International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8162
***Article Received:** 29 June 2023 **Revised:** 18 August 2023 **Accepted:** 05 September 2023*

Configuring and Implementing IPS Solutions for IoTDevices using NST

[1] V. Maruthi Prasad, [2] Dr. B. Bharathi

[1]Research Scholar, Department of CSE, Sathyabama Institute of Science and Technology, Deemed to be University,Jeppiaar Nagar, Chennai, Tamil Nadu 600119,
Asst.Professor, Madanapalle Institute of Technology & Science, Email: maruthi.vv@gmail.com
[2]Research Supervisor, Department of CSE, Sathyabama Institute of Science and Technology, Deemed to beUniversity, Jeppiaar Nagar, Chennai, Tamil Nadu 600119, Email: bharathi.cse@sathyabama.ac.in

Abstract: The necessity to ensure that Internet of Things (IoT) networks are secure is one of the biggest issues that has arisen as a result of the growing demand for technology that uses the IoT. Considering how many gadgets are linked to the internet, safeguarding their networks is a growing worry. Due to the IoT's network's complexity and resource constraints, traditional intrusion detection systems encounter a number of problems. The main objectives of this projectare to design, develop, and evaluate a hybrid level placement method for an IDS based on multi-agent systems, BC technology (Block-Chain), and DL algorithms (Deep Learning). Thebreakdown of data administration, data collection, analysis, and reaction into its component parts reveals the overall system design. The National Security Laboratory's knowledge discoveryand data mining dataset is used to test the system as part of the validation procedure. These results demonstrate how deep learning algorithms are effective at identifying risks at the network and transport levels. The experiment shows that deep learning techniques function wellwhen used to find intrusions in a network environment for the Internet of Things.

Keywords: Block-chain, IoT, IDS, MAS, MAT, NST.

I. INTRODUCTION:

Internet of Things technology may be thought of as a network that relies on standard protocols to facilitate communication and data sharing among internet-connected gadgets. The idea of smartness is now being introduced to products, sensors, houses, streets, and even cities thanks to recent breakthroughs in IoT [1]. It consumes significantly impacted a number of industries, from the agricultural industry to the automation of cars. As it interacts with every kind of linked item indaily life, IoT is now also known as the Internet of Everything (IoE). It is predicted that there willbe up to 21.5 billion linked devices by 2025. A network layer is one of the layers that make up the Internet of Things. The network layer, which is modelled after the standard Internet protocol stack, is responsible for the transmission of data packets between hosts. In addition, the network layer inIoT architecture is

complex and a weak spot, which results in a number of security issues [3]. To address the security concerns, a number of security frameworks have been put in place.

Certain frameworks must be deployed in order for the IoT architecture and/or the devices to operate normally and handle security problems. Most security frameworks, however, need a large memory and CPU investment. Nevertheless, there are a number of methods that may be utilised to circumvent the restrictions, such as lightweight encryption and authentication systems. The sheernumber of hosts, nodes, or devices that are linked to the IoT is one of the primary factors that contributes to the existence of security flaws in this network. If the system's integrity is compromised at even a single node, the whole infrastructure is at risk [1].

The most common security threats that IoT systems must contend with include well-known assaults such as attacks like DDoS, botnets, ransomware, remote recording, routing assaults, and data outflow. It is common knowledge that the first line of defence against assaults on Internet of Things devices is a firewall; yet, due to the very different and intricate nature of IoT systems, this line of defence isuseless [5].

Recently, intrusion detection systems (IDSs) have gained popularity because of their reliability. James defined an IDS and introduced the concept for the first time in 1980. IDSs are designed to find intruders in a space. A host seeking to gain unauthorised access to some other nodes can be considered an invader in an IoT environment [2]. An IDS consists of three main modules like agent, analysis engine, and a reaction part of the modules. The agent is solely responsible for observing events and collecting data from the data stream. The warnings are generated by the analytical engine, which also maintains track of the symptoms of an incursion [3]. Over the years, intrusion detection systems (IDSs) have become more effective and reliable; nevertheless, cybercriminals have also developed a growing variety of attack tactics in order to evade detection by these systems. After receiving the information from the analysis engine, the response module will process the data it has been given.

Not only that, but the IoT's several network levels make it impossible for traditional IDSs to protect against. Recent advances in ANNs have led to the use of distributed IDSs in combination with a wide range of machine learning methodologies, including as deep learning, reinforcement learning, and artificial neural networks, among others [3]. Common ANNs aren't always up to snuff when it comes to dealing with the complexities of IDSs [1]. These technical shortcomings must be addressed before IDSs may reach their full potential in practise. The primary contributionof this paper is the evaluation of BC's potential in a multi-agent system utilising a widely-used dataset. Evidence suggests that the majority of assaults originate at the transport or network layers. This study's main goal is to inspect the potential for using the technology like blockchain conceptin a MAS [4]. In this work the goals to create a remedy by an intelligent IDS that may identify intruders and stop attacks in IoT contexts [18].

This may be achieved by first evaluating the current status of IDS models built using machine learning methods. IoT system attacks that have previously happened are investigated to discover prospective security and privacy concerns. Additionally, the drawbacks of current IoT devices areassessed [5]. Different optimization strategies are investigated in order to enhance IDS performance. Intrusion detection systems and network firewalls are two types of cybersecurity solutions that may be used to safeguard a network or an endpoint. These solutions are examples of what are known as "cybersecurity solutions." Both of these categories of potential answers are open to consideration. Despite this, each of the goals of the group is slightly distinct from the goals of the others in the group.

