Journal of Theoretical and Applied Information Technology
15th March 2024. Vol.102. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FN-AN: FREQUENT NODE BEHAVIOR ANALYSIS USING AUDITOR NODE FOR INTRUSION PREVENTION IN NETWORK CODING ENABLED SMALL CELLS

CHANUMOLU. KIRAN KUMAR[1] , NANDHA KUMAR[2]
[1,2]School of Computer Science & Engineering, VIT-AP, Andhra Pradesh-522237, India.
E-mail: [1] mounikakiran.138@gmail.com [2]nandhakumarr03@gmail.com

ABSTRACT

New vulnerabilities exist in wireless networks because of their exceptional design, which are deficient in traditional wired networks. As a result, advanced Intrusion Detection and Prevention Systems have become a necessity in today's modern information infrastructure. Mobile small cell technology is seen as a 5G enabling technology because of its potential to efficiently and cheaply bring ubiquitous 5G services to users. In addition, Network Coding (NC) technology can be expected to be an advantageous option for the wireless infrastructure of mobile small cells to boost its throughput and functionality. However, mobile small cells that use NC are susceptible to pollution attacks and Denial of Service (DoS) attacks due to the shortcomings of NC itself. The flexibility and portability of mobile small cells offered by NC is seen as a viable technology for 5G networks that may encompass the metropolitan environment on demand. Despite the many advantages that NC-enabled mobile small cells provide to the 5G of mobile networks, they present substantial security threats, which take advantage of NC's inherent vulnerabilities. Therefore, in order for NC-enabled mobile small cells to function to their full potential, intrusion prevention methods to identify and neutralize attacks are of the utmost necessity. In common parlance, an intrusion is any form of unauthorized intervention, which is almost often done maliciously. The goal of an intrusion is to gain access to an organization's internal network so that malicious actors can gather intelligent information about the organization, such as the layout of its networks or the types of software it uses, such as the operating system, tools, or applications. The Intrusion Prevention System (IPS) is sometimes known as a Intrusion Detection System (IDS), or Intrusion Detection/Prevention System. It is a program designed to keep NC enabled small cells safe by monitoring the suspicious behavior of nodes in the network. Intrusion prevention systems' primary roles include detection, analysis, reporting, and prevention of harmful behavior. Blockchains are decentralized databases that consist of continuously expanding lists of entries called blocks that are cryptographically linked together. Each block includes transaction data, a timestamp, and a cryptographic hash of the prior block. This research can make use of blockchain for recording the transactions occurred in the network. The node behavior can be stored in a block that is used for detection of malicious nodes easily in further transactions. This research presents a Time Frequent Node Behavior Analysis using Auditor Node with Flag Variable based Intrusion Prevention System (TFNBA-ANFV-IPS) with block register module using blockchain for accurate detection and prevention of intrusions. The proposed model when contrasted with traditional models performs better performance in intrusion prevention..

Keywords: *Network Coding, Small Cells, Intrusion Detection, Intrusion Prevention, Attack Detection, Node Behavior, Blockchain, Auditor Node.*

1. INTRODUCTION

The numbers of internet-enabled devices are already in the billions and growing rapidly. This trend is being driven by the increasing prevalence of sensor integration in consumer electronics. Due to limited processing capabilities, these devices often rely on others to conduct data management [1]. In order to share data like time and position, modern devices may be able to connect with one another and set up channels of communication. The proliferation of the Internet of Things (IoT) network architecture cannot be supported by the current state of mobile 4G networks [2]. The logical conclusion is that the next generation of high-bandwidth data transfer systems will be built upon

Network Coding (NC) enabled small cells [3]. The need for exceptionally high throughput and low-latency was highlighted by the introduction of NC enabled small cells, prompting the creation of next-generation networks [4]. In order to build reliable networks, 5G and later technology makes use of the IoT, Artificial Intelligence (AI) [5], and blockchain [6]. The application of Machine Learning (ML) and AI techniques has the potential to be extremely useful in the incorporation of safety procedures. To identify and classify malicious traffic [7], ML algorithms are used by scientists developing Intrusion Detection Systems (IDS). Networks using 5G and beyond will also benefit greatly from real-time threat detection [8]. The inefficiency of using the technology to detect and categorize threats in real time is the key problem in this investigation, along with the need for a lightning-fast safety mechanism and low processing latency [9].

This research proposes an IDS with prevention model that can be designed, implemented, and deployed to fulfil the stringent needs of high-bandwidth NC enabled small cells [10]. As a result, data flow has often been filtered using automated approaches. The results they provide when trying to recognize patterns in data are usually mediocre, and they can't adapt to new data and recognize new patterns [11]. An integrated Intrusion Detection And Prevention System (IDPS), such as the one described in this research [12], is notable because it is one of the few such systems that has been shown to correctly identify both recognized and unidentified threat patterns in an enormous NC enabled small cell environment without adversely affecting the low-latency levels inside the implied data network as experienced by end users [13]. NC enabled mobile small cells, the building blocks of NC enabled networks, are seen as a promising technology since they can be deployed on demand anywhere in an urban area [14]. There are severe security issues since NC enabled mobile small cells are susceptible to pollution assaults, despite the fact that this technology has numerous beneficial implications for the 5G of mobile networks [15]. Therefore, intrusion detection and prevention techniques to identify and neutralize attacks are of vital requirement for NC-enabled mobile small cells to function to their full potential [16].

Computer security rules, acceptable usage regulations, and standard security procedures are all part of what is known as "intrusion detection," which is keeping an eye on what's happening on a network or system and evaluating it for any indications of potential incidents. The performance of intrusion detection sensors should be sufficient to keep up with the networks or hosts they are monitoring, allowing them to collect all the necessary data without missing any packets. Furthermore, an adversary should be unable to identify them.

The IDS engine uses preexisting signature-based rules to identify intrusion, and then generates a new detection signature using an anomaly-based method [17]. The Software Defined Networks (SDN) controller can affect the underlying data plane by installing flow entries, some of which are security-related and filter and handle malicious traffic according to detection signature information provided by the aforementioned IDS engine [18]. Coordinated defence is enabled through a blockchain peer configuration that generates and processes transactions to disseminate the detection signature from one SDN controller to another. The intrusion detection system model is shown in Figure 1.

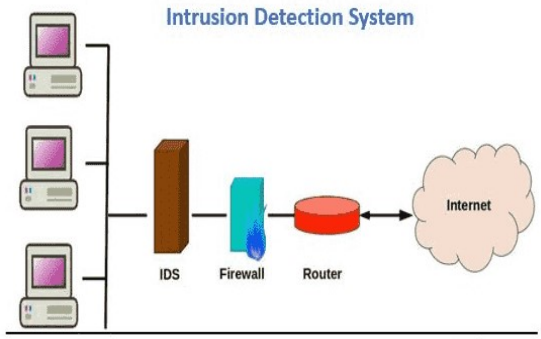

Fig 1: IDS System

The term Intrusion Prevention System (IPS) can also be used to describe a mechanism for discovering and blocking malicious attacks [19]. It is a security programme for systems and networks that monitors for unusual activity [20]. The fundamental functions of an intrusion prevention system are to monitor for malicious activity, collect relevant data, report on it, and then take measures to stop or at least slow it down. IPS and IDS are typically seen as complementary technologies since they both monitor network traffic and system processes for hostile behaviour [21]. Common IPS features include logging events, notifying security staff of significant events, and generating reports [22]. Many IPSs can do more than just identify threats; some may even respond to them. In response, the IPS may do anything from just blocking the attack to changing the security settings in the immediate area to changing the very nature of the attack itself [23]. The Figure 2 depicts the IPS model for prevention of intrusions entering into the network.

