Jestr

Journal of Engineering Science and Technology Review 18 (1) (2025) 57-79

Research Article

JOURNAL OF
**Engineering Science and Technology Review**

www.jestr.org

# Intrusion Detection Using Blockchain in Software-Defined Networking: A Literature Review

**Patikiri Arachchige Don Shehan Nilmantha Wijesekara***

*Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Galle 80000, Sri Lanka*

Received 12 February 2024; Accepted 28 January 2025

***Abstract***

Network Intrusion Detection (ID) attempts to detect diverse security attacks using a security system to monitor, analyze, detect, and respond to threats. In Software Defined Networking (SDN), ID that typically occurs at the controller is influenced by application policies and is advantageous over generic networking due to the network and flow awareness of the controller and the threat response capability of the controller itself. A blockchain system embodies a succession of attached blocks that implicitly maintain the purity, preserve the indisputability, and preserve the quasi-anonymity of its transactions/activities because of consensus protocols and cryptographic algorithms. Being the front-line reviewers for BC-centered ID in SDN, we group blockchain roles in ID in three ways and elaborately examine those pertaining to ID techniques and ID approaches, blockchain components, attack detection, network components, and so forth. We stacked a preliminary sample of 97 paper sources by sifting through the articles for selection guidelines inquired from virtual libraries, applying an elaborate and overtime procedure. Centered upon this examination, blockchain-centered ID in SDN involves collaborative ID by engaging smart contracts while storing data required for threat detection in blockchain, off-chain ID while applying blockchain for trust management, and applying blockchain for authentication and secure data storage for off-chain ID. Elaborate examination divulges that from blockchain-centered SDN ID proposals, 48.9% apply blockchain-centered secure storage for off-chain ID, 91.2% engage systematic blockchain architecture, 8.9% apply PoAuthority consensus, 100% online, 75.5% active response, 71.1% fully distributed, and 57.8% apply hybrid host and network-centered ID, with DDoS being the most dominant (17.8%) specific attack category. Finally, we explore the potentials and hardships of the schema of blockchain-centered ID in SDN and then supply insights to overtake them.

*Keywords:* SDN, intrusion identification, blockchain-centered ID, collaboration, DDoS

## 1. Introduction

Software Defined Networking (SDN) is a paradigm that necessarily has a logically centralized controller decoupled from the data plane to decide upon network operations like routing, load balancing, energy management, and such [1]. Owing to the logically centralized controller, this architecture is enhanced by a global network view, resulting in high programmability and flexibility compared to traditional networking [2]. Nevertheless, so as to prevent the primary point of breakdown and to improve scalability, a hierarchy of controllers or multiple same-level (flat) controllers that control a subset of network equipment can exist in SDN [3].

Network Intrusion Detection (ID) involves the detection of network centered-attacks, host-centered attacks, software attacks, physical attacks, human attacks, etc. using a security framework that can monitor, analyze, detect, and respond to threats in an online or offline approach [4]. There are 3 high-level ID techniques as signature-centered detection, anomaly-centered detection, and hybrid signature and anomaly-centered detection. In signature-centered detection, network traffic is compared with a database of threat signatures, while in anomaly-centered detection, the behavior of network activities, events, connections, etc. is monitored for deviation from normal behavior [5]. In each of the high-level ID techniques stated before, different low-level ID techniques, namely statistics, patterns, rules, states, heuristic algorithms, artificial intelligence, etc., can be assisted as bases for ID [6]. Furthermore, ID can be classified centered upon data collection technique: in centralized data collection, network-centered ID can be implemented, whereas in a distributed and collaborative approach, hybrid host and network-centered ID can take place, and in a distributed and standalone approach, host-centered ID can be implemented [7].

Compared to ID in traditional networking, ID in SDN is additionally driven by the influence of application policies in addition to the implemented Intrusion Detection System (IDS), where the decision made by the controller regarding ID is taken considering the application policies defined by the network administrators [8]. Additionally, the types of threats detected by ID techniques in traditional networking and SDN are similar, as both network paradigms' ID attempts to detect diverse network threats such as Denial of Service (DoS), traffic anomalies, malware or viruses, unauthorized access, etc. [9]. However, the approaches to threat detection and response are different in SDN, where the centralized controller can be applied to enforce security policies defined by the administrator and make a response such as rerouting traffic dynamically in response to detected threats [10]. Moreover, in SDN, it allows flow-centered threat detection that operates on the basis of flows due to the natural awareness of flows by the centralized SDN controller, in contrast to traditional networking, where additional techniques are required to be aware of flows [11]. Furthermore, SDN promotes network slicing, and ID can involve monitoring with respect to each network slice within a given physical network [12].

*E-mail address: nilmantha@eie.ruh.ac.lk
ISSN: 1791-2377 
doi:10.25103/jestr.181.07

A blockchain indispensably embodies a succession of blocks attached in a systematic or erratic approach modeled after the design of the cryptographic ledger advancement [13]. Especially when transactions/blocks are tied to one another, utilizing a specific block/transaction that keeps the cryptographic hash of one or more parent transactions/blocks establishes their permanence [14]. Furthermore, they enforce a collective decision protocol like proof-centered collective decision or vote-centered collective decision for verifying the blocks in the circle of peers preceding the addition of a block in the cryptographic ledger advancement [15]. Besides, they harness cryptographic hash computations to preserve purity and cyber signatures to preserve transaction indisputability [16]. Further, they have the capacity to include tough cryptographic algorithms like non-interactive proofs of knowledge and cutting-edge cryptography for shielding against quantum intrusions [17], boosting the facet of confidentiality defense in blockchain. Nonetheless, authentic blockchain on its own, which bypasses cryptographic algorithms like open-key cryptographic techniques for preserving the confidentiality defense, lacks absolute certainty for the confidentiality defense because blockchain activities/transactions are quasi-anonymous, conveying that activities/transactions are designated by a ciphered non-real address rather than the true addresses of subscribers [18]. Precisely, the amount of confidentiality protection is modifiable depending upon the cryptographic ledger category: closed, federated, and open. Open blockchain is the established decentralization blockchain, whereas closed and federated blockchains bear a definite amount of centralized power, dispensing greater seclusion and information access governance than open blockchains [19].

The role of blockchain in existing literature on ID applying blockchain in SDN can be three-fold. First, blockchains facilitate cooperative intrusion identification in SDN by implementing intrusion identification using Smart Contracts (SCs) on the blockchain while also storing the required data for ID securely in the blockchain, such as in the framework in [20], where SCs are applied to diagnose potential misbehaviors by securely storing and verifying manifests. The second approach is off-chain ID in SDN, where blockchain is applied for trust management (securely storing data). As an example, in [21], blockchain is applied for secure trust management among the SDN controllers using digital certificates to manage them and protecting the integrity of the signatures using blockchain, preventing insider attacks. Thirdly, blockchain is applied for providing both authentication and secure data storage in the method of intrusion identification by an off-chain intrusion identification approach [3].

The review paper [22] discusses blockchain-centered cooperative anomaly identification systems in cloud systems. Similarly, the review paper [23] reviews blockchain-centered intrusion identification in the broad class of networking. Even though there are review papers for blockchain-centered network ID (review papers [22], [23] stated before), no critical assessment article exists discussing and analyzing intrusion identification by applying blockchain to SDN. Thus, we are the front-line reviewers on blockchain-centered intrusion identification in SDN, which will disseminate precious referring material for researchers to identify existing blockchain-centered solutions for intrusion identification in SDN, identify existing research shortfalls and evolving tendencies centered upon our analysis related to blockchain-centered parameters and SDN parameters, and also recognize advice to overcome hardships.

The tiered arrangement of this documentary analysis is graphically represented in Fig. 1.

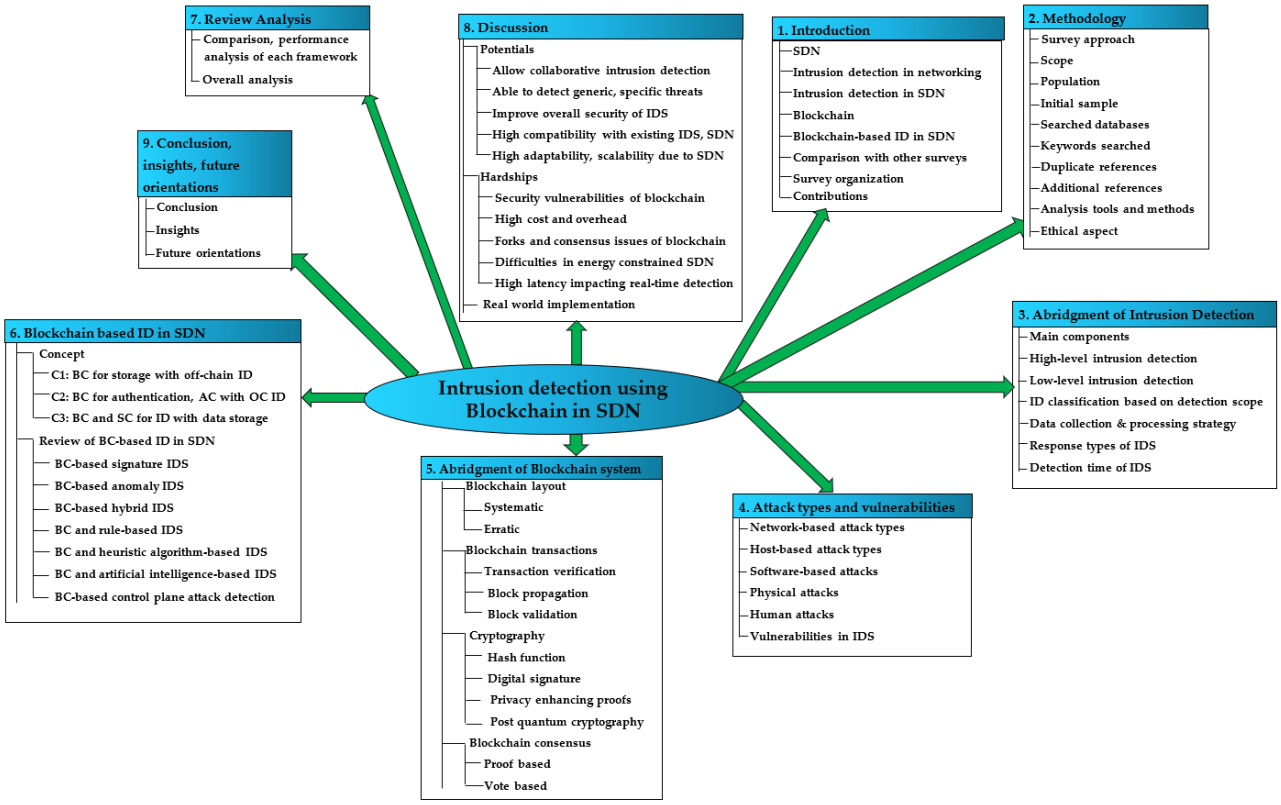



**Fig. 1.** Tiered arrangement of documentary analysis on ID by applying blockchain in SDN.

Contributions to extant literature:

- We organized and briefly explicated an abridgment to intrusion detection (Section 3).
- An abridgment of attack types in SDN and vulnerabilities in IDS is briefly explicated (Section 4).
- An abridgment of blockchain advancement is demonstrated (Section 5).
- Assess extant blockchain-centered intrusion identification in SDN (Section 6).
- Examine elaborately the assessed blockchain-centered ID frameworks in SDN (Section 7).
- The potentials and hardships of blockchain-centered intrusion identification in SDN are examined (Section 8).
- Insights and future orientations for applying blockchain-centered intrusion identification in SDN are demonstrated (Section 9).

