (DDoS) attack that took place in 2017 against a mining pool revealed the most significant flaws in the blockchain-powered Internet of Things network. In addition, a tremendous amount of data is generated by using this application. Machine learning, which is often referred to as ML, is used as an analytical tool since it enables full autonomy in the processing of enormous amounts of data and provides decision-making capabilities. In this research, we propose a novel distributed intrusion detection system that makes use of fog computing in order to identify DDoS attacks that have been launched against mining pools that are enabled for blockchain technology. The purpose of this investigation is to come up with a solution to the problems that were discussed before. In order to keep an eye on performance, fog nodes are trained using Random Forest and the XGBoost gradient tree boosting technique. These nodes are dispersed throughout the network. The usefulness of the proposed technique is evaluated with the use of a real dataset based on the internet of things (IoT) known as BoT-IoT. The most recent attacks found in blockchain-powered IoT networks are included in this dataset, which is used to analyse the data. According to the findings, XGBoost is superior over Random Forest when it comes to distinguishing binary attacks, but Random Forest is superior when it comes to recognising multiple attacks. When compared to XGBoost, the amount

of time needed to train and test RF on dispersed fog nodes is much shorter [6].

As the Internet of Things (IoT) becomes more widespread, there are an increasing number of things that are capable of establishing a connection to the internet. The Internet of Things (IoT) sensors produce a sizeable volume of data, which necessitates a considerable number of resources for the processing of analytics. Because to edge processing, it is now feasible to process sensor data at a distance that is substantially closer to its original source than was previously possible. The building of infrastructure that requires a significant amount of resources outside of a metropolitan area is not always practical or cost-effective. According to the findings of this research, the optimal method for enabling edge processing for IoT devices is to use decentralised software that is based on a blockchain. Given the current configuration, a resource owner might potentially join the ecosystem and make their processing power available as needed, according to the theory. When it is absolutely essential, edge processing may be offloaded from devices linked to the internet of things to the nodes that are managing the resources. This article discusses the architectural components as well as the general strategy for carrying out the project. On the basis of the use case of video analytics at the edge, an experimental configuration for an Internet of Things edge solution using the Hyperledger Sawtooth Blockchain has been constructed [7].

This article provides a description of the future research paths that will be taken in the field of blockchain applications for cyber security. Despite the fact that almost all of the research on blockchain cyber security has indicated that the security of Internet of Things (IoT) systems may be revitalised if it is backed by blockchain, Internet of Things security has still been regarded as a critical industrial necessity. This is the case despite the fact that almost all of the research on blockchain cyber security has shown that. At this moment, the decision-making process, the practicality of putting the technology into practise, and the ways in which it may be utilised realistically to solve existing IoT security problems and threats are not well understood or managed. Moreover, there are a variety of methods in which it may be used to address these issues. As a direct consequence of this, the particular location in question offers the opportunity for creative expression as well as the generation of new vectors. Therefore, future research has to incorporate quantitative ideas and methods that might contribute to the process of filling in the blanks in the existing body of knowledge. There is also the potential for the development of blockchain-based solutions for Internet of Things devices that have limited resource capacity and operate independently of a computer network [8].

The transactions carried out over a network of computers are recorded on the blockchain, which is a decentralised and open ledger. Almost every industry, including banking and healthcare, as well as real estate, tourism, and the supply chain, may one day use cryptocurrencies like Bitcoin and Ethereum. Among these industries are also real estate and tourism. The following is a literature review that we are doing for the innovative concept of reinforcement learning integrated into an autonomous supply chain in the most effective manner: Take into consideration the following as an illustration: How the distributed ledger technology, often known as blockchain, may be used to artificial intelligence to improve its trustworthiness, data security, and transparency. Calculations made by AI might be applied to the diagram database in order to find possible answers to problems requiring designs and information, arrange those answers, and make predictions about those problems. It may be said that the benefits of our earlier communications are analogous to those of the deep assist learning strategy that is outlined. contrast reasonable thinking with the route and control based on security, both of which utilise flawed future methods. In order to have a complete grasp of defence, it is vital to be familiar with a wide variety of techniques, such as independent driving and fooling prospective fields. The authors stressed that the board-related problem of the store network influences how product development and the procurement of raw materials must proceed in order to prevent financial waste and illogical expenditures. This was done in order to avoid wasting money and spending in a manner that was not reasonable.