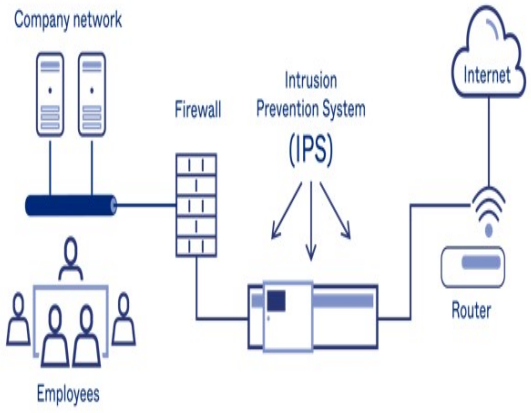

Fig 2: IPS System

In order to detect many forms of hostile network activities, modern intrusion detection systems employ a wide variety of detection techniques [24]. Although intrusions can be detected using existing methods, these approaches have their limits, which could affect the overall detection system and network performance [25]. Blockchain technology is currently one of the most innovative and crucial technologies in the modern business sector that is used in large networks for maintaining security [26]. The blockchain is undergoing continuous innovation and change. Recently, blockchain has been integrated into IDPS to boost their effectiveness. Blockchain technology is being adopted by many sectors, including the healthcare industry [27], the logistics industry, and the IoT. Using private and public key cryptography, blockchain offers various features that have enhanced the effectiveness of security in distributed peer-to-peer networks [28]. In order to investigate and stress the necessity of studying and merging both technologies, this research provides a comprehensive introduction to both systems for intrusion detection and prevention and blockchain technology. This study introduces a blockchain-based block register module for reliable intrusion detection and prevention based on Time Frequent Node Behaviour Analysis utilizing Auditor Node with Flag Variable based Intrusion Prevention System (TFNBA-ANFV-IPS). In accordance with intrusion prevention requirement to never trust but always verify, the proposed model moves trust away from the endpoint and onto the blockchain, where it can be checked against an immutable authority.

2. LITERATURE SURVEY

With the rise of bring your own device (BYOD) and telecommuting policies in businesses, traditional perimeter defence strategies are no longer enough. Zero Trust Architecture (ZTA) is a relatively new security architecture that places emphasis on preventing breaches. The ZTA assumes that each given endpoint is malicious until proven otherwise. Nevertheless, Advanced Persistent Threats (APT) can still be used to hijack a legal session, even after identification has been confirmed by the endpoint. Since ZTA's adversaries can launch a wide variety of attacks via the endpoint, it serves as the organization's primary vulnerability. Alevizos et al. [1] presented a Blockchain-enabled Intrusion Detection and Prevention System (BIDPS) that ZTA to endpoints in order to foil APT attacks. The BIDPS aims to do two things: to remove trust from the endpoint and relocate it on-chain to build an immutable system of explicit trust; and to detect and block attackers' strategies and tactics according to MITRE's ATT&CK enterprise grid before the lateral movement stage.

Most IoT devices cannot reasonably fulfil the requirements of a blockchain node due to their limited processing power and storage capacity. Therefore, blockchains are often placed on a single master node, like an edge device or the cloud, wherein they are susceptible to the following three problems: When there are few delegates, the delegate node is the single weak link. Second, the delegate node's involvement in replicating blockchain data can compromise the privacy of individual users. Because, a DDoS assault can easily bring down the delegate node. To get around these limitations, Sun et al. [2] proposed utilising IoT devices as specialized blockchain nodes to cut down on blockchain redundancy. In this paper, the author developed a blockchain-based IoT access control system that is secure, lightweight, and domain-agnostic by fusing a permission blockchain (HLF) with attribute-based access control (ABAC) and identity-based signatures (IBS). For easier management and analysis, the author divided the IoT architecture into several functional areas called IoT domains. The author builds a local blockchain ledger for every IoT domain to convert more devices into blockchain nodes. A local blockchain ledger stores the attributes of IoT domain entities, the digests of policy files, and the authorization decisions. The author deployed HLF's channel technology to permit cross-domain access and make use of the IBS to selectively filter genuine

requests for access to specific IoT domains as a defence against DDoS attacks.

Blockchain solutions have been adopted in many different industries because to its immutability. A pBFT-based Delegate PoS(DPoS) consensus technique is employed by many blockchain systems today since just a small number of validators need to agree on a shared set of rules. Since a hostile cartel controlling more than a third of the total stake can launch persistent censorship operations that disrupt the consensus process, this is a weakness of the pBFT-based DPoS consensus mechanism. To get over this drawback, Kim et al. [3] proposed an original method of defence against persistent censorship attacks. In the first step, the author introduced a consensus architecture with a main-validator and a sub-validator in a hierarchical structure. In this consensus design, sub-validators can disagree with the conclusions reached by main-validators, also known as existent validators, at any point in the process. Censorship attacks cost more money the more sub-validators that oppose the attack. Second, the author introduced a behavior-based credit-scoring function that is compatible with this consensus approach. The author proposed a function that reallocates validators depending on their behaviour to reduce the likelihood of malicious cartels developing and the persistence of censorship attacks.

WSNs rely on ad hoc nodes to coordinate its backbone architecture, with all nodes reporting back to a central base station (BS). A WSN can help speed up the creation of IoT connections between apps by merging multiple sophisticated technologies. The speed and cost of data transmissions in the IoT are two areas where numerous experts have lately presented solutions. However, most methods have been focused on constructing and developing static topologies, rather than taking into account the ever-evolving of mobile sensor nodes. Also, data protection against malicious actions needs to be rethought with minimal network overheads because sensor nodes have limited assets and the wireless communications channel is easily accessible. Haseeb et al. [4] provided an intrusion prevention architecture for mobile IoT devices that incorporates with WSN with the aim of offering data security with an enhanced network delivery ratio. The proposed model consist of two sections. The author employed the uncertainty principle to construct and maintain stable, non-overlapping clusters. As a second step, the author established multi-hop, end-to-end secure routing methods based on blockchain technology.

Due to its ability to offer 5G services to users rapidly and affordably, mobile small cell technology is viewed as a 5G enabling technology. NC technology is also being looked at as a possible solution to improve the performance and throughput of wireless networks comprised of mobile small cells. However, NC-enabled mobile small cells are open to pollution attacks due to NC's shortcomings. Although there are a variety of published methods for identifying pollution attacks, it is still possible for attackers to taint packets in transit as they send identically coded packets from the node that is the source to the destination nodes. In this study, Parsamehr et al. [5] provided an intrusion detection and location-aware prevention (IDLP) technique, which not only drops polluted packets upon detection, but also pinpoints the exact location of the attacker in order to prevent more packet pollution in the future. In order to do both detection and localization, the IDLP method employed a homomorphic MAC strategy that operates in the null space. To protect the NC-enabled mobile small cells from resource depletion, however, the proposed IDLP technique is effective since it does not have to be applied to all mobile devices in the first phase.