## 2. Methodology

This examination assesses the up-to-date studies on blockchain-centered intrusion identification in SDN released to the public across the years, making use of an elaborate and over-time procedure [24]. Furthermore, it considers various aspects of ID, network attack types, and vulnerabilities of IDSs, the SDN, and the cryptographic ledger. As a result, all inventive scholarly outputs and digital web documents featured in published form on ID, network attacks, blockchain, SDN, and blockchain-centered intrusion identification in SDN fill the whole group as part of this analysis. However, the whole group of references is difficult to investigate in this analysis. As a result, making use of proper search inquiries and selection guidelines, we assembled 101 references from inventive scholarly outputs and digital web documents.

We inquired IEEE Xplore technical data storage, ScienceDirect science knowledge storage, ACM virtual library, Wiley virtual library, MDPI information discovery engine, Google Scholar learning material discovery engine. The search inquiries we habitually went for were "SDN" OR "Blockchain" OR "Intrusion detection" OR "Network attacks" OR "Blockchain-centered intrusion identification in SDN" OR "Blockchain-centered signature intrusion identification in SDN" OR "Blockchain-centered anomaly intrusion identification in SDN" OR "Blockchain-centered hybrid intrusion identification in SDN" OR "blockchain and rule centered intrusion identification in SDN" OR "blockchain and heuristic algorithm centered intrusion identification in SDN" OR "Blockchain with artificial intelligence centered intrusion identification in SDN" OR "Blockchain centered attack identification in SDN.

Plentiful considerations for sifting through the articles structured the selection guidelines. The first selection guideline mentions that the paper mandates English script, and the second selection guideline mentions that it ought to be vastly correlated to the search inquiry. Thirdly, with the intention of intensifying the solidness of the conducted examination, journal papers were focused on with urgency when juxtaposed with convention papers and time-advanced manuscripts. In contrast, we didn't promote research documents of a distinct literary press in the selection guidelines; on the flip side, we recognized all literary presses in the same way. The last selection guideline affirms that a distinct paper necessitates dissemination amidst the years, starting in 1985.

The preliminary sample was slashed to 97 paper sources following the spotting of 4 paper sources as clones. Furthermore, we credited descriptions and explanations concerning the wide-ranging areas extended in this examination using 43 papers. To juxtapose this examination with preceding examinations, we further appended 2 further examination articles to the cluster of texts, delivering the utter number of paper sources to 142.

To judge in force network ID approaches utilizing blockchain in SDN according to plentiful considerations, such as blockchain characteristics, ID characteristics, network properties, and operation, we made use of the tabulated information structure for the descriptive examination. Furthermore, we built graphic illustrations making use of Microsoft's spreadsheet tool to unprejudicedly inspect examination data associated with ID-centered, SDN-centered, and blockchain-centered considerations [25].

Ethics are immaterial owing to the fact that this examination is connected with networking systems.

## 3. An abridgment of intrusion detection

### 3.1 Main components of IDS

There exist 3 major components of an IDS: monitoring, analysis and detection, and response. An IDS is diagrammatically represented in Fig. 2.

#### 3.1.1 Monitoring

The monitoring component is responsible for local events and neighbor monitoring. Specifically, it will monitor traffic flows, security events, performance metrics, resource usage data, sensor data, etc. Hierarchical monitoring can be applied to improve the detection accuracy of a distributed system [26].

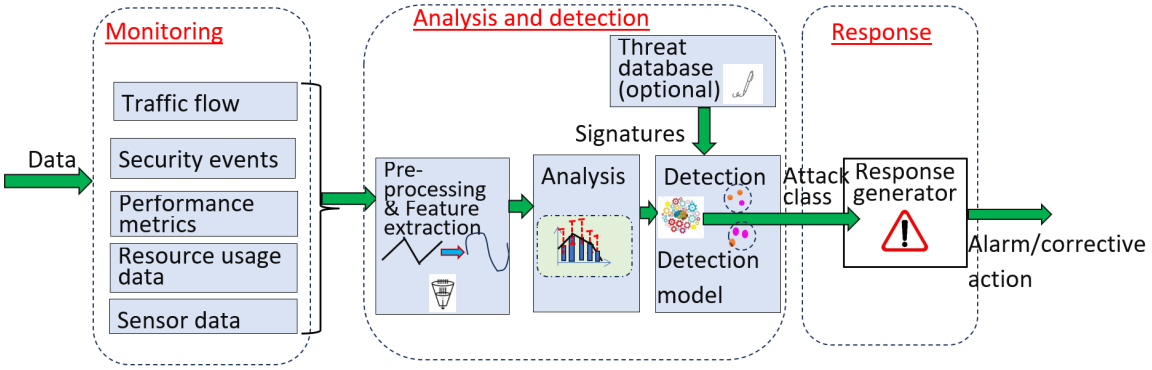



**Fig. 2.** The process of intrusion identification in an IDS.

#### 3.1.2 Analysis and detection

The analysis and detection module is responsible for analyzing the input data (network operations/activities) using an algorithm or an artificial intelligence approach to class the input as malevolent or not in the case of binary classification or as a malicious class in multi-class classification. In a distributed system, multiple agents will act as analysis and detection agents, where effective inter-agent communication techniques mitigating interference are required [27].

#### 3.1.3 Response

The response module generates a response in case intrusions are detected so as to take necessary actions by other systems or network administrators. Note that IDSs may generate an alarm, and this alarm can be applied for subsequent preventative actions by an intrusion mitigation system. Some IDS can respond with corrective action to directly mitigate the threat. Moreover, in IDS, the response can be different centered upon the class of network attack identified, where an alarm can be given for low-intense threats while corrective action can be taken for serious threats [28].

### 3.2 High level intrusion detection techniques

#### 3.2.1 Signature/Knowledge centered

A signature/knowledge-centered IDS monitors network traffic and juxtaposes it with a repository of signatures (attributes) of already-recognized threats. In case the input data has a high correlation with the signatures, the IDS will classify the input as malicious. As an example, in [29], signatures are derived from real-world scenarios in a controller area network of a vehicular network to implement a light-weight signature-centered IDS that can be applied to vehicles.

#### 3.2.2 Anomaly/Behavior centered

An anomaly/behavior-centered IDS maintains a record of the network' regular activities, events, connections, etc. through the passage of time. The IDS contrasts the real-time input data with these normal profiles to check whether there is any deviation from the regular conduct or not. If there is a high deviation from regular conduct, then the traffic/event will be classified as malicious. Anomaly detection can be realized using Machine Learning (ML) [30] with filter-centered feature selection and synthetic attacks generated for training using generative adversarial networks to detect anomalies related to different attack types [5].

#### 3.2.3 Hybrid signature and anomaly centered

Hybrid IDSs use a combination of signature- and behavior-centered IDSs. These are renowned for accurate intrusion identification, which has low false-positives due to the utilization of both signature detection and anomaly detection. The two detection modules are: signature detection will detect well-known attacks using signatures, while anomaly detection detects deviations from normal network behavior. As an example, in [31], a hybrid signature and anomaly centered ID applies a random forest categorizer for signature-centered detection and K-means clustering for anomaly detection.

### 3.3 Low level intrusion detection techniques

Note that the following ID approaches can exist in an anomaly detection or signature-centered IDS.

#### 3.3.1 Statistics centered

Statistics-centered IDS is typically applied in anomaly detection techniques. Statistics such as mean and standard deviation, probabilities, predefined thresholds, etc. are applied in attack detection in this approach. Deviations from the normal statistics are classified as threats. As an example, in [32], flow statistics are applied to generate histograms of network parameters as features for classifying network flows.

#### 3.3.2 Pattern centered

Pattern detection-centered IDS is typically applied in signature detection. They involve pattern-matching input data to already-known attack patterns. These are effective against known attacks. However, these systems struggle to detect new threats. In [6], a pattern-matching-centered IDS has been put forward using an improved pattern-matching algorithm in the analysis module of the IDS.

#### 3.3.3 Rule centered

Rule-centered detection uses predefined rules to detect attacks. As an example, they can use simple if-then-else conditional rules to develop the profile (behavior) of known attacks. These systems are effective against attacks, for which rules have been created. As an example, port scan detection rules can be fed into a security engine to diagnose ingenuous port scan threats in live fashion [33].

#### 3.3.4 State centered

State-centered IDSs monitor the condition of the network through the passage of time. This stratagem is good at identifying complex threats that involve multiple steps. The most common state-centered IDS approaches are state transition analysis and protocol analysis. As an example, in a process control network, network anomalies have been detected by applying high-pass filters and Euclidian displacement among the present conditions with the latest conditions that can adjust the severity of detection and adapt to network variations by changing the anomaly limit [34].

#### 3.3.5 Heuristic algorithm centered

Heuristic algorithms use a combination of predefined rules and behavioral analysis to detect intrusions. These systems are more effective than rule-centered IDS, as heuristic algorithms are capable of detecting evolving threats. In [35], a multi-variable heuristic algorithm has been applied for ID in a network by applying various flags and entropy values to shared data, where detection thresholds and default values for the algorithm have been decided experimentally.

#### 3.3.6 Artificial intelligence centered

Artificial intelligence-based ID can apply techniques, namely ML, fuzzy logic, etc., to learn from large datasets and identify complex patterns for detecting both known and unknown threats [36]. Fuzzy logic has been applied to detect local repair threats inside low-power lossy networks' routing protocols with an elevated positive prediction fraction [37]. Moreover, many researchers have applied ML to network ID. As an example, in [38], a dilated casual Neural Network (NN) is applied for binary classification of network intrusions using a public dataset to implement an IDS in a resource-constrained network environment.

### 3.4 Classification centered upon detection scope

#### 3.4.1 Host-centered

Host-centered IDS (HIDS) concentrates on surveillance tasks on single hosts (network endpoints such as servers and user

equipment). These systems analyze host-specific data types such as system logs, flow statistics, audit trails, etc. for threat detection. HIDS detects local attacks on a specific, single host. A host-centered IDS has been tested in a home automation system by tracing the user space and kernel space information of hosts to detect threats using ML techniques and raise alerts [39].

#### 3.4.2 Network-centered

Network-centered IDS (NIDS) have a network-level scope for intrusion identification that typically involves monitoring network traffic to detect intrusions. NIDS is not able to provide much status about each individual host like HIDS, as NIDS detects network-level attacks. The NetFlow metadata collection protocol has been put forward as a standard to collect feature sets for network ID because feature selection using NetFlow has resulted in better network ID performance than using raw datasets [40].

#### 3.4.3 Hybrid host and network centered

Hybrid ID is a more effective approach that utilizes both NIDS and HIDS in combination to provide a comprehensive view of threats. These systems can detect more complex attacks that involve both host exploitation and network corruption. HIDMN is a host- and network-centered IDS designed for mobile telecom networks using SIM-centered methods for detecting various threats, just like DoS, SIM cloning, etc. [41].

### 3.5 IDS data collection and processing strategy

#### 3.5.1 Collected data

Network ID collects different categories of data, just like traffic flows, system records, appliance utilization, and performance measurements. The data collection strategy can differ in the IDS as follows.

#### 3.5.2 Centralized

In centralized data collection and analysis, data is collected from a central location and analyzed. This approach is simple; however, it has the drawback of a single point of collapse [42]. Network-centered ID in centralized networks typically uses this data collection approach. In SDN, which has a logically centralized controller, network ID takes place in a centralized manner by collecting network data for the centralized controller to detect intrusions using a statistical approach [1].

#### 3.5.3 Distributed/Decentralized and collaborative - hybrid

In a distributed or decentralized collaborative approach to data collection and analysis, data are analyzed locally for ID before sharing their output with other nodes to collectively identify threats. Blockchains can apply a decentralized and collaborative data collection and analysis approach for collaborative ID. This approach implements a hybrid approach of network-centered and host-centered intrusion identification. As an instance, in [7], blockchain has been applied to improve distributed and collaborative ID by providing trust among the monitors, accountability, and consensus.