Because of the pecking order of food, the planning process, certain contagions, and distribution were all done behind the backs of the person who made the product as well as the customer. According to the authors' network of Halal inventory, the process of making anything halal must start from the time it is granted and continue until it is in the hands of the recipient. The following assertion will give further information about this tactic. In the present day, the chain of halal inventory has to begin at the farm and the butcher shop, and it needs to continue with the setting aside of the chicken products before the recipient comes. As was said earlier, it is very important to take the necessary steps to guarantee that a particular interpretation of the word "halal" does not apply to any products or meals, with the exception of all activities that take place inside a building that is designed for the management and preservation of goods. In this case, the only exemption is activities that take place within a structure. The authors in addressed how a Chain of Halal Food Supply may operate over an association blockchain by drawing on the existing mechanical, engineering, and other components as well as application components. This was done using the components that already existed. This

was done out in a manner that is consistent with the requirements of the application's components. This contains the appliance for the grant and details segment, the empowerment of details safety, and the kind feature of the peer-to-peer system. Customers are finally able to access more information and make more informed decisions as a direct result of the ability of the Shared Registry Mechanism to improve confidence among the many parties involved in the supply chain [9].

In their research, looked at the usage of Blockchain technology to investigate the ongoing process of developing new agreement designs and how such designs are implemented in supply chains. The recommended tactic produces an environment in which a powerful approach is used to cooperate with the operation and management firm while also coordinating the devious concurrence. When the concurrence phase was finally accomplished without any problems, the approach began to gain greater popularity. embedding state-controlled components into blockchain-based processes, taking command of computerised data inputs, monitoring the execution of contracts, and keeping an eye out for disruptions are all examples of this. The authors defined the agricultural supply chain as having traceability thanks to the technology of blockchain. The findings of the inquiry do provide specialists with assistance in developing strategies for making use of blockchain technology in agriculture, which will ultimately result in a supply chain for agricultural goods that is knowledge-driven. The ultimate findings ought to be valuable in the process of developing legislation for the rapid implementation of blockchain technology, which has the ability to sanitise and clean up the agricultural supply chain. An architecture for managing supply chains that is based on blockchain technology has been created by the authors for use in international online commerce. In the event that a copy strike, forgery label strike, or forgery result strike occurs, the management of the supply chain will be handled properly thanks to this technology. Planning is an essential component in the management of the supply chain because it ensures that the distribution of the completed product from the point of origin to the final consumer is precise and error-free. This particular supply chain has had good development in the sense that the level of pain experienced by the consumer has decreased. On the other hand, the strategy for survival anticipates that a few stray events (such as damaging goods as a result of bad luck or introducing cross-infection into the product) may occur as a consequence of such accidents, which would result in the consumers feeling upset. Examples of such occurrences include damaging items as a result of bad luck or bringing cross-infection into the product. Because of this allusion, the relevant developer or producer fears that their firm will suffer financial loss as a consequence [10].

3. Edge Computing in Cyber Security

Computing power in the network's periphery is absolutely necessary for enhancing network security in a variety of different ways. In this day and age of advanced digital technology, it denotes a significant shift in the manner in which data is saved, assessed, and protected. In the field of cybersecurity, some applications for edge computing include the following (Figure 2):

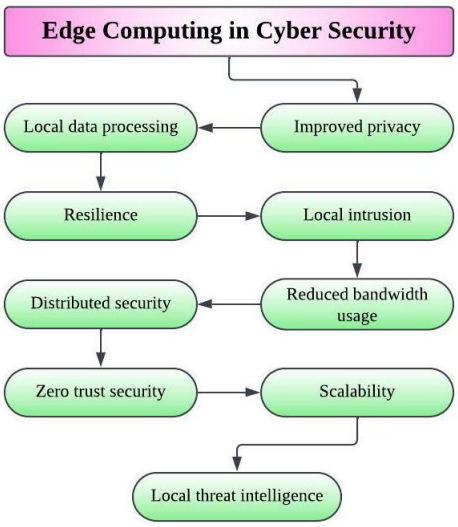

Fig 2: EDGE COMPUTING IN CYBER SECURITY

❖ **Improved Privacy:**

Edge computing allows for data processing to take place locally or directly on the device, which improves privacy by reducing the need to transport sensitive data over the internet. Edge computing is also known as fog computing. Computing at the edge of a network makes it possible to do data processing at a distance. This is of the utmost relevance for apps that deal with personal or confidential information.