Industries of all stripes can stand to benefit from the IIoT's promise of improved market performance with the pervasive connection, intelligent data, statistical analysis, and decision-making tools. Common IIoT architectures are highly susceptible to a wide variety of security flaws and network breaches, compounding the issues of lack of privacy, integrity, trust, and centralization. Selvarajan et al. [6] proposed a lightweight blockchain security model (AILBSM) driven by artificial intelligence as a means of protecting the privacy and reliability of IIoT infrastructure. The purpose of this novel idea is to address concerns about data security and privacy in Cloud-based IIoT systems that perform data processing in the Cloud or at the network's edge. This study contributes significantly by merging the advantages of blockchain technology with those of artificial intelligence mechanisms based on the Convivial Optimised Sprinter Neural Network (COSNN), resulting in safer and more efficient practises. Characteristics are translated into encoded data using an Authentic Intrinsic Analysis (AIA) model, which considerably lessens the effect of attacks.

Industry 4.0 paves the way for novel applications including personalized production, real-time production monitoring, data-driven decision making, and remote maintenance. However, they are more susceptible to a wide array of cyber

threats because of their limited resources and unique composition. Theft of confidential information and financial losses are just two of the risks that these dangers bring to businesses. A more diverse industrial network is harder for attackers to penetrate. For this reason, Sivamoha et al. [7] developed an original intrusion detection system called the Bidirectional Long Short-Term Memory based Explainable Artificial Intelligence framework (BiLSTM-XAI). First, the preprocessing procedure of cleaning and normalising the data improves the data quality for network intrusion detection. The databases are then mined using the Krill herd optimisation (KHO) approach, which prioritises characteristics. The proposed BiLSTM-XAI approach enhances security and privacy in the business networking infrastructure by correctly identifying intrusions.

Cyber attacks are becoming an increasingly serious problem for today's society. The need for stronger defences is glaringly obvious. The detection of irregular behaviour on a host or network can be thought of as an example of intrusion detection. An intrusion detection system can aid in the identification of suspicious system behaviour. The primary uses of intrusion detection are to monitor intruders and to notify system administrators of any suspicious activity. Even while each network node receives only a limited number of login attempts, the current intrusion detection system cannot handle sophisticated attacks that target the entire network. Due to its inability to detect coordinated dispersed attacks, the current intrusion detection system has been replaced with a CIDS proposed by Gupta et al. [8]. The lack of trust is the primary obstacle for the CIDS. There needs to be trust between nodes in the network so that everyone can rely on the data being shared. Blockchain technology was used to implement the proof-of-concept and establish a foundation of trust. Pluggable authentication modules (PAM) were also implemented to stop an attacker from changing previously recorded login information.

Brute-force FTP, Brute-force SSH, Web Attack, Infiltration, and Botnet are just some of the attacks that may be launched against nursing homes that leverage IoT, big data, cloud computing, and machine learning technologies. The ability to correctly identify data transmitted across a network is crucial for ensuring the safety of information exchanged between client devices and a central cloud server. To detect intrusions using this data from communication security issues, Zhou et al. [9] proposed the NIDD (Network Intelligent Data Detection) model, which integrates deep convolution generation adversarial network (DCGAN), Light Gradient Boosting Machine (LightGBM), and Shapley Additive exPlanations (SHAP). The NIDD model initially generates new attack samples by learning the feature distribution of the existing attack sample data, which allows it to successfully increase the rare attack samples. The second step in building the intrusion detection model is to use the Light Gradient Boosting Machine (LightGBM) method as baseline classifier and put it through its paces on training data. The model's parameters are adjusted based on the classification results' contribution analysis with SHAP. Successful network intrusion detection using the best available model has been achieved.

Network attacks are currently the world's most pressing issue. The size of a network has little bearing on its susceptibility to attack. An IDS is crucial for spotting and stopping cybercriminal actions within a network. Effective intrusion detection systems are being developed using machine learning and deep learning in a number of fields, including information security. These devices provide quick and accurate detection of potential dangers. New hazardous threats are always being discovered and perfected, though, so networks need a smart security solution. Therefore, research into ways to create an effective intrusion detection system is crucial. Research into intrusion detection can make use of a wide variety of open-source datasets. Publicly available intrusion databases must be routinely updated to keep up with the ever-evolving nature of intrusion detection and the sophistication of new attacks. Qazi Euh et al. [10] employed deep learning to develop a hybrid intrusion detection system based on a convolutional recurrent neural network. Using a network of convolutional neural networks to collect local features and a deep-layered neural network with recurrent learning to extract the features, the proposed Hybrid Deep-Learning-Based Network Intrusion Detection System (HDLNIDS) enhances the efficiency and predictability of the intrusion detection system.

Artificial intelligence has been developed to aid in solving complicated problems throughout the scientific and business worlds that require rapid analysis and interpretation of enormous amounts of data. Network security, and IDS in particular, have benefited greatly from the application of machine learning over the past two decades. Pattern recognition, a machine learning technology, has found uses in medical applications, image processing, and video processing, among others. Abdeldayem et al. [11] suggested a two-tier IDS

architecture in this article. Network connections are categorised at the most fundamental level based on the services they offer. The author next identified the most essential characteristics for detecting malicious behaviour on that service. Next, a pattern recognition tool is used to analyze the information and decide whether or not a certain network connection is malicious. During the training phase, multivariate normal statistical techniques are used to create models of both "normal" and "attack" behaviour. In order to determine whether or not a network connection is malicious during the deployment and operation stages, the author employed two multivariate normal statistical models and a maximum likelihood estimation function. The testing results proved the proposed IDS are superior to others in its ability to identify network intrusions.

3. PROPOSED MODEL

An IDPS is a proactive method of cyber defense that monitors and reacts to unusual network activity in real time. In order to determine if allowed users are abusing their privileges or if unauthorized users are exploiting security gaps to gain unauthorized access, it monitors the network's health, activity, and usage. A block chain is a distributed ledger built with the help of cutting-edge tools including peer-to-peer networking, smart contracts, and cryptography. Using block chain technology, a distributed, immutable database can be constructed that stores node behaviour and its attributes in a secure manner. Accordingly, intrusion detection and prevention is a supplement to the conventional approach to computer security. Improving the all-encompassing nature of network and system security is the primary focus of current research and development on dynamic security protection solutions.

There are a number of methods used for intrusion detection, and each one has its advantages and disadvantages. Using a database of known threat signatures, signature-based detection compares network behavior. It works wonders against established dangers, but it can miss emerging risks. The efficiency of intrusion detection systems can be hindered and the false alarm rate can be increased by bad packets caused by flaws, faulty DNS data, or local packets that manage to escape.

As a result of the broad adoption of networking tools, people from various locations are now more connected and more at risk than ever before. Information available over networks is growing at an incredible rate. The number and variety of invasions appears endless. More complex methods of attacking computer networks are being developed. Security breaches are growing more common and more hazardous with time. Defence alone isn't enough to keep a system safe. Keeping tabs on user behaviour in real time and being able to spot new network intrusions as soon as they occur are also crucial. People's regular network needs will be compromised, and they'll be at risk from serious network threats. This research looks into intrusion detection and prevention systems in networks using blockchain so that people may take more than simply preventative measures to keep their networks safe.