#### 3.5.4 Distributed and standalone

In distributed and standalone data collection and analysis, data is collected locally by nodes, intrusion is detected in each host, and the detection output is not collaborated with other nodes in the networks. Note that a decentralized and standalone data collection and analysis approach can be applied to host-centered intrusion identification. Therefore, blockchains can be applied for distributed and standalone host-centered intrusion identification as well. In [43], the authors have presented a blockchain-centered distributed IDS that can be applied for host-centered intrusion identification in the distributed cloud infrastructure.

#### 3.5.5 Hierarchical data collection

Hierarchical data collection and analysis involves a network divided into a hierarchy of IDSs with cluster heads. Each cluster head detects intrusions of the nodes under the control of the head, and cluster heads in the lower level will report the malicious activity to the cluster head in the upper level, ultimately cooperating with a central authority for global ID. As an instance, in [44], a multiple-tier hierarchical network IDS is applied to improve the overall ID accuracy by applying multiple hierarchical ML models and using a genetic algorithm to adjust the variables of ML algorithms in the first tier.

### 3.6 Response type of IDS

The response type of an IDS can take one of the following forms: passive or active.

#### 3.6.1 Passive

A passive response is an alarm in the form of detection output that can be applied by administrators or another threat mitigation system to mitigate the attack. However, passive responses expose the network devices to attacks as the alarm events are not necessarily blocked in this type of response [45].

#### 3.6.2 Active

The active response of an IDS can be of two types as corrective and proactive.

#### Corrective

The corrective response of an IDS is when a threat occurrence in the network has been confirmed. Corrective actions will help reduce further damage to the network. These actions include blocking and quarantine, isolation of devices, initiating backup, etc. An intrusion identification and response system for mobile adhoc networks detects attacks using audit data and responds to the intruder using a corrective action to protect the network [46].

#### Proactive

Proactive threat mitigation involves preventing threats before they can compromise the network through early detection. Actions such as rate limiting, blocking source internet protocols, etc. represent proactive actions. In a cyber-physical IDS, IDS works by analyzing virtual and physical information pipelines simultaneously and providing a proactive reaction upon detection of a threat such as packet replay attacks [47].

### 3.7 Detection time of IDS

#### 3.7.1 Online

Online detection involves monitoring network data flows in a live fashion when intrusions occur in the network, and the IDS responds with the classification output in real-time [48]. Online ID works in continuous mode, where the network is monitored continuously in the time domain. In [4], real-time network traffic flows are monitored by a rule-centered inspector, and untriggered traffic flows from the inspector are

analyzed by an artificial intelligence module (XGBoost) to detect attacks.

### 3.7.2 Offline

Offline detection involves analyzing historical data about the network, not in real-time. It detects intrusions that may have occurred in the past and gone unnoticed [48]. Offline IDSs work in periodic mode, where detection and analysis are performed at specific time intervals, and in between those time frames, data will be collected. As an example, in [49], an offline IDS using an extended radial centered policy deep learning network within an offline reinforcement learning model trained using labeled datasets to learn parameters for the NN.

Table 1 represents an abridgment of the extant literature on ID.

**Table 1.** An abridgment of extant literature on ID

| Intrusion detection feature | Specific feature | Tactic | Performance |
|---|---|---|---|
| Main components | Monitoring | Hierarchical monitoring in distributed systems [26] | Improved detection accuracy |
| | Analysis & detection | Multi-agent analysis, detection with intercommunication [27] | Scalable, no primary point of breakdown |
| | Response | Alarm and corrective action centered upon threat seriousness [28] | No performance evaluation |
| High-level ID techniques | Signature-centered | ID centered upon signatures derived from vehicular network [29] | Improved detection ratio for content related anomalies |
| | Anomaly-centered | Machine learning with filter-centered feature selection [5] | Accuracy of 91% with adversarial training |
| | Hybrid | Random forest classifier (signature)+K-means (anomaly) [31] | Good detection rate, precision, recall, etc. |
| Low-level ID techniques | Statistics-centered | Flow statistics to generate histograms to classify flows [32] | 99% detection rate, 2% misclassification rate |
| | Pattern-centered | Improved pattern matching algorithm [6] | High detection speed |
| | Rule-centered | Security engine with port scan detection rules [33] | Low false positive alarm rate |
| | State-centered | High-pass filters, Euclidian distance among states [34] | Highly effective in detecting anomalies |
| | Heuristic algorithm | Multi-variable heuristic algorithm using flags, entropy [35] | Perform better with low number of iterations |
| | Artificial intelligence | Fuzzy logic to detect local repair attack [37] | High TPR, low FPR |
| | | Dilated casual NN for binary classification [38] | High precision, 99.7% attack detection rate |
| Detection scope | Host-centered | ML to trace user, Kernal space information [39] | High detection rate with low overhead |
| | Network-centered | NetFlow metadata collection protocol for ID [40] | Consistent high classification performance |
| | Hybrid (Host + Network) | SIM-centered methods for detecting attacks (HIDMN) [41] | Can detect attacks of 3 classes |
| Data collection & processing strategy | Centralized | Controller detects intrusions using statistics [1] | Effective statistical-centered ID |
| | Distributed & collaborative | Blockchain to provide trust among the monitors [7] | No performance analysis presented |
| | Distributed and standalone | Host-centered IDS using blockchain [43] | Scalable, as the computing power, performance was consistent |
| | Hierarchical | Multiple hierarchical ML models with a genetic algorithm [44] | Considerable improvement in error generalization metrics |
| Response type | Passive | Passive alarm upon threat detection [45] | Optimum configuration in active response is light |
| | Corrective | ID using audit data, respond with CA [46] | Energy consumption & queue length drop with corrective action |
| | Proactive | Analyze data streams and provide proactive response [47] | Successfully detect and respond to packet replay attack |
| Detection time | Online | Rule-centered inspector & XGBoost [4] | High accuracy, low packet inspection time |
| | Offline | Extended radial basis NN in RL [49] | Good candidates for designing classifiers |

## 4. An abridgment of attack types in SDN and vulnerabilities of IDS

### 4.1 Network-centered attack types

#### 4.1.1 Scanning

A scanning attack involves probing a target network for potential vulnerabilities. These systems typically analyze the responses received for the probe packets to identify vulnerabilities. Examples are port scanners, network scanners, etc. In [9], an algorithm implementing a mathematical model to detect port scans using anomaly detection to identify the source of the attacker has been put forward.

#### 4.1.2 Denial of service (DoS)

A DoS attack attempts to completely shut down or degrade the performance of a service and deny access to authorized users by attacking the service with excessive traffic and overloading the target with massive amounts of demand. DoS, or DDoS (Distributed DoS), where multiple systems from various locations launch the DoS attack, forms a component of the preeminent habitual threats found in SDN, where the data, control, and application planes are attacked for service

denial by flooding [50]. Fig. 3 graphically represents the DoS attack and spoofing attacks that are preeminently common in SDN.

As represented in Fig. 3, several attackers from the data plane can launch the DDoS attack to flood the controllers, applications, and other data plane elements, as evident from the attack flow. In [51], a fine-grained DoS attack detection scheme using looking-back-centered ML, identifies the specific attack type (distributed/centralized) and packet type of the attack, enabling the application of countermeasures based on the packet type.

### 4.1.3 Penetration

An attacker obtains unauthorized ingress into the network in the penetration attack to identify vulnerabilities in the network. This is also known as ethical hacking, where the goal is to detect vulnerabilities so as to get root access by exploiting the vulnerabilities later. Penetration testing for an end-to-end system consisting of end devices, communication, control units, etc. by gathering various information from the network has been applied to provide security recommendations to the penetrated system [52].

### 4.1.4 Spoofed routing

The spoofed routing attack refers to an attacker gaining control over the routing protocols of the network. Thus, the attacker is capable of manipulating routing for various tasks such as loop creation, repelling traffic, shortening or extending the routes, rerouting traffic through a compromised network for interception and manipulation of data, etc. A computationally efficient, real-time routing attack detection system using mark maps has a two-step adaptation process where, in the first stage, patterns in routing control traffic are identified using rules extracted from the mark map and prioritized, whereas in the second stage, the detection model is updated with new patterns [53].

### 4.1.5 Selective forwarding

In this attack, malicious nodes in the network either drop packets or forward them to different nodes that do not adhere to the flow rules or packet forwarding instructions. In SDN, this involves bypassing flow rules installed by the controller [54]. In [55], an atypical appliance identification technique using an appliance conduct measuring framework and trust amount assessment scheme is applied to detect the selective forwarding attack coupled with a network recovery mechanism in software-defined wireless sensor networks.

### 4.1.6 Worm Hole Attack (WHA)

WHA involves numerous attackers creating a high-speed communication channel in the network, typically over an extended displacement, and forwarding traffic through this channel (worm hole) without being subjected to normal network protocols. In [56], wormhole attacks and attacker nodes are detected by an IDS for the Internet of Things (IoT) by using location data of a node among its neighbors coupled with acquired signal intensity measurement values and the number of hops.

### 4.1.7 Sybil Attack (SA)

In a SA, the malevolent appliances present diverse identifying information to the network that can cause the routing to occur incorrectly due to flow tables saturated with incorrect flow rules. A sybil attack has been detected in a software-defined VANET network that detects Sybil appliances by analyzing the received signal strength of neighboring nodes with the cooperation of two high energy nodes [57].

### 4.1.8 Black-hole attack

A malevolent appliance drops all the network data flows that are transmitted to be forwarded through it, causing network traffic to disappear (end) at the malicious node in a black-hole threat. A secure routing protocol is presented in [58] that detects threats by applying a cryptographic approach to traditional routing, where changes in the encrypted, received packets are applied to detect the black hole attack.

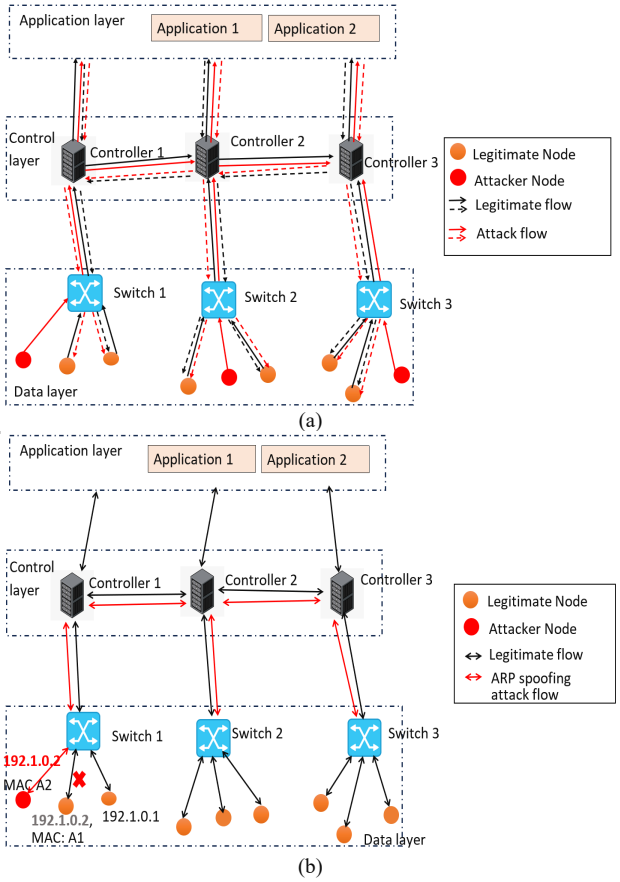



**Fig. 3.** Typical attacks in SDN (a) DDoS. (b) ARP Spoofing.

### 4.1.9 Hello flooding

Hello messages that are applied in neighbor discovery in wireless networks are flooded in this attack to unnecessarily exhaust neighboring nodes and consume network energy. In [59], a secure protocol is applied to reduce hello flooding attacks coupled with malevolent appliances and the appliances struck by the attack to make a safe topology discovery environment for SDN.