❖ **Local Data Processing:**

It is not necessary for information to be transported to a centralised server or to the cloud in order for edge devices to be able to handle data on their own locally. This local processing lessens the likelihood that sensitive data will be exposed while it is being carried. As a result, it will be more challenging for cybercriminals to read and alter the data in transit.

❖ **Resilience:**

In terms of their resilience to invasions, decentralised edge networks offer an advantage that is already built into them. If just one of the network's edge devices is hacked, the network may not be susceptible to an attack. As a result of this decentralisation and redundancy, it is far more difficult for adversaries to hinder operations or acquire unauthorised access.

❖ **Local Intrusion Detection:**

Edge devices that are able to locally host intrusion detection systems (IDS) have the capacity to monitor system activity and network traffic in real time. This makes it feasible for businesses to prevent cyberattacks. As a direct consequence of this, it is now quite easy to recognise strange behaviour and potential dangers in a timely manner.

- **Distributed Security:**

It may be possible for computers at the network's edge to offer many degrees of security if various security methods are dispersed across the network. It is possible that this strategy might prevent attacks at a large number of network nodes, so making it more difficult for attackers to pinpoint vulnerable areas.

- **Reduced Bandwidth Usage:**

By performing data processing and filtering operations on a local level, edge computing has the potential to dramatically cut down on the volume of data that must be sent over a network. As a consequence of this, it will be more difficult for attackers to gain control of the network since the attack surface will be reduced and the bandwidth will still be available.

- **Zero Trust Security:**

Edge computing is aligned with the Zero Trust security paradigm, which recognises the possibility that attacks may originate from both within and outside the network. When it comes to security, Zero Trust puts a significant amount of importance on measures such as stringent identity verification and continual monitoring, both of which are made feasible by edge-based security strategies.

- **Scalability:**

Edge computing offers a great degree of scalability, which makes it simple for enterprises to expand their cybersecurity infrastructure. As the network grows, there is a possibility that there will be a need to deploy more edge devices in order to stay up with the continuously shifting cybersecurity threats.

- **Local Threat Intelligence:**

Edge devices that make use of threat intelligence feeds and databases may be able to recognise and defend against known threats without having to rely only on centralised security updates if they are given the ability to do so.

Computing in the periphery is becoming an increasingly important component of modern cybersecurity systems. It delivers benefits such as lower latency, higher resilience, more privacy, and the ability to process data locally. All of these advantages work together to give a more effective and adaptable defence against cyber threats. As the digital landscape continues to evolve, edge computing will play an increasingly important part in the effort being made to maintain the safety of our interconnected world.

4. Research Methodology

Within the realm of cybersecurity, the purpose of this investigation was to investigate whether or not blockchain technology might provide decentralised edge computing in a fashion that would make it possible for enhanced intrusion detection. In order to get a comprehensive comprehension of this cutting-edge paradigm, our investigation into it made use of a variety of methodologies. In order to collect all of the necessary data, there were three primary steps that needed to be taken. An exhaustive literature review was performed initially in order to provide a summary of the information that was previously accessible about blockchain technology, edge computing, and intrusion detection in the field of cybersecurity. This was done in order to offer an overview of the knowledge that was previously available. The findings of this corpus of previous research will serve as the foundation for our investigation. Reinforcement learning (RL) and deep reinforcement learning (DRL) are two forms of machine learning that are used in the process of developing algorithms that are utilised for assessing trust and distributing processor resources on edge servers. Both types make use of Bayesian inference and attempt to optimise the number of central processing units (CPUs) in order to evaluate the service reputation of edge servers and reduce the amount of computing resources that these servers need. Computing performance may also be improved by using convolutional neural networks (CNNs) to reduce the size of the state space and a modified Boltzmann distribution to establish the optimal number of central processing units (CPUs). Both of these approaches are described in the statement that came before that. A group known as CBACSEIOT has proposed a broad ecosystem for the Internet of Things that would use blockchain technology to make access control feasible. This system incorporates both the phases of key management that take place between edge servers and cloud servers and the phases of access control that take place between devices and gateway nodes. Defending against attacks such as identity-revealing attacks, session hijacking attacks, relay attacks, and man-in-the-middle attacks is now possible thanks to the combination of blockchain technology and edge computing, which creates a security system for the storage and access of data in a completely decentralised architecture. This architecture makes it possible to protect against these types of attacks. In the following table, Table 1, a summary of the most important results from the study on a blockchain-based security layer for edge computing is provided.