The need to protect data and networks, and the need to stop attacks and prevent it is the reason that the IPS was found [3]. Firewall act like IPS, but IPS focus on attack prevention at layers that most firewalls are not able to decipher, at least not yet. [1]. There are many types of IPS that practice in many areas, these types are inline network intrusion detection system, application-based firewalls/IDS, layer seven switches, network-based application IDSs, deceptive applications. [1]. IPS is typically designed to operate completely invisibly on a network. IPS products do not typically claim an IP address on the protected network but may respond directly to any traffic in a variety of ways. As we mentioned before IPS products have ability to implement firewall rules, but it is not a core function of IPS. Also IPS offers deeper watch and monitor into network operations like bad logons, inappropriate content and many other network and application layer functions. [2]. IPS focus on what attack does, its behavior. IPS use signatures and it detect intrusions on the analysis of the traffic. The IPS prevents a large amount of downtime that would occur if it were not there, this is done by it stopping any damage that may have made its way to the databases from internal or even external attacks. The IPS also makes it easier for the administrators to see where attacks are coming from so that they can address them and prevent any further attacks from that location [3].

The need to protect data and networks, and the need to stop attacks and prevent it is the reason that the IPS was found [3]. Firewall act like IPS, but IPS focus on attack prevention at layers that most firewalls are not able to decipher, at least not yet [1].

IPS is typically designed to operate completely invisibly on a network. IPS products do not typically claim an IP address on the protected network but may respond directly to any traffic in a variety of ways. As we mentioned before

IPS products have ability to implement firewall rules, but it is not a core function of IPS. Also IPS offers deeper watch and monitor into network operations like bad logons, inappropriate content and many other network and application layer functions [2].

The combination of IDS with an IPS provides a comprehensive security solution for a reliable network. Provision of, or upkeep of, secure network services is essential. In this sense, IDS and IPS are both examples of network security devices. The methods through which these devices are integrated into the network are distinctive. In contrast to IPS, which can be deployed in either a promiscuous or out-of-band mode, IDS can only be placed outside of the network and can only get a copy of the traffic. When IPS detects malicious traffic or suspicious activity, it takes actions like terminating, blocking, or dropping the connections, whereas an IDS will only detect the malicious traffic, take no action, and generate only alerts. By fusing the functions of firewalls and IDS, an IPS creates a smart instrument that can adapt the settings of network gateways in response to actual threats and records in the blockchain. Typically, an IDPS system will operate in either a detection mode or a prevention mode. It takes up residence in the network like any other node and, once activated, quietly scans the data without interfering with the flow of information. However, in the prevention mode of IDPS, all normal traffic is routed through IDPS. IDS can monitor for intrusions and notify a security administrator, but it cannot take any action to fix the problem itself. Like IDS, IPS can take preventative measures against intrusions, but it needs to be set up by a security administrator for each different kind of traffic and assault. As part of a standard operating procedure, this cannot be computerized. Having security mechanisms in place may be ineffective if the company lacks the resources to promptly address issues and alarms. The working of IPS model is shown in Figure 3.

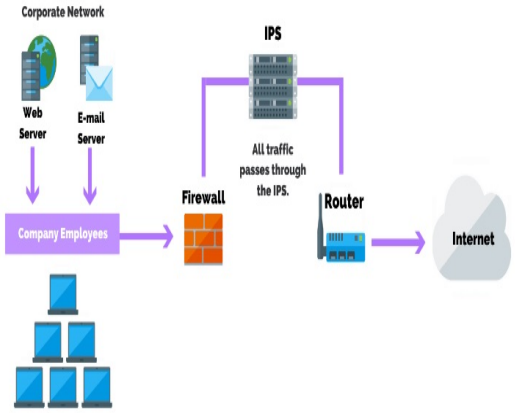

Fig 3: IPS Model Working

The security policy and network architecture of the organization will dictate the optimal placement and configuration of the sensors. Deploying in detection mode is the recommended starting point for each mission. It is best to switch to prevention mode once the IDS has a firm grasp on the network and the baseline profile has been established. In most cases, IPS is created to be entirely stealthy while yet doing its job on a network. While IPS devices usually don't take up residence at a specific IP address on the protected network, they can nonetheless react to traffic in a number of different ways. Although firewall rule implementation is possible with IPS systems, it is not a primary function of IPS. In addition, IPS allows for more in-depth monitoring of network activities like malicious logins, offensive content, and other operations at the network and application layers. IPS systems analyze the actions and patterns of an attack. Intrusion Prevention Systems analyze traffic based on signatures to identify malicious activity. By thwarting any harm that would have been done to databases by internal or external assaults, the IPS eliminates a great deal of downtime that would otherwise occur. The IPS also aids administrators in tracing the origin of attacks, which is crucial for mitigating the current one and preventing future ones.

The 51% attack is a critical flaw in the security of the block chain. According to the consensus mechanism of the block chain, two fork chains are created when two miners mine two different blocks at the same moment. After the longer chains have been validated, the shorter ones will be dropped. If the fork is maliciously created, however, the original chain will be abandoned in favour of the longer fork chain. The likelihood of an assault on the entire system increases proportionally with the size of the network. In addition, the miners could

potentially corrupt the data of the entire block chain system if they are greedy and join together to gain an advantage in the mining process. However, block chain technology is secure since it is immutable. Due to the fact that the Bitcoin block chain does not require the user to reveal their true identity, the address data of the relevant user are included in the transaction and are thus untouchable. If an individual's address is related to their personal information, then it is protected. If the user's email address were made public, all of their transactions would be at risk. Although information disclosure can be moved by creating multiple additional addresses, it is not yet clear if this satisfies the psychological needs of users for smooth functioning. The proposed model architecture is shown in Figure 4.

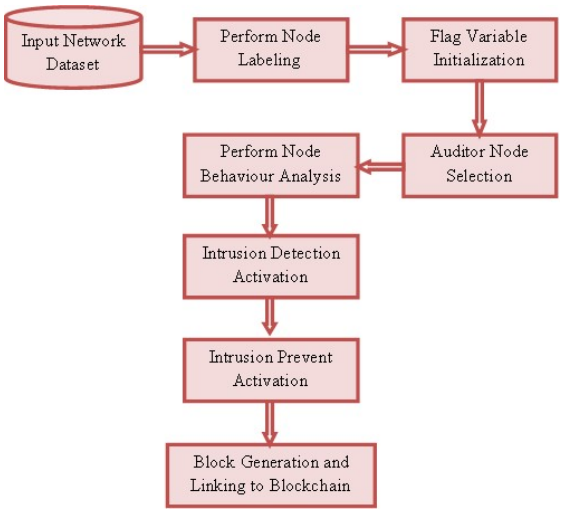

Fig 4: Proposed Model Architecture

Block chain technology uses cryptography and other security measures to create novel approaches to storing and processing data. Block chains, which are designed to be more secure against tampering and denial-of-service attacks, have more stringent requirements for network setup than conventional databases. Secure communication is attained by employing block chain technology. In a wide variety of network configurations, block chain technology can reliably provide communication services. A blockchain network does not require a central server. If a block chain network experiences a disruption in communication between some of its nodes, the network as a whole can still function normally. The normal pattern of information transfer over the network has been maintained. The management of both mobile and immovable property can benefit from the increased use of block chains. Information stored in a block chain cannot be altered once it has been recorded; hence this feature is used to verify the integrity of data during network resource management and monitoring. This research presents a Time Frequent Node Behavior Analysis using Auditor Node with Flag Variable based Intrusion Prevention System with block register module using blockchain for accurate detection and prevention of intrusions.