### 4.1.10 Spoofing

In acknowledgement spoofing, an attacker spoofs the acknowledgement packet sent from a receiver back to the sending appliance to persuade the sending appliance that a dead node is alive or data has been successfully transmitted, when it is actually not. ARP spoofing, on the other hand, sends fake ARP communications to couple an attacker's MAC address with the IP address of an authorized user to redirect traffic through the attacker [60]. This attack is represented in Fig. 3(b), where the attacker assigns its MAC address A2 to the IP address 192.1.0.2 of a legitimate user by ARP address update to instruct all controllers to update the flow rule

mapping of switches accordingly. In [61], a centralized SDN controller has been put to use to mitigate ARP spoofing and prevent DoS attacks.

### 4.2 Host-centered Attack types

#### 4.2.1 Worm

A self-replicating malware program that can spread across multiple hosts without requiring user intervention is identified as a worm. In high-speed software-defined networks, the honeynet scheme has been applied for host-centered worm detection by host behavior classification, traffic monitoring, and pattern recognition for anomaly detection [62].

#### 4.2.2 Virus

A virus is malware attached to a legitimate file, and upon execution of the file, the virus begins to infect other files and programs. Viruses can corrupt data, modify data, or delete data. With the aim of detecting unknown viruses, a malware detection scheme at the SDN controller by traffic analysis has been put forward in [63] by enforcing security rules.

#### 4.2.3 Adware

Adware is software that shows unnecessary advertisements to users, redirects traffic to unnecessary networks, and consumes hardware resources. An SDN-driven adware detection system that achieves its purpose through network traffic flow features has proven to have high accuracy and generalizability [64].

#### 4.2.4 Spyware

Spyware secretly gathers the user's information with his consent by using various approaches, namely keystroke monitoring, tracking user history, capturing sensitive information, and transmitting it to malicious users. OpenSec is a SDN scheme that leverages security policies to generate network-wide OpenFlow messages for spyware and spam detection by matching up appliance data with network data flows related to the disloyal program, where classed spyware provides the signatures characterizing malicious behavior [65].

#### 4.2.5 Trojans

A trojan is a malevolent sequence of operations that is deceived to the user as a lawful program that tricks the user to execute it, allowing it to perform malicious activity such as stealing data, host manipulation, unauthorized access, etc. In a software-defined network environment, trojan horse detection has been feasible using mandatory network security policies [66].

#### 4.2.6 Ransomware

Ransomware is malicious software that keeps compromised hosts' files encrypted until the host pays a ransom to decrypt them. Ransomware causes financial losses to individuals and organizations. SDN has been applied for ransomware detection by inspecting the characteristics of ransomware communication using HTTP message sequences [67].

### 4.3 Software-centered attacks

#### 4.3.1 Code/Packet injection

Code/packet injection is an attack where an attacker injects malicious code into a system to execute malicious actions. Typically, code injection targets web services that process user inputs, just like SQL insertion and script insertion across sites to steal cookies at the application layer, while packet injection involves injecting crafted packets at the network layer. In [68], a software-defined network IDS detects new obscured and understandable packet insertion threats known as PIEDefender.

#### 4.3.2 Fingerprinting

Fingerprinting identifies the type and version of software running on a device such that attackers can detect vulnerabilities associated with particular software versions in order to launch attacks for intrusion. Research in [69] proves that fingerprinting poses a huge threat for SDN, where attackers can extract control related information from packets, such as matching fields of SDN flow rules, to infer information about the controller and security policies. Thus, it uses lightweight counter-measures to prevent fingerprinting by hiding sensitive control information from packets.

#### 4.3.3 Mis-configuration

Mis-configuration is when certain devices or applications are configured with incorrect settings or leave default settings without carefully configuring them, making the device or application vulnerable to attacks. In [70], a self-healing system for SDN networks to recover from misconfiguration attacks using the Markov decision process to prevent negative impacts on network-level data flows has been put forward.

#### 4.3.4 Fake certificates

Fake certificates involve attackers using fake or counterfeit certificates to act like legitimate services, misleading network users into believing that they are interacting with a legitimate party when they are actually not. Certrust is an SDN network-centered scheme that operates on trust that avoids fake certificates by collecting certificate statistics and DTLShps to verify certificates with the aid of a controller by using Bayesian trust [71].

### 4.4 Physical attacks

Physical attacks attempt to tamper with hardware or its configuration.

#### 4.4.1 Backdoor

A backdoor attack is a malicious activity where unauthorized access is gained by exploiting hidden vulnerabilities to create secret entry points, allowing attackers to bypass the normal authentication process. In [72], machine learning is applied to detect backdoor attacks in a botnet detection framework for SDN-centered networks.

### 4.5 Human attacks

#### 4.5.1 Masquerade

A masquerade attack is a human attack where an attacker mimics a lawful user either by applying legitimate users' credentials or manipulating data packets to look as if they originated from a legitimate user that can provide unauthorized access to systems and data stealing. An IDS to detect masquerade attacks on the host tracking service of the SDN controller using authentication countermeasures and detection methods has been put forward in [73].

#### 4.5.2 Phishing

In phishing attacks, the users are tricked into disclosing their identity and private data, just like usernames and passphrases, using fraudulent messages or websites that mimic legitimate ones. Phishlimiter is a phishing attack detection and mitigation system that uses deep packet inspection and SDN with different forwarding modes by applying an artificial NN to diagnose phishing tasks [74].

#### 4.5.3 Repudiation
A repudiation threat is when an end-user disagrees that he has actually done a particular action or transaction when he has really performed it. This can occur when proper auditing and logging functions do not exist. A strong non-repudiation scheme for SDN using strong trust management with the aid of logical reasoning among the SDN controller and applications, robust authentication and authorization, and network policies has been put forward in [75].

#### 4.5.4 Hijacking
Network hijacking involves gaining unauthorized access to and control over an ongoing legitimate communication among two parties to gain access to sensitive information. In [76], broader gateway protocol hijacking is detected by the SDX validation technique of new routes at the controller with access point embedding in an unsupervised approach.

### 4.6 Vulnerabilities in IDS
#### 4.6.1Buffer overflow
A program error that can pave the way for exceptions in memory access and programs being terminated illegally is recognized as a buffer overflow. It happens once a program writes additional data into memory exceeding the amount it can tackle with. It can act as a vulnerability for attackers to exploit by using input data to trigger a buffer overflow. In [77], to overcome the buffer overflow vulnerability existing in IDSs that apply the Message Queuing Telemetry Transport (MQTT) protocol, an MQTT parsing engine to check against vulnerabilities has been integrated with the IDS.

#### 4.6.2 Input validation error
An input validation error occurs when the systems do not verify the validity of the supplied data before proceeding with it. Thus, IDS should have stratagems to check the validity of the supplied data to prevent attackers from getting unauthorized access [78].

#### 4.6.3 Boundary condition error
A boundary condition error occurs when the input results in crossing some security boundary, such as running out of memory or network bandwidth [79]. IDS should have a mechanism to act in boundary conditions without arbitrary behavior [80].

#### 4.6.4 Access control vulnerability
Access control vulnerability is providing illegitimate access between two network domains due to faulty or weak implementation of access control approaches in the IDS [81].

Table 2 represents an abridgment of the extant literature on attack types in SDN.

## 5. An abridgment of blockchain system
A succession of attached blocks or activities/transactions embodies the cryptographic ledger named blockchain.

### 5.1 Layout
Every individual block as part of a systematic blockchain, which embodies a header portion and payload portion, is attached to its preceding block (aside from the inaugural block), resorting to the preceding block's cryptographic hash, and the activities/transactions as part of the payload portion are sorted into a Merkle tree model [14]. The structure of a systematic blockchain and the model of the Merkle tree are represented by Fig. 4.

An erratic blockchain embodies an assemblage of attached activities/transactions, where one activity/transaction can potentially affirm numerous alternative activities/transactions that formed before its existence. These activities/transactions are short on header portions and payload portions; as such, Merkle trees are non-existent [15].

### 5.2 Transactions/Activities
A customer can begin a blockchain transaction/activity, which is next broadcasted to other customers as part of the network and ciphered, resorting to the non-shared key. A consensus approach will begin once each customer resorts to the exposed key to verify the transaction/activity. Consensus validators regularly connect with consensus/collective decision by appending the transaction/activity as part of a block, which is next broadcasted to the cryptographic ledger network and gets involved by each customer in the cryptographic ledger network afterward block verification [82].

### 5.3 Cryptographic techniques
To preserve the purity of activities/transactions in blockchain, hash computation is resorted to grant invariable extent cryptographic hashes with reduced overlapping [16].

Resorting to a cyber signature, an open-key cryptographic technique having a couple of asymmetric keys is resorted to verify activities/transactions. With the aim of boosting the intimacy of digital assets, it's similarly possible to resort to secure blockchain activities/transactions [83].

Non-interactive proofs are resorted to verify activities'/transactions' accuracy, keeping hidden the identifying data of activities/transactions, boosting intimacy, and thwarting the broadcasting of sensitive facts [84].

Cutting-edge cryptography resorts to impactful cryptographic procedures that preserve against intrusions from quantum calculators, like SIKE, improved Curve448, and others [17].

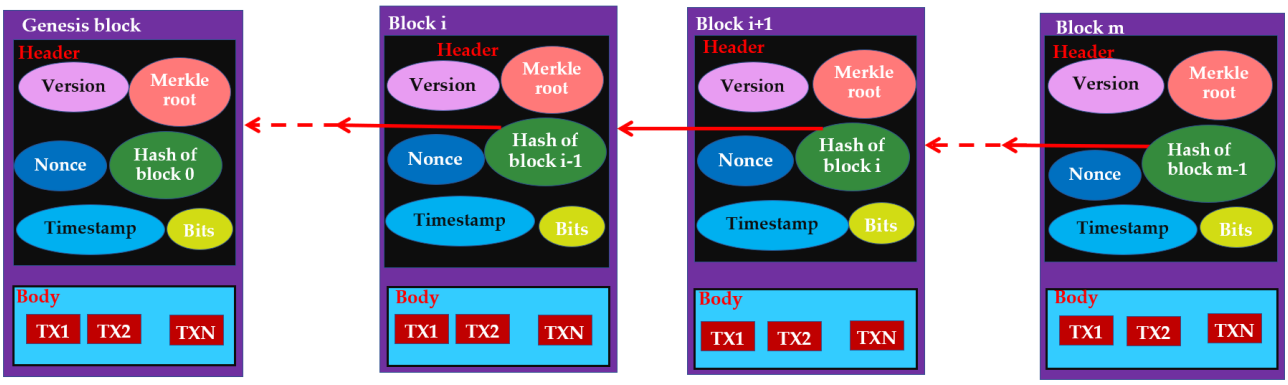
### 5.4 Consensus/Collective decision
Blockchain consensus resorts to a widespread collective decision to craft and verify brand-new blocks, preserving the purity of the cryptographic ledger advancement.

In a vote-centered collective decision, knowledge is handed over and received between the customers as they join forces to verify blocks. The hugely preferred vote-centered collective decision procedure resorts to byzantine fault-tolerance collective decision, while a captain appends activities/transactions as part of a block, broadcasts it, and customers rebroadcast it to verify the block obtained by employing the parent is cloned. If each customer got cloned versions of a brand-new block, outweighing a 66% share of the network's customers, the block may turn out to be appended to the cryptographic ledger [18].