Table 1: Blockchain-Based Security Layer For Edge Computing

Applications	Purposes	Contributions	Other Supporting Technologies
Resources Management	Developing an environment that is self-organizing, safe, and logical in the cloud and at the edge should be a primary focus.	In order to stimulate the participants' interest in the activity, the challenges are first broken down, then the ALLSTAR method and its four subsystems are described, and finally a business model is developed.	Machine Learning (ML),Cloud Computing
Resources Management	helping to simplify the process of deploying resources, managing them, and monitoring them for applications related to the Internet of Things.	The publication of the FogBus framework occurred along with the completion of research on a use case that called for the continuous monitoring of sleep apnea. This framework offers specialised modules and services to facilitate the interaction of disparate Internet of Things-based devices with fog and cloud computing environments.	Cloud Computing Fog Computing
Resources Management	resolving the challenges that arise in cloud computing as a consequence of service failures, rivalry for resources, and a decline in performance.	Additionally, we provide a multi-objective optimisation problem model as well as an NSGA-III resource provisioning solution that is based on blockchain technology and edge computing. This is done in order to increase people's awareness of the process's inherent unpredictability.	NSGA-III
Management of Caching	creating communications that are very reliable for the MEC in terms of their accessibility, connectivity, and ability to last for an extended period of time.	In the current day, research and development efforts are being focused on the creation of neural networks for a blockchain-based intelligent content transit system as well as smart contracts for the caching capabilities of unmanned aerial vehicles (UAVs).	Neural Network. UAV
Mechanism for Building Trust	guaranteeing dependability throughout the whole	BlockEdge is a collaborative edge computing system that utilises blockchain	No

	process of collaborative edge computing.	technology. BlockEdge is capable of using distributed ledgers. BlockEdge was developed to operate on top of the Ethereum network. a management structure for both awards and reputation	
Mechanism for Building Trust	reducing the amount of resources used by the standard blockchain, speeding up the network, and addressing any possible vulnerabilities that may exist are some of the goals of this project.	In light of concerns about the veracity of distributed ledgers, the development of Trustchain, a blockchain that provides users with permissioned privacy protection and is made feasible by edge computing, came about.	No
Mechanism for Building Trust	The safekeeping of data and the efficient processing of information are both essential elements of MEC.	A trust mechanism that is based on blockchain technology is now in the process of being created in order to guard against assaults that are based on faked service records and self-serving edge attacks. DRL is also being used in the process of deciding how to allocate the available computer resources.	DRL
Access Restrictions	providing encrypted communication across several entities operating inside an Internet of Things network with an edge-focused orientation.	the establishment of a consortium access control system that is predicated on blockchain technology with the intention of providing mutual authentication on a number of different levels inside of an environment that is predicated on the edge of the Internet of Things.	No
Authentication	Utilising edge computing while maintaining the confidentiality of user data and protecting user privacy	proposing the use of the decentralised security system that is powered by Dec-Chain for the authentication of users, storage of data, and access by users to the data that has been saved.	No

❖ **Ethical Considerations:**

In this procedure, ethics was a very important factor. In order to ensure that everyone who took part in the survey did so voluntarily, we made careful to ask each responder many times for their informed consent before moving on to the next question. During the whole of our testing, we

did not make use of any real-world data or systems and instead deployed stringent data anonymization procedures instead.

❖ **Limitations:**

We are aware that the procedures used in the research have a number of important limitations. The very small number of people that participated in the survey might be to blame for the restricted generalizability of our findings. In order to produce controlled settings, we began by simplifying and then abstracting the simulation experiments. As a direct result of this, it is probable that the level of complexity that exists in the actual world is not adequately reflected in the surroundings that are strictly controlled. In addition to this, it's probable that some of the respondents gave replies that were influenced by prejudice.