An intrusion detection system, often known as an IDS, is a kind of passive monitoring device thatsearches for any gaps in security and alerts the proper parties when it uncovers a breach in security. An IDS is sometimes referred to as an IDS. This gives the analysts who work in the security operations centre (SOC) or the incident responders the ability to investigate the suspected security breach and react appropriately to it [6]. There is no real security afforded to either the endpoint orthe network by an intrusion detection system (also known as an IDS). On the other hand, in orderfor a firewall to successfully carry out the duties that are associated with a defensive system, it must have been built from the bottom up to do so [19]. After performing an examination of the data contained inside the network packets, it then either permits the traffic to pass through or blocksit according to the rules that have been established. This decision is based on the rules that have been stated. This establishes a limit that cannot be surpassed, and once it is in place, certain typesof traffic or protocols will not be permitted to progress if they attempt to go beyond it.

Due to the fact that it is an active defensive mechanism, a firewall is more comparable to an intrusion prevention system (IPS) than it is to IDS. An intrusion prevention system, also known asan IPS, performs a function that is comparable to that of an intrusion detection system, also knownas an IDS [9]. The main difference between these two kinds of systems is that an IPS really does anything to stop threats from happening, as opposed to only warning people that they exist. As a consequence of this, the capabilities of a firewall are increased, and several next-generation firewalls (NGFWs) are outfitted with integrated intrusion detection and prevention systems (IDS/IPS). This gives them the capacity to recognize and react to cyber threats that are getting more sophisticated (IDS/IPS), as well as the ability to enforce the filtering rules that have been created. Additionally, this gives them the power to filter out content that does not comply with the rules (firewalls). In the next paragraph, you will discover some extra information on the discussionsurrounding IPS and IDS[10].

II. LITERATURE REVIEW

Recent research on IDS performance for IoT devices were analysed thoroughly. IDS was used to examine IoT risks and defences. IDS monitors the system and network for harmful activity. It contains software and hardware to do this. IDS detects cyberattacks and alerts the appropriate parties. IDS protects organization's systems and networks. An IDS is often used after a firewall has already been set up. There has been much study of intrusion detection systems (IDS) in the context of Internet of Things (IoT) security and privacy. Many novels have been released in the last few weeks. Cybersecurity professionals are worried about the privacy and safety of IoT settings. To guard against cyberattacks [2], IDS has been recommended for IoT designs and devices.

The majority of academics are concentrating their efforts on developing innovative defences against intrusions into existing network protocols. However, standard IDS algorithms are not compatible with Internet of Things devices that use IPv6 for connectivity as well as other complex network topologies. A more in-depth investigation of the methods of machine learning is necessary for IDS to be able to protect and defend users' privacy in the IoT [2]. IDS may be broken down into two primary components, which are as follows: IDS that is based on the host IDS that is internet or intranet based on the log and audit data are analyzed by the host-based IDS to search for

DOI: https://doi.org/10.17762/ijritcc.v11i11s.8162
***Article Received:** 29 June 2023 **Revised:** 18 August 2023 **Accepted:** 05 September 2023*

indications of an intrusion. This IDS is widely used on crucial hosts to safeguard their security. The host-based intrusion detection system is preferable to the network-based system because it is less sophisticated, has a lower incidence of false alarms, and gives more detailed information [6]. Yet as a result, the host's log data and monitoring tools become too relied upon, and the application system's effectiveness suffers.

The properties of the IoT and the prospect that a large number of IoT devices will be connected tonetworks highlight the need of network-based intrusion detection systems. Network-based intrusion detection systems may detect anomalies in network traffic and identify potential intrusions. There will be no change to either the configuration of the network host or thefunctionality of the business system [7]. The failure of the network IDS will not have any effect on the regular operations of the firm. A cause for worry is that network-based intrusion detectionsystems only investigate their own direct connections to network segments, ignoring connections to other network segments [3]. In addition, it might be difficult to process encrypted sessions using network-based intrusion detection systems. Signatures, requirements, anomalies, and hybrid methods are the four primary categories

of intrusion detection techniques. These categories are based on the characteristics of various types of intrusion attempts.

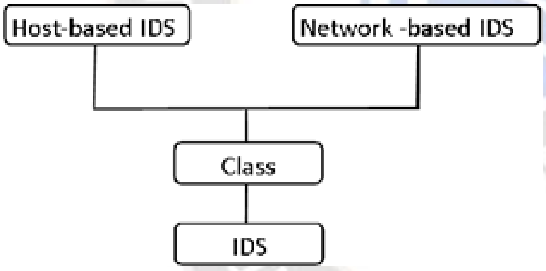

Fig 1: First Phase of IDS

The data in the network is first scanned using signature-based algorithms, who then compare the results with a feature database. The scanned material will be handled as an incursion if it is discovered that the features match those in the signature database. The benefit is that it can precisely identify the attack's type. It is not a lot. convenient to use, and there is just a modest demand for resources. System administrators must pre-set criteria and thresholds for specification- based techniques. According to the guidelines and thresholds established by administrators, IDS determine the condition of the present system and network. If the threshold is exceeded or the rules are breached, the IDS will detect an abnormal situation and respond accordingly. Identification of aberrant patterns and comparison of traffic patterns are the foundation of anomaly-based approaches. The benefit of employing this technique is that it makes it possible to identify fresh and unidentified incursions. The method's main drawback, however, is that it frequently yields large percentages of false positives.