Algorithm TFNBA-ANFV-IPS

BEGIN

The nodes in the network will be monitored using the unique label for each node to identify the behaviour of nodes and their performance in the network. Each node will be allotted with a unique label that is performed as

$$\lambda \leftarrow \sum_{u=1}^{M} getNID(u) + rand(u) \quad (1)$$

$$\gamma \leftarrow \sum_{u=1}^{M} getPrime(u) \quad (2)$$

$$\tau \leftarrow \sum_{u=1}^{M} getTimeInst(u) \quad (3)$$

$$Ulabel[M] = \sum_{u=1}^{M} getaddr(u) + \lambda + \gamma + \tau \quad (4)$$

In the proposed model, getNID() is used to consider the node identity value, rand() model generates a random value for each node and getPrime() is used to consider a unique prime value for each node and getTimeInst() is used to get the registered time instant for avoiding attackers to reuse the data. getaddr() considers the physical address of the node.

The proposed model considers a flag variable that is used to monitor the changes in the network traffic. The changes or updations in the flag variable results in the unusual patterns in the network traffic that need to be monitored. The flag variable initialization is performed as

$$NFV[M] = \prod_{u=1}^{M} setVal(u) \begin{cases} Val \leftarrow 0 & if\ Ulabel(u) > 0 \\ Null & Otherwise \end{cases} \quad (5)$$

Initially, the every registered node will have a Node Flag Variable that is set to zero if the node is successfully initialized. Otherwise null will be maintained.

The nodes in the network after allocating the unique label can involve in network transmissions.

The attacker will perform malicious actions in the network that degrades the network performance. To monitor each node behavior in the network, this proposed model selects a node that has best performance metrics as the Auditor Node (AN). The AN node selection is performed and the node behaviour is analyzed as

$$G[M] \leftarrow \sum_{u=1}^{M} \max(\beta(u)) + Ulabel(u) + \omega \quad (6)$$

$$P \leftarrow \sum_{u=1}^{M} \frac{\max(\mu(u,u+1))}{\omega} \quad (7)$$

$$L \leftarrow \sum_{u=1}^{M} \omega(u) - \max(\mu(u,u+1)) \quad (8)$$

$$AN[M] = \prod_{u=1}^{M} Ulabel(u) + nodeaddr(u) \begin{cases} AN(u) \leftarrow nodeaddr(u) \ if \ (\max(G(u)) + \max(P(u)) + \max(L(u) > Th) \\ Nil \end{cases} \quad Otherwise \quad (9)$$

Here ω is the total generated packets in the network. μ is the packet delivery rate of a node.

The traffic patterns are monitored by the AN node in the network and the changes in the traffic and patterns will result for a intrusion. The Intrusion is activity that degrades the network performance. The intrusion detection is performed as

$$Tanalysis[M] = \sum_{u=1}^{M} \frac{\max(\mu(u))}{\omega} + \max(C(u)) \quad (10)$$

$$IDS[M] = \sum_{u=1}^{M} diff(Tanalysis(u,u+1)) + \frac{loss(P)}{\omega} \begin{cases} IDS(u) \leftarrow 1 if \ diff(Tanalysis(u,u+1)) > Th \ and \ Loss > D \\ IDS(u) \leftarrow 0 \end{cases} \quad Otherwise \quad (11)$$

C() is the model used to consider the capacity of traffic flow in packets. diff() model identifies the traffic differences and limit. Th is the threshold value for similarity levels, D is the loss level threshold level.

The unusual patterns in the traffic triggers the IPS model to keen monitoring of the node behaviour information using AN node and the traffic is blocked and the malicious action detected node is labelelled as malicious not to consider such nodes in further communication. The IPS triggering and blocking is performed as

$$TM[M] = \sum_{u=1}^{M} \delta(Ulabel(u)) + \lim_{u \to M} \left(\omega(u) + \frac{\max(P(u))}{\max(C(u))}\right)^2 \quad (12)$$

$$IPS[M] = \prod_{u=1}^{M} \max(TM(u)) + diff(IDS(u,u+1)) + \frac{\omega(u)}{\delta(u)} \begin{cases} IPS(u) \leftarrow 1 \ if (diff(TM(u,u+1)) \geq \delta \ and \ P(u) < Th \\ IPS(u) \leftarrow 0 \end{cases} \quad Otherwise \quad (13)$$

Here δ is the traffic limit of a node in the network.

When a intrusion is detected and the nodes causing intrusions are detected by the AN node, the information and transaction process is stored in the block of a block chain. The block generation and linking is performed as

$$Block[M(u)] \leftarrow \sum_{u=1}^{M} TimeInst(u) + neighNodeaddr(u) + Trans(u,u+1) \quad (14)$$

$$Hash[M(u)] \leftarrow \sum_{u=1}^{M} \frac{getaddr(u)}{M} + \frac{Ulabel(u)}{\omega} + D \quad (15)$$

$$BC[M] = \prod_{u=1}^{M} \frac{Hash(u)}{\omega} + getaddr(Block(u)) + setlink\left(Block(Hash(u,u+1))\right) + \frac{\min(Hash(u))}{\delta} \quad (16)$$

END

4. RESULTS

The purpose of intrusion detection and prevention system, or IDPS, is to monitor a network or computer system and alert administrators of any suspicious or harmful activities and preventing

them from attacking the network. Protecting networks against intrusion attempts, data loss, and other threats appears to be IDPS's major job. Malicious actions can be gathered in one place by a system or processed and screened by a trusted human. Then, either automatically or manually, preventative measures are taken after false assaults have been defined using filtering procedures. In order to detect many forms of hostile network activities, modern IDPS systems employ a wide variety of detection and prevention techniques. Although intrusions can be detected using existing methods, these approaches have their limits, which could affect the overall surveillance system and network performance. Blockchain technology is currently one of the most innovative and crucial technologies in the modern business sector. The blockchain is undergoing continuous innovation and change. It's a set of building bricks that, despite great distances, may help keep secrets hidden and trust between people strong. Recently, blockchain has been integrated into intrusion detection systems and then preventive system is activated continuously to boost their effectiveness. Using private and public key cryptography, blockchain offers various features that have enhanced the effectiveness of security in distributed peer-to-peer networks. This research presents a Time Frequent Node Behavior Analysis using Auditor Node with Flag Variable based Intrusion Prevention System (TFNBA-ANFV-IPS) with block register module using blockchain for accurate detection and prevention of intrusions. The proposed model is compared with the traditional unsupervised intrusion prevention system (IPS) for automotive controller area networks (UIPS-ACAN), Blockchain enabled intrusion detection and prevention system (BIDPS) and Real-Time Network Intrusion Prevention System based on Hybrid Machine Learning (RNIPS-HML) and the results represent that the proposed model detection and prevention rate is high than the traditional models.