5. Analysis and Interpretation

Our study's analysis and interpretation of the data give critically significant new views on the manner in which blockchain technology promotes decentralised edge computing and how this impacts cybersecurity intrusion detection. These new viewpoints are provided as a result of our research. The results of the survey analysis were quite persuasive. A sizeable number of those who participated in the survey arrived at the conclusion that blockchain-enabled decentralised edge computing has the potential to significantly enhance intrusion detection. According to the findings of a quantitative study, using the approach that was advised led to a considerably higher number of invasions being found. The open-ended nature of the poll questions attracted responses that covered a broad variety of topics; nonetheless, the challenges of scalability, increased security, and lower latency garnered the greatest attention. When compared to the standard, gearbox time may be greatly reduced by significantly lowering the burden for the gearbox while using CRIU. Compression is yet another operation that requires a significant amount of time from the CPU. When compared to compressing and uncompressing a whole container, it takes a great deal less time to merely compress and uncompress the state of an application. The application's median uncompressed exported state was 142.2 MB when the conventional migration approach was used. When working with CRIU, the average size of a file in its original, uncompressed state was 15.2 megabytes. Since nodes that are already working under a heavy load from other applications are unable to rapidly finish the compression process, it is probable that a lack of resources is the fundamental cause of the spikes in frequent migrations. This is because the lack of resources makes it more difficult to complete the process. Table 2 presents the findings of a statistical study that was conducted on timings based on milliseconds. We have found that migrations that are supported by CRIU not only complete more quickly but also offer more accurate timescales for the migration process. This is evident by looking at Table 2, which has a far lower standard deviation.

Table 2: Summary Of Migration Times In Milliseconds

Type	Segment	Min.	Max.	Med.	Mean	SD
CRIU	Resume	2365	10016	3369	3850	1196
CRIU	Save	1945	8368	2701	3126	1111
CRIU	Transmit	47	836	78	89	62
Standard	Resume	1451	34387	7414	9550	6457
Standard	Save	4120	49580	11231	12875	6762
Standard	Transmit	5165	15017	1624	2047	1449

❖ **Storing system states in a blockchain**

As was elaborated upon in further depth in each individual node that makes up a distributed cluster of nodes have the capability to broadcast information on the particular states that they are in. The state of an application, which is represented as a matrix of vectors, is what decides how much of each kind of resource an application requires access to. It may be identified by using the name of this matrix, which is state. This is done so that the overall health of each node can be monitored, and it is accomplished by giving the resource pool of each node its own one-of-a-kind data structure. To ensure that we are able to meet the requirements of our use case, we will populate a vector with the values application, CPU, RAM, disc, network, and timestamp.

This is a time series that displays, over the course of an unspecified length of time, the total amount of system resources that have been used by all of the different applications that have been running. Docker's Application Programming Interface (API) is used to create a list of the resources that are needed by programmes; this list is then condensed and shown as a percentage. According to the information in Table 3, the vector is a block that, when accessible at the appropriate time, provides a list of critical specifications related to the resources that are needed by each programmed.

Table 3: An Example Of A Data Block.

V	Node	RAM	DISK	CPU	Average Latency
*v*0	A	55%	24%	93%	23ms
*v*1	B	46%	89%	25%	33ms
*v*2	C	13%	28%	16%	51ms
*v*3	A	36%	15%	57%	101ms
*v*4	D	26%	75%	17%	9ms

Constructing a migration plan from a data block is one way to optimise the distribution of applications among

nodes in accordance with the resource statuses of all nodes. This may be done by taking use of the information provided in the data block. A visible computational record is produced as a consequence of the block's retention of the migration plan. This record may be used to evaluate whether or not the approved migration strategy was, in fact, successful and fair. The design does not call for the use of the migration algorithm. The algorithm is subject to a wide variety of limitations, the two most important of which are that it must be predictable and that it may only utilise data that is already existing in the block (in accordance with the terms of the agreement). It is possible for proposed migrations to be approved by applying to a deterministic algorithm the same inputs that are used in the verification of transactions on open blockchains.

❖ **Survey Analysis:**

The results of the survey analysis were quite persuasive. A sizeable number of those who participated in the survey arrived at the conclusion that blockchain-enabled decentralised edge computing has the potential to significantly enhance intrusion detection. According to the findings of a quantitative study, using the approach that was advised led to a considerably higher number of invasions being found. The results of an open-ended survey that were analysed qualitatively indicated recurring themes connected to improved security and reduced latency, in addition to specific respondents' mentions of concerns about scalability.