To increase the effectiveness of anomaly-based intrusion detection systems, this research looks at how to include machine learning algorithms into these tactics. Techniques for the detection of intrusion based on anomalies may monitor ongoing footprints left by intrusions and compare those footprints to previously collected data in order to anticipate possible further attempts.

Hybrid methods are any combinations of the aforementioned detection techniques that are used in the same IDS. This strategy can assist in overcoming the drawbacks of a particular method and improve the overall dependability of the IoT system. However, the IDS as a whole will grow to be extremely huge and complex, which is a clear disadvantage. This will make running the entire system more challenging and resource-intensive. Multiple monitoring nodes are used in centralised IDS (Figure-1) to analyse host or network activities. The primary server or node will then get the data for additional analysis. The central server load will rise as the system gets more complicated, lowering system performance and possibly even posing security threats. The majority of data interaction in the IoT environment takes place at the network and perceptual layers, and IoT facilities are dispersed and distributed in a complicated way. As a result, IoT device intrusions cannot be successfully detected by the centralised IDS.

The Distributed Intrusion Detection System (DIDS) is composed of a number of modules, each of which is tasked with performing a unique function. In most cases, they will split the monitoring tasks among themselves. As a result, the intrusion detection modules that are connected with these layers need to be distinct from one another. This has the potential to dramatically improve the system's level of security since it eliminates the requirement for the storing and sharing of data that isn't strictly essential. The key benefit is its scalability, which allows for rapid response to emerging Internet of Things scenarios. The potential for high communication costs and resource usage is a disadvantage that must be considered.

Recent research has offered a few hybrid placement options. The network is divided into several pieces by the first hybrid placement method. There will be a node that keeps an eye on the other nodes in the cluster and performs intrusion detection. These nodes are also responsible for monitoring the data package that comes from the nodes that are close by. It is assumed that attackers have breached the neighbouring nodes if any unexpected behaviour is seen. The border router gathers data from the nodes and renders a verdict regarding the breach. Additionally, centralised IDS is less accurate than hybrid IDS with distributed components [16]. The hybrid system, however, has high resource requirements.

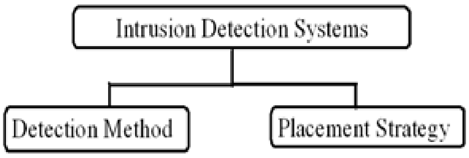

Fig 2: IDS parts

This study focuses a significant amount of attention on improving the IDS of the IoT. In this part,we will present an overview of the advancements and upgrades that have been made to IDS for IoT. Additionally, it is separated from a few other components that are based on specifications.

This is done in order to prepare for any discrepancies that might possibly occur in the future. In order to achieve this goal, it employs a calculation known as unsupervised optimum-path timberland (OPF), as well as engineering based on MapReduce.

The terms "false assaults," "jam attacks," and "reply attacks" are used to refer to the three distinct types of Internet of Things attacks that are distinguished by this manner It's a basis for future developments. Since the arrangement hubs provide data to the interruption detection module and help create event databases, the IDS may be adjusted centrally. Intrusion detection system (IDS) uses occasion analyzer, which uses a specified approach, to identify disruptions. By comparing the activity streams that have already been examined, this IDS is able to efficiently detect jam assaults, bogus attacks, and reply attacks that occur in IoT networks.

They proposed a protocol for the architectural design of peer-to-peer linked networks that would include Ethereum blockchain technology for the purpose of communication.

The outcome is an autonomous agent-friendly protocol. The suggested protocol improves communication safety and helps employees anticipate working situations. This encouraged greater research into blockchain and multi-agent systems. Therefore, we must find a way to keep faith inMAS at a very high level. They came up with the idea to combine MAS, which was built on the JADE, with BTC, which was developed on Hyperledger Fabric, and then put the new system into operation. The approach extends agent identity control to Hyperledger Fabric membership, creating a trustworthy community. In addition to this, the association agent is given with services that make use of the ledger. Transparent mechanisms calculate and store agent reputations. These processes are based on agent communications and interactions. The system is tested with several situations.

Agent behaviours may be broken down into two categories: user-dependent and autonomous. Strategies for smart contracts are used, and these techniques include reputation-based computing as well as agent behaviour monitoring. Because there is an implementation of Hyperledger Fabric that is now available, the system is both stable and scalable as a consequence of this implementation. Make advantage of a command line interface (CLI) during testing (graphical interface eased the interactions). In spite of the existence of a prototype for combining BCT with MAS, there are technological barriers to full implementation. In addition, it includes enforcing cryptographic solutions to boost security and privacy, mapping physical objects to distributed blockchain components, verifying the correctness of smart contract implementation, and enabling the use of blockchain and agent technology in Real Systems. These are some of the tasks involved.These are some of the responsibilities that will be required.