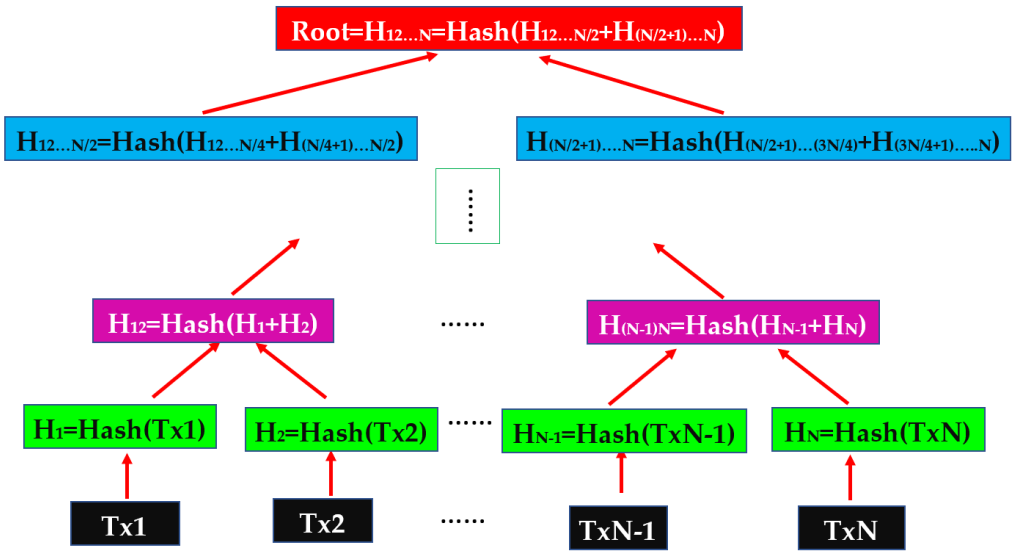
Proof-centered collective decision requires customers to grant compelling verification for what reason they need to be gratified for appending a brand-new block to the cryptographic ledger. The most esteemed proof-centered collective decision procedure is titled proof-of-work, calling for a customer to undertake assignments by dealing with a tough quandary with the aim of preserving its loyalty [82]. Nevertheless, this technique is power-hungry and inefficient.

**Table 2.** An abridgment of extant literature on attack types in SDN.

| Attack variety | Specific variety | Tactic | Performance |
|---|---|---|---|
| Network-centered attacks | Scanning | A mathematical model to detect port scans [9] | Able to identify IP address of the attacker |
| | Denial of service | Looking-back centered ML [51] | 99.8% accuracy |
| | Penetration | Penetration testing using network state information [52] | Provide recommendations for security |
| | Spoofed routing | Mark maps with a 2-step adaptation process [53] | Low computational overhead with slight accuracy decrement |
| | Selective forwarding | Node behavior measurement, trust value assessment [55] | Reduce network recovery delay by 72%, low packet dropping |
| | Worm hole attack | Use location, RSS, hop count, neighbor discovery for detection [56] | Energy efficient, high TPR, low FPR |
| | Sybil attack | Using RSSI of software-defined VANET network [57] | Improves network lifetime |
| | Black hole attack | Detects changes in encrypted received packets [58] | 95%-PDR, 87% high throughput, 98% detection rate |
| | Hello flooding | A secure protocol to reduce attacks, malicious nodes [59] | Successfully mitigate hello flooding attacks |
| | ARP spoofing | SDN controller to mitigate ARP spoofing [61] | High detection rate, low false alarms |
| Host-centered attack types | Worm | Host behavior classification by traffic monitoring [62] | Efficient and robust framework |
| | Virus | A malware detection scheme with traffic analysis [63] | Controller can find infection sources |
| | Adware | SDN-driven adware detection in VANET [64] | High accuracy and generalizability |
| | Spyware | Generate network-wide policy messages for detecting spyware [65] | 95% attack detection capability |
| | Trojans | Security policies implemented by SDN controller to detect trojan horse [66] | Good performance in detecting security attacks |
| | Ransomware | Inspecting features of ransomware using HTTP [67] | Feasible and efficient ransomware detection |
| Software-centered attacks | Packet injection | Floodlight controller detects packet injection attacks [68] | IDS can detect 97.8% packet injection attacks |
| | Fingerprinting | Hiding sensitive control information from packets [69] | Can mitigate SDN control information leakage |
| | Mis-configuration | Self-healing from misconfiguration to prevent negative impact [70] | Accurate results in performance and reliability |
| | Fake certificates | Certificate verification using statistics to avoid fake certificates [71] | Effectively mitigates crossfire attacks |
| Physical attacks | Backdoor | Machine learning [72] | Overall, 97% detection rate |
| Human attacks | Masquerade | Host tracking service masquerade attack countermeasures [73] | Feasible solution |
| | Phishing | Deep packet inspection, ANN, SDN [74] | Effective and efficient phishing detection |
| | Repudiation | Trust, authentication, authorization [75] | Strong non-repudiation and privacy preservation |
| | Hijacking | Inspect routing information by validation app [76] | Obtains trusted routes by detecting and stopping hijacking |




(a)




(b)

**Fig. 4.** Systematic blockchain (a) Block structure. (b) Model of Merkle tree.

## 6. Blockchain-centered ID in SDN

### 6.1 Schema

Rooted in this overview, the blockchain-centered ID in SDN schema can be grouped into the below 3 groups.

- C1 -- Applying blockchain for secure storage of data required for off-chain ID in SDN.
- C2 -- Applying blockchain and/or SCs for authentication, access control, attack mitigation, and/or secure data sharing while detecting threats of SDN off-chain.
- C3 -- Applying blockchain, SCs, and/or consensus to implement ID in SDN on-chain while also storing the data required in the blockchain with or without authentication.

The schema of blockchain-centered ID in SDN is graphically represented in Fig. 5.

### 6.2 Review of existing work on blockchain-centered ID in SDN

#### 6.2.1 Blockchain centered signature IDS

In collaborative ID, so as to secure the trust of the signatures and alarms exchanged among the ID nodes, blockchain has been applied, where signatures received from the software-defined controller are securely shared, known as Snort-centered collaborative ID [10]. Similarly, so as to provide trust management for SDN controllers while protecting the defense data to resist insider attacks, permissioned blockchain-driven collaborative ID is proposed for registering the controllers, using digital certificates to manage them, and protecting the integrity of the signatures to safely transfer them to other controllers [21]. For SDN-centered cyber-physical systems, blockchain has been applied for immutable data sharing in a decentralized manner, allowing trusted challenge-centered ID resistant to both insider and outsider attacks [85].

#### 6.2.2 Blockchain centered anomaly IDS

In a cloud-edge collaborative SDN, attack detection realized at the cloud tier by detecting doubtful network traffic using anomaly detection to reduce the attacks at the edge tier by dynamic traffic flow control using the SDN controller and blockchain is utilized for securing data confidentiality and for user authentication [3]. Trust management is achieved using blockchain technology, allowing trusted sharing of data without having a centralized trusted authority in SDN for challenge-centered collaborative ID, where the SDN controller can decide choices centered upon the preserved details available in the chain and the ID outcome, successfully reducing adversarial attacks [86]. Switches in a software-defined industrial network are registered, substantiated by applying non-interactive proofs, and approved by applying consensus, centered upon voting in blockchain, while deep Boltzmann machine-driven anomaly-centered flow analysis at the controller detects anomalous requests from the switches [87]. BMC-SDN is a blockchain-centered framework for multi-controller distributed SDNs that has master and redundant controllers. In BMC-SDN, the master controller creates network flow update blocks that are validated by other controllers, coupled with a combined-fading reputation mechanism to rate the controllers, allowing the detection of malicious controllers by detecting anomalies [11]. In an SDN-IoT mobile edge and fog computing network territory, the Ethereum blockchain has been applied to overcome failure issues and share model parameters securely, while deep learning is applied for distributed cyber-attack detection such as DoS and flooding attacks using anomaly detection so as to reduce attacks at the edge layer [88]. For within controller domains and between controller domains, an entropy-based DDoS attack detection system has been feasible by deploying a Hyperledger fabric blockchain, where it forms a blacklist of victims preventing the necessity to block victims' ports [134].

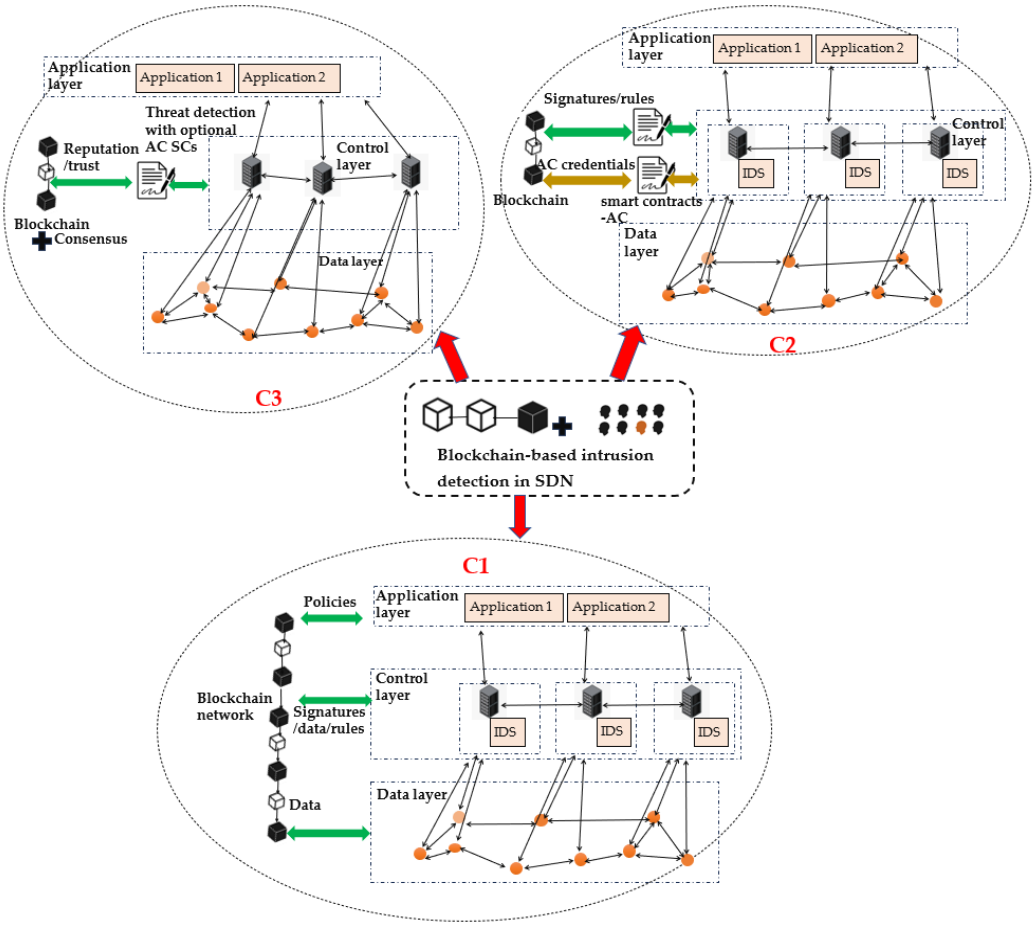



**Fig. 5.** The schema of blockchain-centered ID in SDN.

### 6.2.3 Blockchain-centered hybrid IDS

BlockCSDN is a blockchain framework for secure sharing of data for network ID using either a rule-centered or anomaly-centered approach in SDN, successfully creating a secure database of alarms, rules, and messages by involving applications and controllers for consensus, while maintaining the data integrity for collaborative ID [89]. BSDNFilter is a blockchain-centered stratagem for SDN to filter out malicious traffic using traffic fusion centered upon the output of an IDS using signature or anomaly detection for detecting intrusions to identify a set of malicious nodes and blacklist them to aid in the filtration process so as to reduce malicious traffic, and it has been effective against flooding attacks [90]. For an IoT-centered SDN, the network has been partitioned into domains, where the controllers detect possible attacks, while blockchain is applied for secure and distributed data transmission, providing a distributed and scalable security framework [91]. Permissioned blockchain is presented as a secure service for SDN to mitigate the effects of security attacks just like DDoS, Man in the Middle (MIM) attacks, eavesdropping, compromised data plane elements, etc., known as BlockSDN [92]. For software-defined optical networks, a distributed control framework known as Blockctrl applies blockchain to achieve control with reduced faults by detecting security attacks with low resource utilization [93]. A blockchain-centered IDS that applies blockchain for trusted exchange of alarms, rules, messages, etc. with consensus to update blockchain transactions and detect intrusions, either using a hybrid rule- or anomaly-centered approach, further places controllers by using an optimization approach [94]. BCSDN-IoT is a blockchain-centered distributed secure IoT network built using the SDN paradigm, which prevents threats by employing an IDS that applies a hybrid approach of signature and anomaly-centered threat identification to detect threats such as ARP spoofing, DDoS, etc., where access control and data protection are ensured by the blockchain [95].