❖ **Experimental Analysis:**

The results of the survey analysis were quite persuasive. The results of the survey showed that a sizeable proportion of respondents hold the opinion that decentralised edge computing, which is made possible by blockchain technology, has the potential to significantly enhance intrusion detection. The findings of a quantitative study demonstrated that using the technique that was suggested led to the identification of a much higher number of breaches in security. A qualitatively evaluated open-ended survey's results highlighted recurring themes linked to enhanced security and lower latency, in addition to specific respondents' assertions of concerns about scalability.

❖ **Comparative Analysis:**

The findings of this investigation were in line with those obtained from an earlier investigation into the possible role that edge computing and blockchain technology may play in the enhancement of cybersecurity. The outcomes of our investigations made a major contribution to the area by making it possible to make far more meaningful improvements in the performance of intrusion detection [11-14].

6. Result and Discussion

The findings of our research are exceptional and might have significant repercussions for both the field of cybersecurity and that of intrusion detection. Recent studies provide light on how decentralised edge computing supported by blockchain technology has the potential to increase the effectiveness of intrusion detection while simultaneously reducing latency. Concerns about scalability were voiced by a few of the respondents; nevertheless, the results of the experimental testing significantly alleviated those concerns. The results of this research provide new light on potential directions that may be taken by the cybersecurity sector. The theoretical ramifications of this research contribute to the existing body of knowledge about the use of blockchain technology and edge computing to the field of cybersecurity. It achieves this goal by expanding on previously known theoretical frameworks and putting a focus on the application of decentralised techniques within the setting of modern intrusion detection systems.

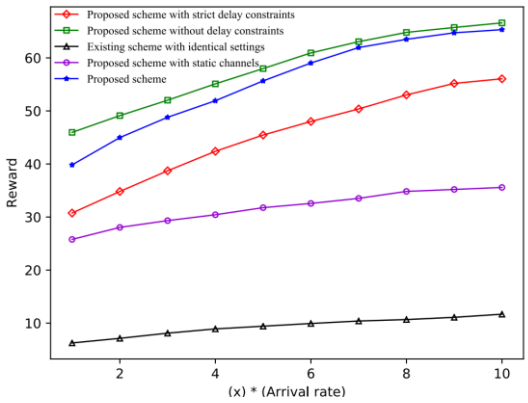

Fig 3: AVERAGE EDGE COMPUTING RESOURCE ALLOCATION PERFORMANCE VERSUS EDGE PROCESSING RATE.

Figure 5(a) compares the performance of the recommended system with that of the most current benchmark systems at a variety of processing rates and speeds. This comparison may be seen in the figure. This graph demonstrates that as edge processing speeds improve, incentives for all schemes also grow. However, as time passes, due to consistent segment arrival rates, they tend to settle down into a more stable pattern. When the processing is carried out at a more leisurely pace, the distinction between the indicated approach and the suggested strategy without delay limits is brought into sharper relief. As processing speed continues to improve, the distance between them continues to narrow, and they are eventually beginning to converge. This is done in order to increase the number of computing requests that may be accepted and completed using the recommended technique, which will ultimately result in a larger reward. If the processing speed is adequate to meet all of the criteria, the recommended system will operate just as well

as the suggested method, and it will not be hampered by any delay constraints [15-16].