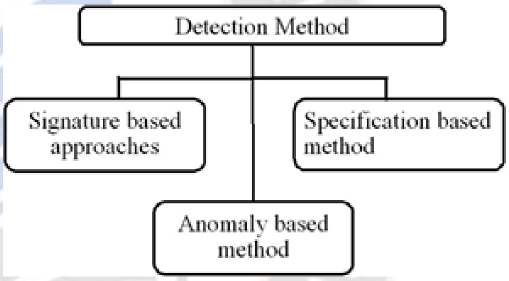

Fig 3: IDS Detection Method

There are ethical considerations to be made in real-world settings that include the merging of BCT and MAS. The process of creating an application domain that empowers system users and promotes trustworthy interactions is intrinsically linked to the immutability characteristic of the ledger and the transparency of reputation management. Because the design is wholly reliant on smart contracts, there is a risk that the privacy of the users will be violated if there is a system fault, regardless of whether the error was deliberate or not. It is not yet apparent how reliable the software and verification process will be in a BCT environment, despite the fact that a BCT- enabled MAS would do away with the need for mediators in the process of dispute resolution.

Motivations, requirements, methodologies, application areas, and strengths and weaknesses were examined. The authors emphasised the need for a full study of new technologies, not only their benefits. The acquisition of data from a large number of connected nodes in a network, such as theInternet of Things, may be accomplished in a dependable manner by combining blockchain technology with multi-agent platforms. This is a concept that is plausible and might be implemented. This was one of the outcomes from the research that took me by surprise the most. The integration of multi-agent systems with blockchain technology could prove to be an efficient method for tackling the problems caused by connected ecosystems, which are infamous for their complexity.

Agents operating inside multi-agent systems often find themselves in predicaments in which it is hard for them to arrive at a "consensus." It is a challenging undertaking to identify agent conflicts of interest and then remove the stagnation that results from such conflicts. The model analyses cooperative inclinations by considering each actor's collaboration possibilities. Candidates' policies might boost overall payment (identifying the candidate action sets). NBS is used to pick the best candidate action sets. Reducing "convergence time" and memory footprint may help. The existing approach isn't adequate for instances with a large state space.

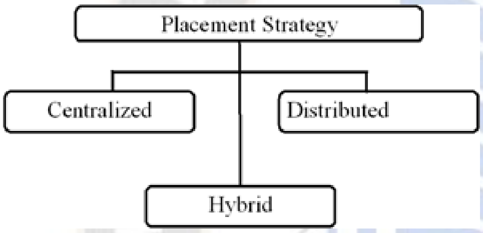

Fig 4: IDS Placement Strategy

Air Traffic Function Management is futile without ATFM. A high-fidelity and mathematically sound ATFM model is needed for high-precision decision-making, but creating one could be difficult owing to its complexity. A blockchain-based, multi-agent, distributed ATFM system with reinforcement learning is needed to solve the problem. Local, blockchain, and global optimization layers make up the system. Local stakeholders might be positioned regionally because of the locallayer

The execution of smart contracts may now incorporate data collected at different scales thanks to the global optimization layer. Reinforcement learning is used by the technology to reduce the amount of time an aeroplane is delayed both while it is in flight and before it takes off. BlockAgent did perform better than traditional ATFM systems in the management of delays when the system was assessed inside a limited environment. Enhancing the functionality of the system is one of the writers' top priorities in order to make it suitable for general use.

III. PROPOSED SYSTEM:

1. MULTI-AGENT SYSTEM/TECHNOLOGY (MAS/MAT)

This part of the article discusses the technology that sits at the heart of our proposed IDS, which incorporates both the blockchain and a multiagent system. An agent is intelligent software in AI and computer science. People usually mean MAS when they say "multi-agent" (MAT). A multi- agent system, or MAS, uses distributed AI. It consists of several agents working together (DAI). Complex systems are amenable to simplification and modularization when using a MAS. The agents, in their individual capacities, are responsible for coordinating and communicating with one another. Because each agent that makes up the MAS is entirely self-sufficient and independent in terms of its form, the system is able to function both alone and in groups. Even if the agents were built using a variety of programming languages and design paradigms, they should all utilise the same communication channels so that they may communicate with one another. This is because mutual communication is impossible in a system that only has one agent. Every agent performs its tasks in accordance with its own own set of characteristics and procedures. They are responsible for completing responsibilities throughout the whole of the MAS's operation in accordance with these action standards. Because of the collaboration amongst the agents in MASs, human beings have the ability to solve a number of difficult problems. Autonomy, responsiveness, initiative, andsociality are the four primary characteristics that should be present in each agent. The intellect and the agency of the system are the primary manifestations of this fact. The term "intelligence" is used to describe a computer's ability to learn, reason, and otherwise digest a large amount of data in order to draw conclusions and draw conclusions about that data. The agent's agent capacity is its ability to recognise messages from the external environment and respond autonomously based onits own knowledge.