The proposed model performs node labeling by allocating a unique value to each node. The node label of each node helps in detection of each node accurately for monitoring the node behaviour and traffic analysis at each node. The Node Labeling Time Levels of the proposed and existing models are shown in Table 1 and Figure 5.

Table 1: Node Labeling Time Levels

Nodes Considered	Models Considered			
	TFNBA-ANFV-IPS Model	UIPS-ACAN Model	BIDPS Model	RNIPS-HML Model
10000	17.1	20.1	18.5	21
20000	17.3	20.3	18.8	21.2
30000	17.4	20.5	19	21.5
40000	17.7	20.7	19.2	21.6
50000	17.8	20.8	19.3	21.8
60000	18	21	19.5	22

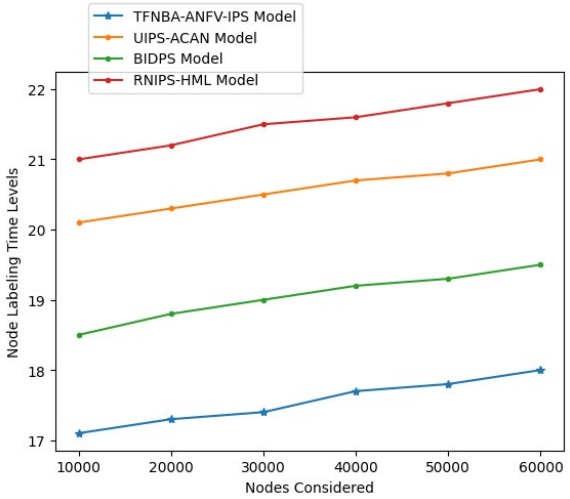

Fig 5: Node Labeling Time Levels

The flag variable is considered for traffic monitoring and is considered for unusual activity detection. The flad variable is updated if there is a change in the traffic flow and traffic patterns. The flag variable remains constant when there is normal traffic pattern and flow. The Flag Variable Initialization Time Levels of the traditional and proposed models are shown in Table 2 and Figure 6.

Table 2: Flag Variable Initialization Time Levels

Nodes Considered	Models Considered			
	TFNBA-ANFV-IPS Model	UIPS-ACAN Model	BIDPS Model	RNIPS-HML Model
10000	4.3	10.4	13.5	11
20000	4.7	10.7	13.8	11.5
30000	5	11	14	12
40000	5.2	11.2	14.1	12.5
50000	5.6	11.5	14.3	13
60000	6	12	14.5	13.5

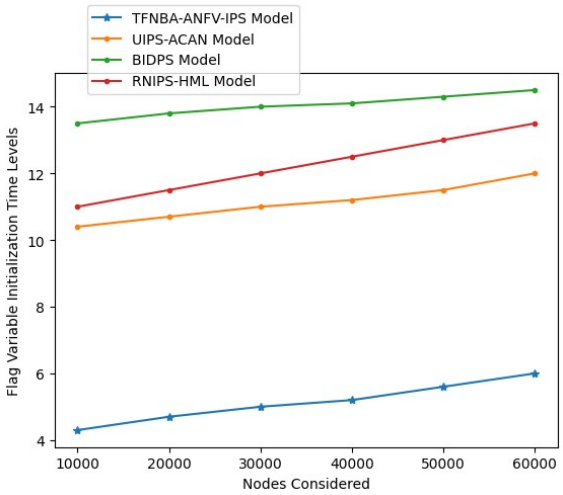

Fig 6: Flag Variable Initialization Time Levels

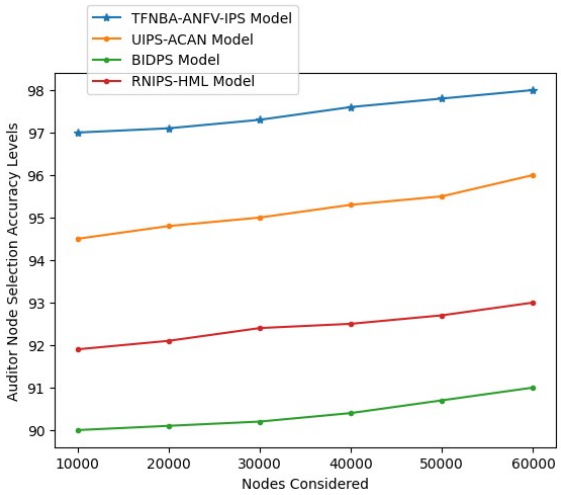

Fig 7: Auditor Node Selection Accuracy Levels

Auditor node is selected from the existed registered nodes. The auditor node will monitor the behaviour of each node in the network during traffic management. The monitoring of the AN node will help in identification of malicious nodes. The Auditor Node Selection Accuracy Levels of the proposed and existing models are shown in Table 3 and Figure 7.

Every node in the network has their own behaviour and the transmission rate. The node behaviour will change if any malicious injections happen in the network. The node behaviour changes in the network in degradation of network performance. The Table 4 and the Figure 8 shows the Node Behaviour Analysis Accuracy Levels of the existing and proposed models.

Table 3: Auditor Node Selection Accuracy Levels

Nodes Considered	Models Considered			
	TFNBA-ANFV-IPS Model	UIPS-ACAN Model	BIDPS Model	RNIPS-HML Model
10000	97	94.5	90	91.9
20000	97.1	94.8	90.1	92.1
30000	97.3	95	90.2	92.4
40000	97.6	95.3	90.4	92.5
50000	97.8	95.5	90.7	92.7
60000	98	96	91	93

Table 4: Node Behaviour Analysis Accuracy Levels

Nodes Considered	Models Considered			
	TFNBA-ANFV-IPS Model	UIPS-ACAN Model	BIDPS Model	RNIPS-HML Model
10000	95	89.8	92.5	91
20000	95.3	90.1	92.7	91.3
30000	95.5	90.3	92.8	91.5
40000	95.7	90.5	93	91.7
50000	95.8	90.7	93.2	91.8
60000	96	91	93.5	92

Journal of Theoretical and Applied Information Technology
15th March 2024. Vol.102. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

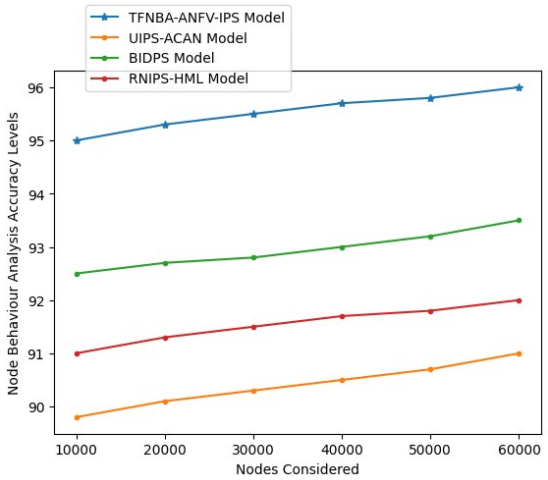

Fig 8: Node Behaviour Analysis Accuracy Levels

The change in the Flag Variable and the node behaviour analysis by the AN node in the traffic monitoring is performed frequently and any malicious actions will be tracked. The intrusion causing nodes will be identified by the behavioral changes. The Intrusion Detection Accuracy Levels of the proposed and existing models are shown in Table 5 and Figure 9.