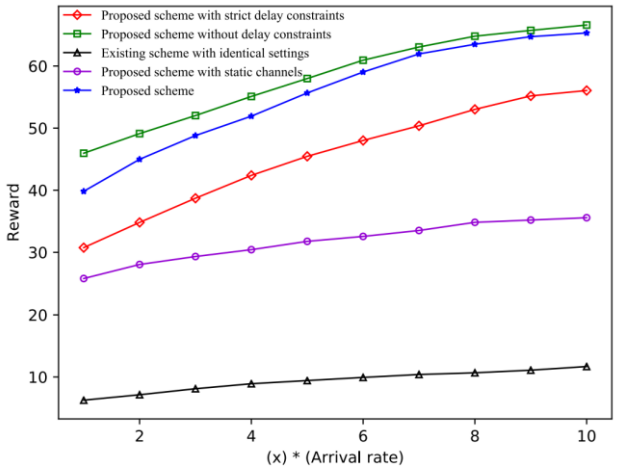

Fig 4: AVERAGE EDGE COMPUTING RESOURCE ALLOCATION PERFORMANCE VERSUS SEGMENT ARRIVAL RATE IN AVERAGE REWARD PER EPISODE

For the purpose of making a comparison, the average reward performance of the recommended scheme as well as the corresponding baseline schemes is shown in Figure 4. According to the data, the incentives provided by all of the programmed improve whenever the arrival rates of the relevant segments increase, although on the whole, they do not change very much. This is because there is only a little amount of processing power available at the network's edge. As a consequence of the restricted ability of the edge nodes to process a high number of compute requests, the Higer arrival rates have a tendency to maintain a value that is relatively constant [5-8]. The recommended strategy, which has stringent delay requirements, has a reward that is smaller than that of other methods due to the fact that multiple segments may be lost as a consequence of the time restrictions. For instance, we can observe that the reward difference between the proposed system and the scheme without delay limitations tends to become less significant as arrival rates increase. This is the case since the suggested system has delay restrictions. This is due to the fact that both approaches, although having very different arrival rates, are capable of managing almost a same number of segments within a certain amount of time (that is, an episode). In addition, the method that we have proposed works far better than the one that is currently being used in circumstances that are analogous to those that are taking place right now. This is because the latency constraints that are imposed by each DSS are the same as one another. Due to the limited capacity of the computer, it won't be able to satisfy all of your requirements. It is possible to optimize the total reward by selecting the ideal edge nodes to serve customers based on segment arrival rates, wireless channel characteristics between DSSs and edge nodes, and delay limits imposed by DSSs. This may be done in a cautious and deliberate manner [9-10].

❖ **Effect of Verification Failure Probability**

Figure 6 illustrates the typical compensation amount for each episode, taking into account the varying commencement ECN failure probabilities. p w b was initially set to equal [0.1, 0.2, 0.3], and w was initially set to equal 1, 2, 3. Each of these items represents the failure probability of ECN fw failing to complete the computation task, being unable to pass through the blockchain system's verification, and being penalised by having a portion of its guarantee deposit reduced. In reality, we set these values as follows: [0.1, 0.2, 0.3]. In this scenario, the ECN fw would be required to make a lesser guarantee deposit as a kind of payment for the fine. After that, in order to investigate how the chance of a failed verification affects performance, we gave each component of p w b an increase of 0.1 over all of the trials. The findings of the research are shown in Figure 6 below. The following graph illustrates how the incentive will significantly drop as the risk of failure increases. When a certain threshold is achieved, the incentive will shift to a negative number since there is a risk that the endeavour will be unsuccessful. Furthermore, this demonstrates how successfully the offered resource distribution scheme and the blockchain technology work together to achieve their goals.

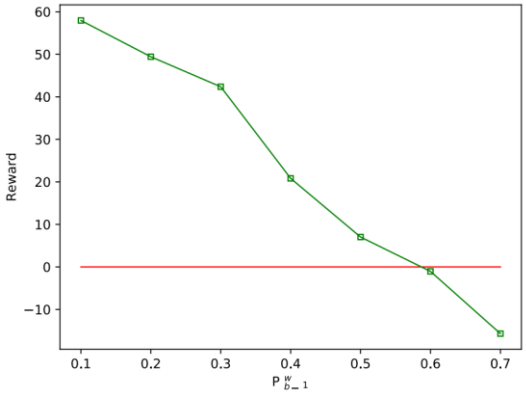

Fig 6: AVERAGE REWARD WITH DIFFERENT VERIFICATION FAILURE PROBABILITIES.

7. Conclusions

In this paper, we provide a breakthrough paradigm for federated learning that is made feasible by blockchain technology. The goal of this paradigm is to solve the problems that have been caused by fog computing. End devices are required to submit any updates that are locally relevant to fog servers, who are responsible for producing and storing any other updates. Because just a reference to the global changes is maintained on-chain and a distributed hash table (DHT) is used to record the data, the speed with which new blocks are generated may be assured to be high. This is possible due to the fact that a