For the purposes of machine learning, "deep learning" refers to approaches that use artificial neural networks (ANNs). The structure and operation of the brain serve as inspiration for ANNs and deep learning. Interconnected brain cells (ANNs) Layers of ANNs are stacked for deep learning. The data flow network has a hierarchical structure with input and output layers. Many other names have been used to describe deep learning, but two of the most common are "deep structured learning" and (DNN). One key feature that sets ANN learning from from deep learning is the presence of hidden layers. Most of the structure between its input and output

DOI: https://doi.org/10.17762/ijritcc.v11i11s.8162
***Article Received:** 29 June 2023 **Revised:** 18 August 2023 **Accepted:** 05 September 2023*

levels is hidden from view. Considering the greater analysis and computation performed by deep learning, it is more trustworthy than ANN. Deep learning is complicated. In reality, more data means more complicated data. Deep learning may learn from previous data layers and large volumes of data. Deep learning is a strong machine learning approach, particularly for categorising unlabeled data. Deep learning can learn fast from massive datasets.

Levels of secrecy exist between the input and output layers of a network's data structure. Since deep learning consumes and computes inputs more than ANN, it is more reliable. As data volume rises, so does data complexity. Deep learning may learn from prior layers or plenty of data. Deeplearning is an effective machine learning paradigm, especially for categorizing unlabeled sample datasets. Order of agent actions regulates a multi-agent system's environment. The agent may builda non-standard Markov environment if it fails to recognize the connection between its actions and changes in the environment. As a result of MASs pattern library, concurrent isolated RL (CIRL) may be used, in which a single agent uses unsupervised learning. The goal of interactive RL is totrain agents to work together effectively. Credit assignment is an important part of RL in both single and multi-agent settings, however in the former case, it is only transient and must be takeninto account.

Decentralization is the major driver that is propelling the development of blockchain technology. The blockchain's public and distributed ledger means that the failure of any one node will not affect the overall system's functionality. The star-shaped structure that was formerly used by the transaction network has been replaced by the point-to-point, or P2P, structure that was introduced by blockchain. This revised framework allows two parties to communicate directly utilising encryption and code-based security. Participants in the transaction system don't need to know the trustworthiness of the other parties since they just need to trust the algorithm for mutual trust. There is no prerequisite. Since the authentication process is handled by the algorithm, the framework doesn't need to be certified by an external security agency. The most well-known blockchain platforms are Ethereum and Hyperledger Fabric. Both of them make use of the same fundamental technological components. Ethereum and Hyperledger are fundamentally different from one another in terms of both the production process that goes into them and the users that they are designed for. The Ethereum virtual computer may be used with Ethereum (EVM). Smart contracts and public blockchains emphasise consumer applications. Hyperledger Fabric's

architecture makes it ideal for business environments. It enables flexibility and freedom while building business logic.

2. SESS (SMART EFFICIENT SECURE AND SCALABLE) SYSTEM:

Science and engineering research as well as design science research are approaches used in this article. It is possible to investigate the viability and worth of this novel purposed intrusion detection system framework by fusing scientific study with technical design and implementation. This system will be used to track the specifics of the IoT network situation and find attacks from the current network traffic[6]. In order to see detection reports and make action rules, users interact with the system through a web interface. There are five parts to the system: data collection, processing, monitoring, and a blockchain-based smart contract. The system must communicate with IoT devices and monitor data flow. The system requires data storage to detect dangerous IoTnetwork behaviour. The web portal just collects data, but the system adds and modifies it. All database communication will utilise the Internet or intranet.

The IoT network administrator will be able to monitor IoT devices using network traffic data thanks to the smart, efficient, secure, and scalable (SESS) system. Based on parameters establishedby the administrator, the region will be monitored. The system collection module's monitoring procedure can be altered in a number of ways by the administrator. The data processing module that performs the initial attack detection based on feature categorization will process the collecteddata. Then, these data will be split into a training dataset and an unidentified dataset. The detectionand analysis module will get these two datasets. The detecting agent will be trained using the training dataset. The performance of the model will be examined using the unnamed dataset.

The system can be used for intrusion detection by IoT network administrators, who can also add data, customise the data process and detection criteria, and remove agents as needed. The system components will be installed and run on various hosts for large-scale IoT networks. This indicatesthat a separate administrator is needed for each SESS module. The modules they oversee should be able to be configured by these administrators.

This paper's intrusion detection system (Figure 2) employs a multi agent method. Each agent performs their duties in a manner that is mainly independent of the others. There are four basic sorts of module components that make up agents. They have conversations with one another using the communication agents that are located in each module. As a result, there is less interdependence between modules and each one may function autonomously. There are four main

DOI: https://doi.org/10.17762/ijritcc.v11i11s.8162
Article Received: *29 June 2023* ***Revised:*** *18 August 2023* ***Accepted:*** *05 September 2023*

parts to the system: data collection, data processing, detection and analysis, and action. Given its widespread acceptance, SESS decided to choose FIPA-ACL as its agent communication language. Foundation of Intelligent Physical Agents-Agent Communication Language is shortened to FIPA-ACL [17]. Interactive learning with reinforcement will enhance the four communication agents. Every agent's behaviour is impacted by everyone else's.