Table 5: Intrusion Detection Accuracy Levels

Nodes Considered	Models Considered			
	TFNBA-ANFV-IPS Model	UIPS-ACAN Model	BIDPS Model	RNIPS-HML Model
10000	97.9	92	93	90
20000	98	92.2	93.2	90.1
30000	98.1	92.4	93.3	90.2
40000	98.3	92.5	93.5	90.4
50000	98.4	92.7	93.8	90.7
60000	98.5	93	94	91

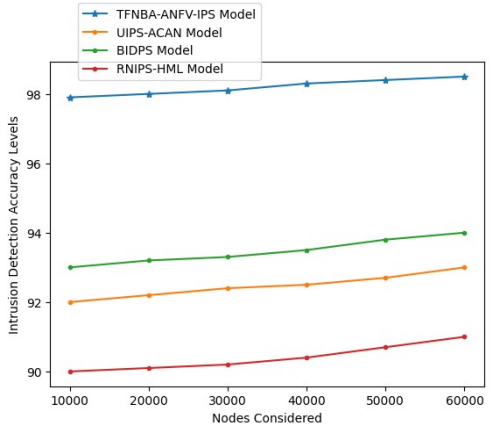

Fig 9: Intrusion Detection Accuracy Levels

IDPS is a system or network security application that keeps monitoring suspicious behaviour. Intrusion prevention systems' primary roles are to detect harmful activity, gather data about it, report it, and then try to prevent or block it. The Table 6 and Figure 10 shows the Intrusion Prevention Accuracy Levels of the proposed and existing models.

Table 6: Intrusion Prevention Accuracy Levels

Nodes Considered	Models Considered			
	TFNBA-ANFV-IPS Model	UIPS-ACAN Model	BIDPS Model	RNIPS-HML Model
10000	98	95.4	90	93
20000	98.1	95.5	90.5	93.2
30000	98.3	95.7	90.7	93.5
40000	98.5	96	91	93.7
50000	98.6	96.3	91.4	93.8
60000	98.7	96.5	92	94

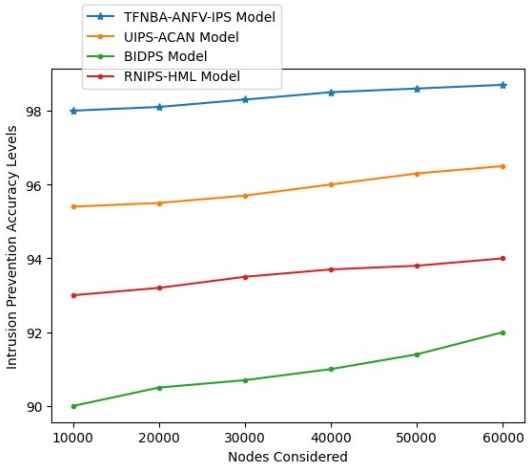

Fig 10: Intrusion Prevention Accuracy Levels

The proposed model generates a block when an intrusion is occurred in the network. The transaction data or node behavior is permanently recorded in the block of a block chain. The block information is used to identify the node properties that help in better performance levels of the network. The Blockchain Generation and Linking Time Levels of the proposed and existing models are shown in Table 7 and Figure 11.

Table 7: Blockchain Generation and Linking Time Levels

Nodes Considered	Models Considered			
	TFNBA-ANFV-IPS Model	UIPS-ACAN Model	BIDPS Model	RNIPS-HML Model
10000	16	22	20.8	26
20000	16.3	22.4	21	26.5
30000	16.7	22.7	21.4	27
40000	17	23	21.6	27.4
50000	17.4	23.5	22	27.7
60000	18	24	23	28

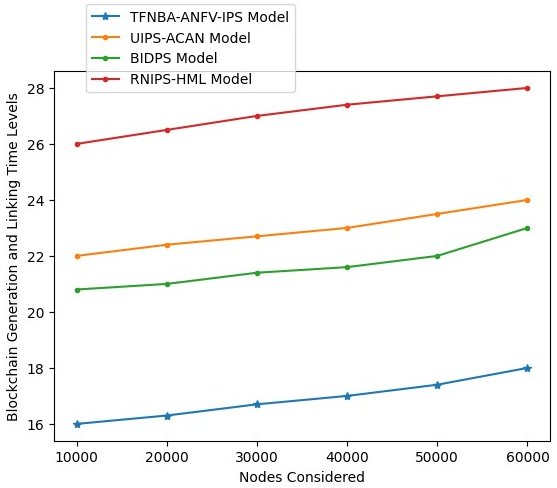

Fig 11: Blockchain Generation and Linking Time Levels

5. CONCLUSION

The combination of IDS with an IPS provides a comprehensive security solution for a reliable network. Provision of, or upkeep of, secure network services is essential. In this sense, IDS and IPS are both examples of network security devices. The methods through which these devices are integrated into the network are distinctive. In contrast to IPS, which can be deployed in either a promiscuous or out-of-band mode, IDS can only be placed outside of the network and can only get a copy of the traffic. Intrusion detection systems have been the focus of cyber security research for the majority of its existence. The goal of intrusion detection technology is to keep a close eye on any suspicious network activity, stop any attacks in their tracks before they can spread, and seal off the compromised area. Due to the network's characteristics, complexity, variety of attacks, and rapid updates, the initial single detection strategy has been shown to be inadequate for effectively and timely monitoring of aberrant behaviour. Integrating IDS with IPS is a fruitful area of study because IDPS strength can increase the security of the individually centralized networks by developing a coordinated defense across multiple domains, and because IDPS has become the standard network management that splits flow control intelligence and the data plane. This research presents a Time Frequent Node Behavior Analysis using Auditor Node with Flag Variable based Intrusion Prevention System with block register module using blockchain for accurate detection and prevention of intrusions. The intrusion detection system in the network will effectively detect the attacks and prevention system will continuously monitor the network for preventing the intrusions from entering into the network. The node behaviors are analyzed and are recorded in the block chain. As block chains are immutable in nature, the data will not be changed and users can easily identify the malicious nodes in the network and avoid them to be part of communication. In future, multiple patterns can be trained to the model for detecting numerous attacks to improve network efficiency. The feature dimensionality reduction models can be applied in future for reducing the training feature set.

REFERENCES

[1] L. Alevizos, M. H. Eiza, V. T. Ta, Q. Shi and J. Read, "Blockchain-Enabled Intrusion Detection and Prevention System of APTs Within Zero Trust Architecture," in IEEE Access, vol. 10, pp. 89270-89288, 2022, doi: 10.1109/ACCESS.2022.3200165.

[2] S. Sun, R. Du, S. Chen and W. Li, "Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain," in IEEE Access, vol. 9, pp. 36868-36878, 2021, doi: 10.1109/ACCESS.2021.3059863.