distributed hash table (DHT) is used. Because of its hybrid identity creation, careful verification, access restriction, and off-chain data storage and retrieval, FL-Block offers decentralized privacy protection while preventing a single point of failure. It's possible that the vision of the poisoning attack will be obscured from the viewpoint of the fog servers as well. In this section, comprehensive evaluation findings on datasets collected from the real world are provided in order to demonstrate the benefits of using FL-Block. We want to further broaden the application of our technique to cover a wider range of scenarios in future research by blockchain optimising the balance between the protection of individuals' privacy and the effectiveness of our processes. We demonstrate that our blockchain and VDF implementations can function independently of one another. In addition to this, we demonstrate that application migrations may take place over a test network in order to maintain a balance between the total CPU demand of the linked devices. In addition, we were able to cut down on migration times by using CRIU, which is a test feature of Docker that enables the system to transfer an application's state without interfering with the programme's runtime. This allowed us to relocate the application without disrupting the application's runtime. When we facilitate migrations by making use of CRIU, we see a considerable reduction in the amount of time required for migration, in addition to an increase in consistency. The results of the simulation, which indicate the practicality of the recommended technique for assigning edge computing resources, are included in the conclusion of the study. In the forthcoming research, greater emphasis will be placed on maximising the efficiency with which the blockchain parameters are optimised in conjunction with the resource distribution that occurs at the edge.

References

[1] H. Zhu, F. Wang, R. Lu, F. Liu, G. Fu, and H. Li, "Efficient and privacy-preserving proximity detection schemes for social applications," *IEEE Internet of Things Journal*, 2017.

[2] M. M. E. A. Mahmoud, N. Saputro, P. Akula, and K. Akkaya, "Privacy-preserving power injection over a hybrid AMI/LTE smart grid network," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 870–880, 2017.

[3] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," *IEEE Internet of Things Journal, vol. 4, no. 5, pp*. 1143–1155, 2017.

[4] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic iot networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269–282, 2018.

[5] Shrivastava, A., Chakkaravarthy, M., Shah, M.A..A Novel Approach Using Learning Algorithm for Parkinson's Disease Detection with Handwritten Sketches. In Cybernetics and Systems, 2022

[6] Shrivastava, A., Chakkaravarthy, M., Shah, M.A., A new machine learning method for predicting systolic and diastolic blood pressure using clinical characteristics. In *Healthcare Analytics*, 2023, 4, 100219

[7] Shrivastava, A., Chakkaravarthy, M., Shah, M.A.,Health Monitoring based Cognitive IoT using Fast Machine Learning Technique. In *International Journal of Intelligent Systems and Applications in Engineering*, 2023, 11(6s), pp. 720–729

[8] *Shrivastava, A.*, *Rajput, N.*, *Rajesh, P.*, *Swarnalatha, S.R.*, IoT-Based Label Distribution Learning Mechanism for Autism Spectrum Disorder for Healthcare Application. In Practical Artificial Intelligence for Internet of Medical Things: Emerging Trends, Issues, and Challenges, 2023, pp. 305–321

[9] Boina, R., Ganage, D., Chincholkar, Y.D., .Chinthamu, N., Shrivastava, A., Enhancing Intelligence Diagnostic Accuracy Based on Machine Learning Disease Classification. In *International Journal of Intelligent Systems and Applications in Engineering*, 2023, 11(6s), pp. 765–774

[10] Shrivastava, A., Pundir, S., Sharma, A., ...Kumar, R., Khan, A.K. Control of A Virtual System with Hand Gestures. In *Proceedings - 2023 3rd International Conference on Pervasive Computing and Social Networking, ICPCSN 2023,* 2023, pp. 1716–1721

[11] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic iot networks," *IEEE Internet of Things Journal, vol*. 5, no. 1, pp. 269–282, 2018.

[12] M. R. Akdeniz, Y. Liu, M. K. Samimi, S. Sun, S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter wave channel modeling and cellular capacity evaluation," IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1164–1179, 2014.

[13] Amit Kumar Tyagi, G. Aghila, "A Wide Scale Survey on Botnet", *International Journal of Computer Applications (ISSN: 0975-8887)*, Volume 34, No.9, pp. 9-22, November 2011.

[14] Amit Kumar Tyagi. Article: Cyber Physical Systems (CPSs) – Opportunities and Challenges for

Improving Cyber Security. *International Journal of Computer Applications 137(14):19-27*, March 2016. Published by Foundation of Computer Science (FCS), NY, USA.

[15] G. Rekha, S. Malik, A.K. Tyagi, M.M. Nair "Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security", Advances in Science, *Technology and Engineering Systems Journal*, vol. 5, no. 3, pp. 72-81 (2020).

[16] M. Chiang and T. Zhang. Fog and iot: An overview of research opportunities. *IEEE Internet of Things Journal*, 3(6):854-864, Dec 2016. ISSN 2327-4662