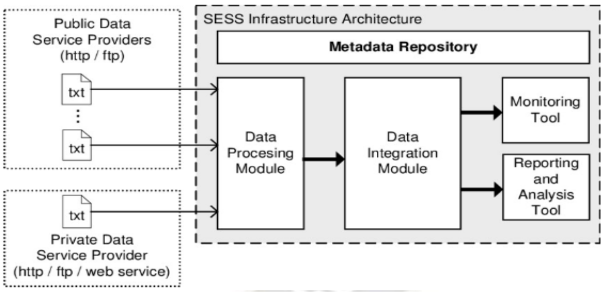

Fig 5: SESS Architecture

Feedback is generated by each successful action performed by other agents and transmitted to thecommunication agent within the same module. Following the collection of input from other agents in the module, communication agents produce a feedback report. Communication agents will be trained using the feedback reports. Depending on their efforts, communication agents will receive credit for providing feedback. Every move communication agent make will be regarded as a transaction. Most security concerns will be brought up by communication agents because they arethe only agents with the authority to give directives. The blockchain will be used to store transactions, and the system manager is the only person with access to the blockchain's smart contract (chain code). Each communication agent action is contained in a single module.

Admin
Collection Module
Data Process Module
Detection and Analysis Module
Response Module
Blockchain Smart Contract

Fig 6: SESS system sequence diagram

IV. IMPLEMENTATION:

Lack of device security, centralised data management, inflexible design, incompatibility with communications protocols, and difficulties in multiparty cooperation are only some of the issues that plague conventional IoT installations. These issues must be addressed by the IDS used for IoT networks. Blockchain's decentralised method of storing and transmitting communication messages, or orders that regulate a system's behaviour, can increase device security. By using a mutually agreed-upon smart contract to control system behaviour and agent behaviour, blockchain also contributes to the development of trust between various parties. Agents give the system the ability to scale up and down, which makes it better equipped to deal with various IoT environmentarchitectures and communication protocols. The use of agents may facilitate the system's responseto these alterations, and blockchain technology can ensure the safety of a wide-area Internet of Things network.

To further strengthen security, this system employs private chain to encrypt agent-to-agent communications. There is just one agent in the system, and it may initiate and terminate processessimultaneously. This agent combines an integrated database with a blockchain node. The cache area is going to be increased so that it includes the most recent interactions. This will reduce the amount of time needed to do a search and will speed up the rate at which agents consume and storedisc data. Doing a local search for the most current data changes can help decrease the amount ofwork that the communication agent has to complete. This may be achieved by having each agent have its own replica of the database (DB). The blockchain's detection and analysis module's communication agent acts as a super node. Its purpose is to ensure that every node in the networkmay connect to each other and get the accurate copy of the blockchain ledger in its entirety. Afterthis point, any further messengers will become complete nodes. Since they are the ones that keep and disseminate the whole blockchain ledger, they are an essential part of the process that verifieseach communication record in the blockchain. Additional agents that have been set up to functionas light nodes are able to establish connections with the communication agent, which serves as the parent node for each module. These light nodes are just responsible for transporting the block header information and are used to determine whether or not their parent node has been altered. The blockchain component is used to establish credibility in multi-party IoT networks where each participant uses their own agents, as well as to control and verify the activities of communicationagents and guarantee the safety of the whole system. The blockchain component is also utilised toestablish credibility in multi-agent IoT networks. Messages broadcast via a channel may also provide information useful for analysing assaults and enhancing agents with RL. The Java classesused by our group during blockchain development are described here.

Agent-specific data, including the agent's identity, public key, and private key, are stored in the agent account object.

The process called as create public and private key will generate these keys.The keys are encrypted using the Elliptic curve digital signature technique (ECDSA), a cryptographic procedure. This is the same mechanism that is utilised to encrypt Bitcoin accounts.As a result, this ensures that certain communication messages can only be created by the appropriate agent. Using the ECDSA cryptographic method, agents may protect the information

they exchange during communication by having their public key and private key randomly generated. This method is based on the elliptic curve digital signature algorithm.

The objective of the learning job for the intrusion detector is to construct a prediction model, also known as a classifier, that is in a position to differentiate between 'bad connections' (intrusions orassaults) and a 'good (normal) connections'.

The following are the four primary types of attacks:

a. R2L: distant machine unauthorised access, such as password guessing;

b. U2R: unauthorised "buffer overflow" attacks, for instance, that grant the attacker local superuser (root) capabilities;

c. DOS: denial-of-service, for example, syn flood;

d. U2R: unauthorised "buffer overflow" attacks, for instance, that grant the attacker local superuser (root) capabilities; surveillance as well as other types of probing, such as port scanning, are examples of probing. Algorithms Applied: Gaussian Naive Bayes, Decision Tree, Random Forest, Logistic Regression.

Linear Regression

Imagine sorting random logs by weight to see how this method works. You can't weigh each log, though. You must predict the log's weight by visually analysing its height and girth and arrangingthem. Machine learning linear regression. Fitting independent and dependent variables to a line establishes a connection. Regression line is Y= a *X + b. where minimizing the squared distance between data points and the regression line yields a & b.

RF algorithm

Random Forests are decision trees. Each tree "votes" for a class to categorise a new item based onits properties. Forest picks the most-voted categorization (over all the trees in the forest).Each treeis grown as follows: If the training set has N cases, N random cases are chosen. This is the tree's training set. If there are M input variables, then mM is provided in a way that, for each node, m variables are selected at random and the best split on these m is applied. The value of m is kept constant. Each tree is fully developed. No trimming.

Decision Tree

In machine learning, the decision tree is a common supervised learning strategy for labelling problems. It does a good job at separating out categorical and continuous data. In this method, the population is divided into two or more groups based on shared characteristics.