### 6.2.4 Blockchain and rule centered IDS

Smart contracts in a private blockchain have been applied for collaborative DDoS attack identification and alleviation in SDN using a rule-centered approach, where the rules are distributed among the hosts using the blockchain, and SDN enforces security policies dynamically [96]. In software-defined industrial IoT edge networks, manufacturer user description manifests are securely stored and verified using blockchain to indicate access and network functionality to devices, where the manifests are verified using security by contract-centered SCs so as to diagnose potential device misbehavior resulting from cyber-attacks [20]. Moreover, SCs have been applied to prevent unauthorized access and DoS attacks by implementing SDN rules inside the SCs to detect and prevent threats and malicious activities to provide security among the distributed SDN controllers [97]. Another framework known as IOTASDN has been put forward to combat against DoS attacks using a heuristic approach with the aid of the IOTA tangle for access control and DoS detection using dedicated smart contracts [135].

### 6.2.5 Blockchain and heuristic algorithm centered IDS

BPP is a blockchain-centered packet parser that considers the security qualities of blockchain and assists in the processing of data by applying P4 language, where an algorithm that applies a mathematical formalism containing a multiple-

variable association technique is applied for attack identification, applying packet data transfers [98]. In a blockchain-centered IoT network, SDN has been applied for Network Function Virtualization (NFV) to implement an ID function by jointly applying proof-of-authority collective decision to verify transactions and detect suspicious nodes and SCs to get rid of induction attacks by blacklisting malicious nodes and deleting them from the network [99]. Similarly, another research applies a blockchain-centered secure framework to implement software-defined NFV for fortifying the security of IoT operations using a virtual security application, where a novel blockchain consensus algorithm is proposed to diagnose and alleviate malicious network traffic [100]. TrustBlock is a double-layer blockchain applied in SDN that is applied to achieve identity authentication and to calculate trust value centered upon forwarding status. In TrustBlock, a consensus algorithm is applied to prevent colluding attacks and filter malicious recommendations, while an entropy-centered historical trust weight is applied to get rid of periodic attacks [101]. FBA-SDN has a federated byzantine agreement system that applies byzantine fault tolerance consensus for collaborative analysis of alert data to reach consensus on intrusions in a distributed manner and has been effective in multi-class and binary intrusion classifications [102]. For genetic algorithm-centered routing in a software-defined IoT network, a hello and acknowledgement packet-centered algorithm is applied to detect malicious and dead nodes to be added to the malevolent appliance list preserved in the blockchain to be applied in subsequent routing path correction [103].

Cochain-SC is a DDoS alleviation scheme in the inter- and intra-domains of SDN that measures the randomness of the data using entropy and a Bayes-centered scheme to classify flows inside domains, while using Ethereum SCs for collaborative DDoS attack detection in the inter-domains so as to mitigate attacks in both the inter- and intra-domains [104].

### 6.2.6 Blockchain and artificial intelligence centered IDS

MiTFed is a zero-day attack and adversarial attack-resistant multiple SDN domain attack detection and mitigation framework that uses federated learning for collaborative privacy-preserving global model training by aggregating local models that apply the Ethereum blockchain with SCs for trustworthy collaborations [105]. Federated learning-centered random forest ML is applied after Fourier analysis, statistical, and entropy feature extractions of controller area network traffic in SDN for detecting multi-class attacks in a vehicular network in which the hash digests of the ML models are stored in a blockchain so as to get rid of model poisoning attacks and the sole nexus of catastrophe [106]. In an SDN-centered cloud that uses NFV, packet and flow features are applied to classify attacks using recurrent NNs, self-organizing maps, deep learning, and support vector machines in different SDN layers, coupled with robust authentication and blockchain to store the hashed flow rules in switches [107]. For the SDN-centered industrial IoT network, a security framework consisting of K nearest neighbor and random sub-space learning for ID to protect from forged commands for industrial control processes, coupled with an integrity checking module using blockchain to prevent misrouting attacks, has been put forward [108]. ShChain_3D-ResNet applies a sharded blockchain to enable smart and trustworthy interactions among the parties in SDN to simultaneously use multiple-user resources, while residual networks are applied to learn spatial and temporal patterns for classifying DDoS attacks [109]. For SDN in IoTs, an efficient forensic architecture that applies blockchain-centered distributed controllers for validating users using linear homomorphic signatures, while every controller is equipped with multi-fuzzy NN to classify packets as malicious or not centered upon the packets' attributes, has been employed [110]. Bloc-sec is a blockchain-centered security stratagem for SDN that has robust authentication using Blake 256, optimization for NFV, blockchain for storing hashed flow rules required to optimization, and spiking double fuzzy NN-centered ID that is executed at the controller by analyzing packet features [111]. Similarly, in another intelligent SDN, a fuzzy NN is applied to identify packets having a potential malevolent payload by analyzing IP packet header fields and TCP segments and validating network nodes using the blockchain implemented access control [112]. BrainChain applies a permissioned blockchain for secure applications in SDN, where blockchain nodes are protected from DDoS attacks by collecting flow statistics, extracting entropy features from them, detecting DDoS attacks using a Bayes network, and finally mitigating the illegitimate flows [113]. Blockchain has been applied for decentralized attack detection at the fog layer in a software-defined IoT networking territory in a smart city scenario to store the attack detection models, where deep learning is applied to detect attacks in the fog tier and alleviated in the edge tier, known as BlockSecIoTNet [114]. Blockchain has been applied for secure data sharing by registering and verifying vehicular nodes using proof-of-authentication consensus, while an autoencoder-equipped LSTM deep NN is equipped to detect illegitimate transactions in the ID process in software-defined unmanned aerial vehicular networks [115]. Blockchain has been applied to ensure security through decentralized data sharing and trust management in SDN-IoT networks that have distributed multiple controllers, while artificial NNs have been applied to detect DDoS attacks and have resulted in high classification accuracy [116]. SliceBlock is an authentication handover and network slicing in software-defined 6G networks using generative adversarial networks for network slicing and erratic blockchain with proof-of-space consensus for secure transactions, while a hybrid neural decision tree is used for intrusion packet classification and a heap-centered optimizer for packet migration [12]. Blockchain is applied for secure transmission of data using a clique proof-of-authority consensus approach, while deep learning, specifically an LSTM-stacked autoencoder with gated recurrent units, is applied at the controller for flow analysis and ID (anomalous switch request) in a software-defined IIoT network [117]. In [118], a capsule NN is applied to categorize packets as typical or malevolent at the edge server, while an erratic blockchain is applied at the control tier to keep the hash digested credentials of end-users and hash digested forwarding rules for authentication and forwarding rule verification, respectively, in software-defined 5G networks. BSDN-HMTD is a deep learning-driven framework that deploys blockchain technology for secure data logging in an SDN scenario to authenticate users with the aid of digital signatures and uses CNN for analyzing traffic characteristics to identify malicious flows [133]. Similarly, an attention-driven convolutional LSTM is deployed to improve the detection of DDoS in SDN by utilizing blockchain to reinforce the security mechanism [136].