[3] J. -S. Kim, J. -M. Shin, S. -H. Choi and Y. -H. Choi, "A Study on Prevention and Automatic Recovery of Blockchain Networks Against Persistent Censorship Attacks," in IEEE Access, vol. 10, pp. 110770-110784, 2022, doi: 10.1109/ACCESS.2022.3214213.

[4] K. Haseeb, N. Islam, A. Almogren and I. Ud Din, "Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things," in IEEE Access, vol. 7, pp. 185496-185505, 2019, doi: 10.1109/ACCESS.2019.2960633.

[5] R. Parsamehr, G. Mantas, J. Rodriguez and J. -F. Martínez-Ortega, "IDLP: An Efficient Intrusion Detection and Location-Aware Prevention Mechanism for Network Coding-Enabled Mobile Small Cells," in IEEE Access, vol. 8, pp. 43863-43875, 2020, doi: 10.1109/ACCESS.2020.2977428.

[6] Selvarajan, S., Srivastava, G., Khadidos, A.O. et al. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. J Cloud Comp 12, 38 (2023). https://doi.org/10.1186/s13677-023-00412-y

[7] Sivamohan, S., Sridhar, S.S. An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework. Neural Comput & Applic 35, 11459–11475 (2023). https://doi.org/10.1007/s00521-023-08319-0

[8] Gupta RK, Chawla V, Pateriya RK, Shukla PK, Mahfoudh S, Shah SBH. Improving Collaborative Intrusion Detection System Using Blockchain and Pluggable Authentication Modules for Sustainable Smart City. Sustainability. 2023; 15(3):2133. https://doi.org/10.3390/su15032133

[9] Zhou, F., Du, X., Li, W. et al. NIDD: an intelligent network intrusion detection model for nursing homes. J Cloud Comp 11, 91 (2022). https://doi.org/10.1186/s13677-022-00361-y

[10] Qazi EUH, Faheem MH, Zia T. HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System. Applied Sciences. 2023; 13(8):4921. https://doi.org/10.3390/app13084921

[11] Abdeldayem MM. Intrusion Detection System Based on Pattern Recognition. Arab J Sci Eng. 2022 Nov 7:1-9. doi: 10.1007/s13369-022-07421-0. Epub ahead of print. PMID: 36373125; PMCID: PMC9638289.

[12] V. Bourne, Global Study: Nearly Nine Ten Employees (89%) Would be Willing to Take a Pay Cut if Their Employer Let Them Choose Their Work Device, Sep. 2021, [online] Available: https://www.jamf.com/resources/press-releases/global-study-nearly-nine-in-ten-employees-89-would-be-willing-to-take-a-pay-cut-if-their-employer-let-them-choose-their-work-device/.

[13] H. Bian, T. Bai, M. A. Salahuddin, N. Limam, A. A. Daya and R. Boutaba, "Uncovering lateral movement using authentication logs", IEEE Trans. Netw. Service Manage., vol. 18, no. 1, pp. 1063-1094, Jan. 2021.

[14] P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo and F. L. Soares, "An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks With a Low-Cost Platform," in IEEE Access, vol. 9, pp. 166855-166869, 2021, doi: 10.1109/ACCESS.2021.3136147.

[15] L. Alevizos, M. H. Eiza, V. T. Ta, Q. Shi and J. Read, "Blockchain-Enabled Intrusion Detection and Prevention System of APTs Within Zero Trust Architecture," in IEEE Access, vol. 10, pp. 89270-89288, 2022, doi: 10.1109/ACCESS.2022.3200165.

[16] W. Seo and W. Pak, "Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning," in IEEE Access, vol. 9, pp. 46386-46397, 2021, doi: 10.1109/ACCESS.2021.3066620.

[17] L. Alevizos, V. T. Ta and M. Hashem Eiza, "Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review", Secur. Privacy, vol. 5, no. 1, pp. e191, Jan. 2022.

[18] A.Gabillon, R. Gallier and E. Bruno, "Access controls for IoT networks", Social Netw. Comput. Sci., vol. 1, no. 1, pp. 1-13, Jan. 2020.

[19] Ghaleb, F.; Saeed, F.; Al-Sarem, M.; Ali Saleh Al-rimy, B.; Boulila, W.; Eljialy, A.E.M.; Aloufi, K.; Alazab, M. Misbehavior-Aware On-Demand Collaborative Intrusion Detection System Using Distributed Ensemble Learning for VANET. Electronics 2020, 9, 1411. [Google Scholar] [CrossRef]

[20] Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G.; Efstathopoulos, G.; Panaousis, E.A. A Novel Multivariate Intrusion Detection System for Smart Grid. Sensors 2020, 20, 5305. [Google Scholar] [CrossRef] [PubMed]

[21] Iwendi, C.; Anajemba, J.H.; Biamba, C.; Ngabo, D. Security of Things Intrusion Detection System for Smart Healthcare. Electronics 2021, 10, 1375. [Google Scholar] [CrossRef]

[22] Kotecha, K.; Verma, R.; Rao, P.V.; Prasad, P.; Mishra, V.K.; Badal, T.; Jain, D.; Garg, D.; Sharma, S. Enhanced Network Intrusion Detection System. Sensors 2021, 21, 7835. [Google Scholar] [CrossRef] [PubMed]

[23] Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. Ad Hoc

Netw. 2019, 90, 101842. [Google Scholar] [CrossRef]

[24] Elrawy, M.F.; Awad, A.I.; Hamed, H.F. Intrusion detection systems for IoT-based smart environments: A survey. J. Cloud Comput. 2018, 7, 1–20. [Google Scholar] [CrossRef][Green Version]

[25] Elsaeidy, A.; Munasinghe, K.S.; Sharma, D.; Jamalipour, A. Intrusion detection in smart cities using Restricted Boltzmann Machines. J. Netw. Comput. Appl. 2019, 135, 76–83. [Google Scholar] [CrossRef]

[26] Saba, T. Intrusion Detection in Smart City Hospitals using Ensemble Classifiers. In Proceedings of the 13th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, UK, 14–17 December 2020. [Google Scholar] [CrossRef]

[27] Muhannadu MS (2019) Generative adversarial networks for launching and thwarting adversarial attacks on networks intrusion detection systems[C] // 15th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE, Tangier, pp 78–83

[28] Salem M, Taheri S, Yuan J (2018) Anomaly generation using generative adversarial networks in host-based intrusion detection[C] // IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference(UEMCON). IEEE, Seattele, pp 683–687

[29] Ramasamy LK, Khan F, Shah M, Prasad BVVS, Iwendi C, Biamba C (2022) Secure Smart Wearable Computing through Artificial Intelligence-Enabled Internet of Things and Cyber-Physical Systems for Health Monitoring. Sensors 22:1076. https://doi.org/10.3390/s22031076

[30] Onyema EM, Dalal S, Romero CAT et al (2022) Design of Intrusion Detection System based on Cyborg intelligence for security of Cloud Network Traffic of Smart Cities. J Cloud Comp 11:26. https://doi.org/10.1186/s13677-022-00305-6

[31] Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y (2020) Generative adversarial networks. Commun ACM 63(11):139–44. https://doi.org/10.1145/3422622