Gaussian Naive Bayes

A Naive Bayes classifier presupposes that a class's features are unrelated. Even though these characteristics are connected, a Naive Bayes classifier considers them separately when computing probability. An easy-to-build Naive Bayesian model is beneficial for large datasets. Simple and outperforms complex classification algorithms.

V. EVALUATION MEASURES

Evaluation of intrusion detection effectiveness will be carried out using the aforementioned accuracy, precision, recall, and F1 score metrics. Accuracy is defined as the fraction of total samples that match the prediction pair. The accuracy is based on the results of the predictions. It indicates the proportion of confirmed positive samples relative to expected positive samples. The proportion of correctly anticipated positive instances from the original sample is measured by its recall. The F1 score completely takes into consideration the estimated outcomes of the model's accuracy rate and recall rate. The better the model performs as the F1-score rises. Overfitting also has to be considered. Training, validation, and test datasets may all be made uniform with the use of one-hot coding and z-score metrics.

The same structure is used by normalisation. All of the datasets used for training, validation, and testing using one-hot encoding include categorical variables. For certain data sets, this is a replacement for a category variable. As a precaution against falling into the "dummy variable trap," a category variable has been removed from each parameter requiring one-hot encoding. The labelfor the output is located in the last "class" field. There is a single hot encoding that may be used to turn information about protocol types, services, and flags into a numerical format. By not having a protocol type, service, or flag category value, the trap of using a dummy variable may be avoided.

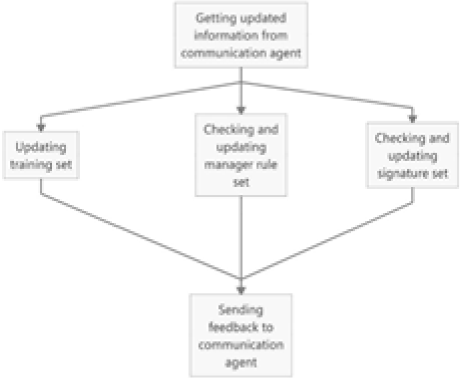
Getting updated information from communication agent
Updating training set
Checking and updating manager rule set
Checking and updating signature set
Sending feedback to communication agent

Fig 6: Database agent procedure

The database, host, and network data process agents are all under the supervision of the data process communication agent. The collecting component issues instructions to the data process agents and solicits responses from them in the form of data packages. At its request, the database agent will perform system updates. This agent not only adjusts its schedule and communication with other agents based on the health of the system. Data agents may be either stored in a database, used in a process, or accessed through a network. The gathering component issues instructions to the data processing agents and solicits responses from them in the form of data packages. At its request, the database agent will perform system updates. This agent interacts with other agents andadapts its schedule based on the state of the system.

The outcomes of these tests demonstrate that this approach may be applied to IoT networks at various scales, supporting even more complicated networks. However, additional study in this area is still required. Although the DNN model can distinguish between many attack kinds with a high degree of accuracy, some uncommon attack types cannot be detected. Future research will need to find a solution for the agents' prolonged learning curve and the requirement for large training sets. Further research is required to understand how several agents can interact effectively together in a large IoT network. Future designs need to take into account the issue of high computing power requirements.

VI. CONCLUSION

A multi-agent, deep learning and blockchain intrusion detection system are discussed in this work. The operation of each component and the overall operation of the system has been described. These innovative IDS can be used in a number of IoT scenarios thanks to multi-agent systems. Every action a communication agent does will be recorded by blockchain, protecting the system from flaws like information manipulation and disclosure. The system's performance may be improved with the help of multi-agent reinforcement. The application of neural networks is under consideration. These simulations' findings demonstrate that on the same kind of IoT network, deeplearning performs better than traditional techniques. This system can be implemented on numerous distant hosts because BC technology is used to secure ACL and agent communication. complex networks and numerous attacks.

VII. FUTURE WORK

In this article, a model for an intrusion detection system for the Internet of Things is proposed using research on multi-agent technologies, block chains, and neural networks (IoT). After that, the system will be put through its paces in an actual setting so that the modules may be continuallyimproved upon and it can be made certain that each agent is able to interact efficiently with the others. The next thing that needs to be done is to collect data sets from different IoT networks in order to improve the performance of the system and train the detection model. In addition, the creation of databases of different kinds of innovative attacks is a possible field for future research. The performance of the system might be improved by using multi-agent algorithms that are both more trustworthy and speedier. These algorithms could be used to train the communication agents, improve the process of feedback training, and increase overall system performance. Investigatingcutting-edge techniques of deep learning is one approach one might take to improve the performance of the system. Due to testing a condensed version of the block chain, the maximum height of the blocks and the DNN model hyper-parameters may be changed in later iterations utilising multi-agent reinforcement learning. Expanded IoT networks must incorporate underutilised communication output pools to ensure flow control. UNSW-BN15 datasets may alsobe tested. Future IoT system testing may need a data simulator or other tools to verify the intrusion detection system's accuracy (IDS).

REFERENCES

[1] Balamurugan, S., Ayyasamy, A., Suresh Joseph, K., (2020), Improvement of C5.0 algorithm using internet of things with Bayesian principles for food traceability systems, Modern Supply Chain Research and Applications. .