**Table 3.** Examination of blockchain-centered SDN ID frameworks.

| ID technique | Tactic | Blockchain schema | Blockchain Layout | Blockchain consensus | Blockchain variety | ID approach | Attack variety | Network variety | Performance | App. Year |
|---|---|---|---|---|---|---|---|---|---|---|
| Signature-based | SBCIN [10] | C1 | Systematic | PoW | Public | Hybrid, collaborative, no response, online | 7 attack types | SDN | 96% true positive rate | 2019 |
| | CIDS [21] | C2 | Systematic | PoA+PBFT | Permissioned | Network, collaborative, no response, online | Intrusion | SDN | Efficiently share signatures, IA resistant | 2020 |
| | CID-CPS [85] | C1 | Systematic | Generic | Generic | Network, collaborative, no response, online | Intrusion | SDN-CPS | Resistant to insider, outsider attacks | 2023 |
| Anomaly based | BE-DSF [3] | C2 | Systematic | Generic | Generic | Network, distributed, active, online | Intrusion | SD-IoT | Efficiently satisfy data confidentiality | 2020 |
| | Challenge [86] | C1 | Systematic | Generic | Consortium | Network, collaborative, passive, online | Intrusion | SDN | Reduced adversarial attacks | 2020 |
| | DLBF [87] | C2 | Systematic | Vote-based | Permissioned | Network, distributed, active, online | Anomaly | SDIN | 88% accuracy, 0.83 precision | 2020 |
| | BMC-SDN [11] | C3 | Systematic | Vote-based | Private | Network, distributed, active, online | Flow injection | SDN | Efficiently detect fraudulent flow rules | 2021 |
| | BCAD [88] | C1 | Systematic | PoS, PoW | Private | Network, distributed, active, online | Flooding, DoS | SDN-IoT | Low attack detection time, high accuracy | 2021 |
| | Intra-inter DDoS [134] | C2 | Systematic | PBFT | Permissioned | Hybrid, distributed, active, online | DDoS | SDN | Low attack mitigation time | 2024 |
| Hybrid | BlockCSDN [89] | C1 | Systematic | Generic | Consortium | Network, collaborative, active, online | Intrusion | SDN | Resist insider, outsider attacks, high trust | 2022 |
| | BSDNFilter [90] | C1 | Systematic | Generic | Consortium | Hybrid, distributed, active, online | Flooding | SDN | Higher CPU use, effective for FA | 2021 |
| | SF-IoT [91] | C1 | Systematic | Generic | Generic | Network, distributed, active, online | Intrusion | SDN-IoT | 12.75% performance improvement | 2022 |
| | BlockSDN [92] | C1 | Systematic | Generic | Permissioned | Hybrid, distributed, active, online | DDoS, MIM, ED | SDN-SC | Detect different attacks | 2020 |
| | Blockctrl [93] | C1 | Systematic | Generic | Generic | Hybrid, distributed, active, online | Intrusion | SDON | Low resource utilization, fault tolerant | 2019 |
| | STFOA-CPP [94] | C1 | Systematic | Generic | Generic | Hybrid, distributed, passive, online | Intrusion | SDN | Minimum cost with respect to others, high trust | 2023 |
| | BCSDN-IoT [95] | C2 | Systematic | Generic | Generic | Network, collaborative, passive, online | ARP spoofing, DoS, scanning | SDN-IoT | Scalable, detect attacks, low overhead | 2022 |
| Rule-based | DDoS-SDN [96] | C3 | Systematic | Generic | Private | Hybrid, collaborative, active, online | DDoS | SDN | Reduces traffic after DDoS detection | 2019 |
| | MUD-IIoT [20] | C3 | Systematic | Generic | Public | Hybrid, distributed, active, online | Device misbehavior | SD-IIoT | High forwarding efficiency, accuracy | 2021 |
| | SC [97] | C3 | Systematic | PBFT | Permissioned | Network, distributed, active, online | Intrusion, DoS | SDN | Reduce controller failure, prevent unauthorized entry | 2021 |
| | IOTASDN [135] | C3 | Erratic | FBC | Public | Hybrid, distributed, active, online | DoS | SDN | High scalability and efficiency with low latency | 2024 |
| Heuristic-based | BPP [98] | C1 | Systematic | Generic | Generic | Network, distributed, passive, online | DoS, probing | SDN | Detects attacks and policy from packets | 2020 |
| | TR-IoT [99] | C3 | Systematic | PoAuthority | Public | Hybrid, distributed, active, online | DAO induction | SDN-IoT | Scalable, flexible, agile | 2020 |
| | B-SDN [100] | C3 | Systematic | PoAuthority | Generic | Hybrid, distributed, active, online | Intrusion | SDN-5G-IoT | High throughput, low latency | 2021 |
| | TrustBlock [101] | C3 | Systematic | PoW | Generic | Hybrid, distributed, active, online | Periodic, colluding | SDN | 98.8% detection rate | 2020 |
| | FBA-SDN [102] | C3 | Systematic | BFT | Generic | Hybrid, collaborative, passive, online | Intrusion | Edge-SDN | High efficacy in reaching rapid, reliable consensus | 2023 |
| | LRA [103] | C2 | Systematic | PoW | Public | Network, distributed, active, online | Malicious/dead nodes | SD-IoT | Optimum resource utilization | 2021 |
| | Cochain-SC [104] | C3 | Systematic | PoW | Private, public | Hybrid, collaborative, active, online | DDoS | SDN | High accuracy, cost-effectiveness, flexibility | 2019 |
| Artificial intelligence-based | MiTFed [105] | C1 | Systematic | PoS | Public | Network, collaborative, active, online | Intrusion | SDN | Zero-day, adversarial attack resistant | 2023 |
| | BFF-IDS [106] | C1 | Systematic | PoAuthority | Generic | Network, collaborative, no response, online | Fuzzy, DoS, impersonation | SDN-CAN | 0.98 detection rate, resource efficient | 2021 |
| | LID [107] | C1 | Systematic | Generic | Generic | Network, hierarchical, active, online | MIM, flow table overflow | SDN-5G | Good detection rate, accuracy, precision | 2021 |
| | RSL-KNN [108] | C1 | Systematic | None | Private | Network, distributed, active, online | Misrouting, intrusion | SDN-IoT | protect from forged commands, misrouting | 2019 |
| | ShChain_3D-ResNet [109] | C1 | Systematic | Generic | Private | Hybrid, distributed, no response, online | DDoS | SDN | 95.6% accuracy, low encryption, decryption times | 2022 |
| | CoC [110] | C2 | Systematic | PoW | Private | Hybrid, distributed, active, online | Malicious packets | SDN-IoT | Low delay, response time, processing time | 2019 |
| | Bloc-sec [111] | C2 | Systematic | PoW | Public | Network, distributed, active, online | Replay, spoofing, MIM, impersonation | SDN-B5G | 99.6% accuracy, high detection rate | 2020 |
| | FNN-CE [112] | C2 | Systematic | PoW | Private | Hybrid, hierarchical, active, online | DDoS, flooding | Intelligent-SDN | Low latency, high throughput | 2022 |
| | BrainChain [113] | C1 | Systematic | Generic | Permissioned | Hybrid, distributed, active, online | DDoS | SDN | High accuracy, low FPR | 2020 |
| | BlockSecIoTNet [114] | C1 | Systematic | PoW | Public | Hybrid, distributed, active, online | DDoS, flooding | SDN-IoT-SC | Cheaper computation, low latency | 2019 |
| | SCSAE-ALSTM [115] | C2 | Systematic | proof-of-authentication | Generic | Hybrid, distributed, active, online | Eavesdropping | SD-UAV | Detect illegitimate transactions | 2022 |
| | D-ANN [116] | C1 | Systematic | Vote-based | Private | Hybrid, distributed, active, online | DDoS | SDN-IoT | High detection accuracy, security | 2023 |
| | SliceBlock [12] | C1 | Erratic | PoSp | Generic | Hybrid, distributed, active, online | Intrusion | SD-6G | Scalable | 2022 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | LSTMSCAE-AGRU [117] | C1 | Systematic | PoAuthority | Generic | Hybrid, distributed, active, online | MIM, replay, impersonation | SD-IoT | Detect cyber threats, prevent SPF | 2022 |
| | DAG-SAC [118] | C2 | Erratic | Generic | Generic | Hybrid, distributed, active, online | Intrusion | SD-5G | High detection accuracy, low authentication time | 2023 |
| | BSDN-HMTD [133] | C2 | Erratic | Generic | Generic | Hybrid, distributed, active, online | DDoS | SDN | High survival and defender success rates, high attacker cost | 2024 |
| | C-LSTM [136] | C1 | Systematic | Generic | Generic | Hybrid, distributed, passive, online | DDoS | SDN-IoT | 98.3% accuracy | 2024 |
| Pure blockchain-based | BCS [132] | C3 | Systematic | PBFT | Permissioned | Network, distributed, active, online | Intrusion | SDN | Improves the attack detection rate | 2024 |

### 6.2.7 Blockchain-centered control plane attack detection

Recently, a framework known as BCS has been proposed to detect security attacks in multiple controllers in the control plane of SDN by using immutable features of blockchain to securely administrate controller communication [132].

## 7. Review examination

### 7.1 Examination of every study

Table 3 represents the examination of BC-centered SDN ID frameworks concerning ID technique, BC concept and parameters, ID detection parameters and attack types, performance, and time.

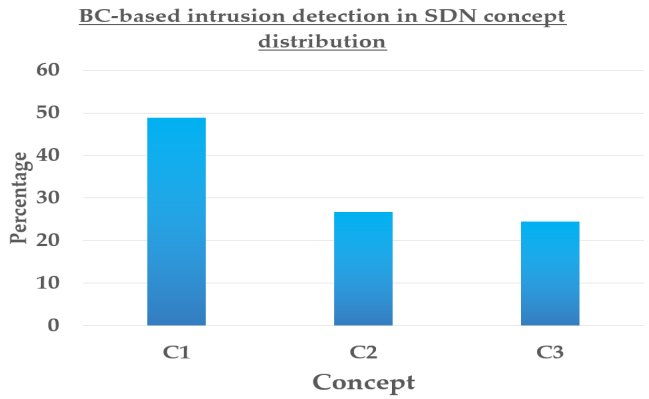
### 7.2 Overall examination

A summary of performance evaluation of blockchain-centered intrusion detection in SDN is given Table 4.

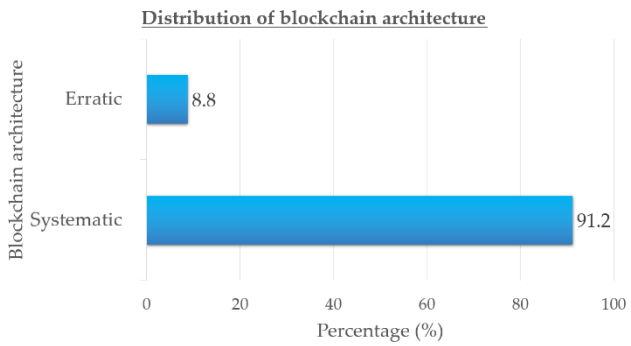
**Table 4.** Summary of performance evaluation of blockchain-centered SDN ID frameworks.

| Performance metric | Performance |
|---|---|
| Accuracy | 98.3% [136], High [118, 105], 99.6% [11], 95.6% [109], <95% [88], 88% [87] |
| Attack detection rate | 89.3% [132], 100% [108, 104], 0.98 [106], 98.8% [101] |
| Defender success rate | 86.5% [133] |
| Authentication time | Low [118] |
| Scalability | High [12, 135] |
| F1-score | 1.0 [116] |
| Detection time | <25 ms [88, 114], <3 s [108] |
| False positive rate | <40% [113], <10% [20, 108], <26% [104], <0.6% [98] |
| Latency | <6 ms [112], [110], <1100 ms [102], Low [135], <300 ms [20], <0.02 [3] |
| Processing time | <12 s [110], <4 s [107] |
| Response time | <6 ms [110], 15 ms [20] |
| Encryption time | <33 ms [109] |
| Decryption time | <37 ms [109] |
| Execution time | <10 s [108], <0.5 s [11] |
| Precision | <0.95 [107], 0.83 [87] |
| Gas consumption/cost | <5e5 [103], No fees [135], <0.17 [94], 40000 [21] |
| Throughput | High [100], <120 Gbps [98] |
| Bandwidth | <14 Mbps [98], <2 Mbps [90], <2.5 Mbps [89] |
| Efficiency | High [135] |
| Energy utilization | <90% [91] |
| Packet loss rate | <50% [91] |
| CPU usage | <18 [90] |
| Trust value | <1 [89] |
| Mitigation time | < 65 s [134] |
| Jitter | <0.03 [3] |
| Energy consumption | <0.60 [3] |
| Packet delivery ratio | <50% [3] |
| Networking overhead per payload | <700 ms [21] |
| True positive rate | 96% [10] |

Fig. 6 graphically represents the diffusion of BC-centered SDN network ID frameworks concerning blockchain linked components, ID and attack categorizations, and time.




(a)




(b)

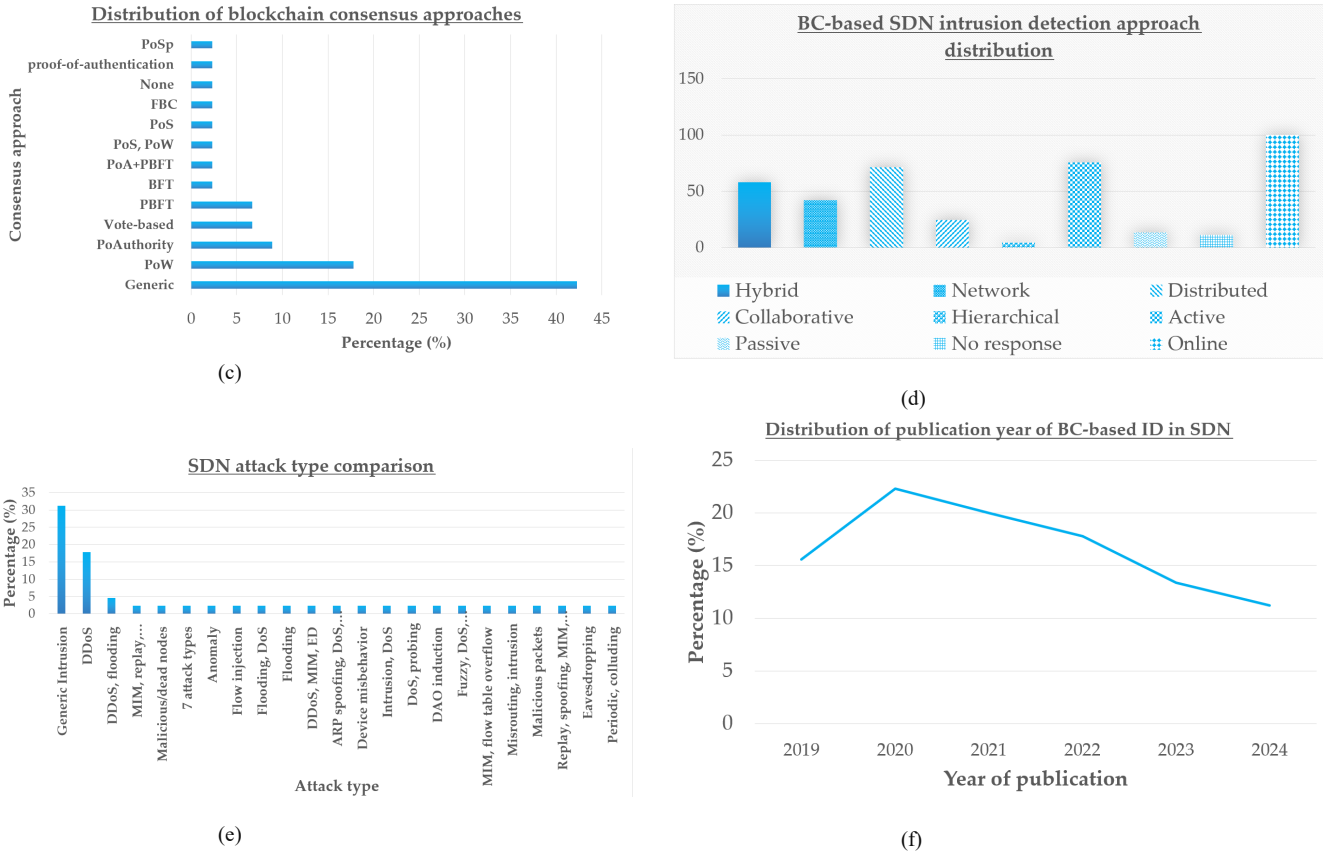



**Fig. 6.** Overall examination (a) BC-centered SDN-ID schema (b) BC category (c) BC collective decision protocol (d) BC-centered ID approach (e) Attack category (f) Appeared year.