[2] Balamurugan, S., Ayyasamy, A., Suresh Joseph, K., (2020), Enhanced Petri Nets for Traceability of Food Management using Internet of Things, Peer-to-Peer Networking andApplications.

[3] "Security in Internet of Things: Issues, challenges, taxonomy, and architecture" by Adat, V. Gupta, B. Model. Anal. Des. Manag. 2018, 67, 423–441.

[4] "Security Attacks at MAC and Network Layer in Wireless Sensor Networks" by J. Adv. Res. Dyn. Control Syst. 2019, 11, 82–89.

[5] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[6] "Routing Attacks and Countermeasures in the RPL-Based Internet

of Things" by Wallgren, L.; Raza, S.; Voigt, T. Int. J. Distrib. Sens. Netw. 2013, 9, 794326.

[7] " Research on immunity-based intrusion detection technology for the Internet of Things. In Proceedings of the 2011" by Liu, C.; Yang, J.; Chen, R.; Zhang, Y.; Zeng, J. Seventh International Conference on Natural, Shanghai, China, 26–28 July 2011.

[8] " Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach " by Bostani, H.; Sheikhan, M. Comput.Commun. 2017, 98, 52–71.

[9] K. Dass , A. ., & Lokhande , S. D. . (2023). Machine Learning Based Prediction of Obsolescence Risk . International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 293–301. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2667.

[10] A Multi-tier Reinforcement Learning Model for a Cooperative Multi-agent System" by Shi, H.; Zhai, L.; Wu, H.; Hwang, M.; Hwang, K.; Hsu, H. . IEEE Trans. Cogn. Dev. Syst.2020.

[11] Calvaresi, D.; Dubovitskaya, A.; Calbimonte, J.P.; Taveter, K.; Schumacher, M. Multi- Agent Systems and Blockchain: Results from a Systematic Literature Review. In Proceedings of the International Conference on Practical Applications of Agents and Multi-Agent Systems, Toledo, Spain, 20–22 June 2018.

[12] Shi, H.; Zhai, L.; Wu, H.; Hwang, M.; Hwang, K.; Hsu, H. A Multi-tier Reinforcement Learning Model for a Cooperative Multi-agent System. IEEE Trans. Cogn. Dev. Syst. 2020. [CrossRef]

[13] Dr. Govind Shah. (2017). An Efficient Traffic Control System and License Plate Detection Using Image Processing. International Journal of New Practices in Management and Engineering, 6(01), 20 - 25. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/52.

[14] Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Gener. Comput. Syst. 2018, 82, 761–768. [CrossRef]

[15] Duong, T.; Todi, K.K.; Chaudhary, U.; Truong, H. Decentralizing Air Trac Flow Management with Blockchain-based Reinforcement Learning. In Proceedings of the IEEE 17th International Conference on Industrial Informatics (INDIN), Helsinki, Finland, 23– 25 July 2019; pp. 1795–1800. [CrossRef]

[16] Casado-Vara, R.; Prieta, F.D.L.; Prieto, J.; Corchado, J.M. Blockchain framework for IoT data quality via edge computing. In Proceedings of the BlockSys'18: 1st Workshop on Blockchain-enabled Networked Sensor System 2018, Shenzhen, China, 4 November 2018.[CrossRef]

[17] Li, D.; Deng, L.; Lee, M.; Wang, H. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. Int. J. Inf. Manag. 2019, 49, 533–545. [CrossRef] Electronics 2020, 9, 1120 26 of 27

[18] Kanna, D. ., & Muda, I. . (2021). Hybrid Stacked LSTM Based Classification in Prediction of Weather Forecasting Using Deep Learning. Research Journal of Computer Systems and Engineering, 2(1), 46:51. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/22

[19] Le, T.-T.-H.; Kim, Y.; Kim, H. Network Intrusion Detection Based on Novel Feature Selection Model and Various Recurrent Neural Networks. Appl. Sci. 2019, 9, 1392. [CrossRef]

[20] Arshad, J.; Azad, M.A.; Abdeltaif, M.M.; Salah, K. An intrusion detection framework for energy constrained IoT devices. Mech. Syst. Signal Process. 2020, 136, 106436. [CrossRef]

[21] Anthi, E.; Williams, L.; Slowinska, M.; Theodorakopoulos, G.; Burnap, P. A Supervised Intrusion Detection System for Smart Home IoT Devices. IEEE Internet Things J. 2019, 6,9042–9053. [CrossRef]

[22] Thomas Wilson, Andrew Evans, Alejandro Perez, Luis Pérez, Juan Martinez. Integrating Machine Learning and Decision Science for Effective Risk Management. Kuwait Journal of Machine Learning, 2(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/208.

[23] V. Maruthi Prasad, B. Bharathi, "A Novel Trust Negotiation Protocol for Analysing and Approving IoT Edge Computing Devices Using Machine Learning Algorithm", International Journal of Computer Networks and Applications (IJCNA), 9(6), PP: 712-723,2022, DOI: 10.22247/ijcna/2022/217704.

[24] Prasad, V. M. ., & Bharathi, B. (2023). Security in 5G Networks: A Systematic Analysis of High-Speed Data Connections. International Journal on Recent and Innovation Trends in Computing and Communication,11(5),216–222. https://doi.org/10.17762/ijritcc.v11i5.6608