First, according to Fig. 6a, the most supreme blockchain-centered SDN ID technique is C1 (blockchain-centered secure storage for off-chain ID), having a percentage of 48.9% pursued by concepts C2 (26.7%) and C3 (24.4%). Secondly, most BC-centered ID frameworks in SDN engage a systematic blockchain architecture (91.2%), while only 8.8% engage an erratic architecture, according to Fig. 6b. Moreover, the specific collective decision protocols used by most researchers for ID engaging blockchain are PoW (17.8%), PoAuthority (8.9%), PBFT (6.7%), and vote-centered collective decision protocol (6.7%), while 42.3% of frameworks have been crafted to engage generic collective decision, according to Fig. 6c. Moreover, when examining the SDN ID approach, as represented in Fig. 6d, they have been 100% online, 75.5% provide active response, the remaining 24.5% provide either no response (11.2%) or passive response (13.3%), 71.1% are fully distributed, 24.4% are explicitly collaborative, and 4.5% are hierarchical in the ID approach. Furthermore, 57.8% of the frameworks engage hybrid host and network-centered ID, while the remaining 42.2% are network-centered. When looking at the SDN attack type distribution in Fig. 6e, it is certain that most frameworks engage generic ID (31.2%), pursued by DDoS (17.8%), DDoS and flooding (4.6%), while the rest of the attacks, just like MIM, Eavesdropping (ED), replay, ARP spoofing, scanning, probing, DAO induction, misrouting, flow table overflow, spoofing, impersonation, periodic, colluding attacks, and so forth, have the least distribution percentage. When contemplating the BC-centered IDS proposed concerning time, frameworks have expanded prior to 2020, achieved a pinnacle by 2020, and gradually dropped afterwards, according to Fig. 6f.

## 8. Discussion

### 8.1 Potentials

#### 8.1.1 Allow collaborative ID

In collaborative ID, signatures, anomalies, alarms, etc. are exchanged among the devices in the network to detect intrusions collaboratively [119]. Blockchains can facilitate collaborative ID by elevating the trust of data exchanged among the endpoints [120]. Moreover, in SDN, faith among the SDN controllers can be managed by registering them in the blockchain to detect intrusions by collaborating with each other for the exchange of ID-related data. In this technique, a trusted, centralized third party is not required for ID, and the SDN controller can make decisions centered upon the data available in the blockchain.

#### 8.1.2 Potentiality of detecting generic and specific threats

Blockchain-centered ID in SDN is capable of detecting both specific and generic threats. Specifically, blockchain-integrated signature detection can be applied to identify insider and outsider threats; anomaly detection can be applied to diagnose adversarial assaults, DoS, flooding attacks; hybrid signature and anomaly-centered threat identification can be applied to diagnose MIM attacks, eavesdropping, etc.; heuristic algorithms can be applied to detect induction attacks, colluding attacks, periodic attacks, DDoS attacks, etc.; artificial intelligence can be applied to identify zero-day attacks, adversarial threats, DDoS attacks, etc. Furthermore, anomaly threat identification can be applied to identify generic threats that deviate from normal behavior [121]. Thus, blockchain can be highly integrated for secure data sharing for generic and specific threat detection using any of the

detection approaches specified above in an off-chain or on-chain approach.

#### 8.1.3 Strengthens entire security of the IDS

Blockchain indeed improves the validity of the detection output by strengthening the trustworthiness, validity, and integrity of the data utilized for threat detection [122]. It can not only improve the validity but also the entire performance of the IDS, such as the true positive rate, accuracy, etc. Moreover, blockchain facilitates trustworthy collaborations such as privacy-preserving ML model sharing in federated learning, preventing model poisoning attacks, and developing a global model for network threat detection [123]. Furthermore, blockchains can strengthen security by implementing robust authentication to register endpoints and validate the data or rules stored in the blockchain.

#### 8.1.4 High consonance with existing IDS and SDN

Already existing ID techniques, namely anomaly-centered, signature-centered, hybrid signature- and anomaly-centered, rule-centered, heuristic algorithm-centered, AI-centered, etc., can be readily integrated with blockchain, either in an off-chain or on-chain approach using SCs. Specifically, consensus approaches, namely proof-of-authority, can be incorporated to validate transactions and detect malicious endpoints in the network [124]. Moreover, proof-of-authentication can provide robust authentication by registering and verifying blockchain endpoints [125]. Furthermore, blockchain is readily applicable to the SDN paradigm to allow collaborative ID, where blockchain endpoints can collaboratively detect network intrusions with or without a global model for the SDN controller to make decisions accordingly.

#### 8.1.5 High adaptability and extensibility on account of SDN

Unlike blockchain-centered ID in generic networking, it is highly adaptable and scalable in SDN. For instance, conventional networks such as underwater acoustic networks lack adaptability and scalability [126]. SDN involves continuously monitoring the network to habituate to dynamic variations inside the network [127]. Thus, blockchain-centered IDS in SDN will also collect data continuously, such that these systems will be able to detect intrusions in real-time when the network state changes. Moreover, a given blockchain-centered ID in SDN can be allocated to a specific controller in a multi-controller architecture to divide the workload of the ID among multiple controllers, effectively providing an answer to the expandability issue of blockchains. Otherwise, in large networks, blockchains may perform poorly on account of degradation of performance related to latency, throughput, etc. on account of intensified processes such as distributed consensus on account of the large network scope.

### 8.2 Hardships

#### 8.2.1 Security exposures of blockchain

Even though blockchain strengthens the security aspect of ID in SDN in terms of protecting data integrity, providing authentication and access control, transaction validation, non-repudiation, etc., blockchain itself is known for a set of security vulnerabilities of its own [128]. For instance, in 51% vulnerability, malicious endpoints that compromise the majority of the network can compromise the security of the blockchain. Moreover, SCs in blockchains can be misconfigured, which can lead to undesirable behavior in contractual actions. Furthermore, there are other known intentional misuse attacks such as selfish mining, double spending attacks, etc., and network attacks such as eclipse attacks, domain name service attacks, etc. that can deteriorate the security of blockchain networks.

#### 8.2.2 High cost and overhead

When blockchain is integrated for ID in SDN, it will demand additional resources in terms of computation, memory, and transmission. These additional resources will demand a high cost for the network administrators, making them install additional hardware and software resources on end devices and controllers. Due to the cryptographic techniques, SCs, and consensus approaches in blockchain that serve in ID either by securing data or implementing ID by itself, blockchains consume computation and memory resources. Moreover, on account of peer-to-peer communication involved in consensus approaches, communication resources are frequently utilized, and this causes an additional communication overhead for ID, ultimately expanding the entire communication cost.

#### 8.2.3 Forks and consensus issues of blockchain

Forks occur in blockchain networks when there is a temporary divergence in transaction history on account of disagreement among participants involved in consensus. This can lead to temporary false positives in the IDSs that rely on blockchain data. Moreover, if the blockchain network decides to rollback transactions so as to undo data recorded during fork, it can have a negative effect on IDS that relied on those data. Specifically, if ID is implemented using a SC, forks will cause disruptions in their execution, making them produce unintended outcomes.

#### 8.2.4 Hardships in implementing in energy constrained SDN

Some networks, such as wireless sensor networks, IoT networks, etc., centered upon the SDN paradigm can be energy-constrained [129]. Applying blockchain to these energy-constrained networks can be challenging, as traditional blockchain causes the depletion of energy in network devices rapidly [130]. This is because of the manner in which blockchain networks behave on account of distributed consensus approaches involving multiple peer-to-peer broadcasts and algorithmic runs for validating and adding transactions. Moreover, cryptographic techniques applied to blockchains to protect the sensitivity and integrity of data consume additional energy. Furthermore, if ID takes place on the blockchain itself using SCs, they will also cause a depletion of energy, making the entire ID method using blockchain difficult to implement in energy constrained networks.

#### 8.2.5 High latency can impact real-time detection

Many IDSs in SDN require the threats to be detected in real-time so as to make timely decisions centered upon the output of detection to prevent or mitigate the threat [131]. On the other hand, blockchains can cause high latency in this method, making real-time threat detection challenging. This is true in both situations where blockchain is applied for secure data storage for ID by a conventional approach or pure blockchain centered ID by storing data and detecting using SCs. Either way, blockchain consensus requires transactions to be propagated in the blockchain network during block creation that involve broadcasting, multiple computations for

validation, etc., making the process time-consuming. Moreover, if there are disagreements during the consensus method leading to forks, it can cause additional time to resolve forks and maintain consistency.

### 8.3 Real world implementation

As real-world implementation, there exist blockchain-driven intrusion detection systems in industrial IoT. For example, case study [140] demonstrates the effectiveness of the collaborative intrusion detection leveraging blockchain for multi-microgrids in smart grid systems using blockchain consensus and a detection mechanism suggesting the suitability of blockchain-based distributed intrusion detection. For instance, manufacturer user description manifests are safely stored and validated using blockchain in software-defined industrial IoT edge networks to indicate device access and network functionality. Here, contract-centered SCs use security to validate the manifests in order to identify possible device misbehavior brought on by cyber-attacks [20]. In another case study for an internet of drones scenario, blockchain-driven RBFNNs are deployed for predictive analytics for intrusion detection [141]. Moreover, in a software-defined industrial network, switches are registered, validated using non-interactive proofs, and authorized using consensus, which is based on blockchain voting. In this application, at the controller, anomaly-centered flow analysis driven by deep Boltzmann machines identifies unusual requests from the switches [87]. Alternatively, in another case study, an integrity checking module using blockchain to prevent misrouting attacks and a security framework combining random sub-space learning for ID and K nearest neighbor have been proposed for the SDN-centered industrial IoT network to guard against forged commands for industrial control processes by using a case study of industrial control power systems [108].

Next, there are numerous recent works that have implemented blockchain-based intrusion detection in software-defined 5G networks. For instance, with Blake 256 authentication, NFV optimization, hashed flow rule storage on the blockchain, and a spiking double fuzzy NN-based IDS at the controller for packet analysis, Bloc-sec is a blockchain-based security approach for SD-5G [111]. In [118], a dynamic blockchain at the control tier holds hashed user credentials and forwarding rules for authentication and verification in software-defined 5G networks, while a capsule NN at the edge server categorizes packets as benign or malicious. In another case study of collaborative intrusion detection, the performance of the blockchain-centered ID has been evaluated under internal and external attacks [86].

Moreover, for blockchain-assisted SDN cyber-physical systems, a case study on collaborative intrusion detection proves that the system is viable and effective for intrusion detection [85]. In a practical framework known as BCNBI, blockchain has been utilized for authentication in the northbound interface of the SDN controller, and it studies worst-case and peer attack cases [142].

## 9. Conclusion, insights, and future orientations

In this examination, we first catered an abridgment of schema on ID concerning detection techniques, approaches, etc. and then briefly examined attack types that can exist in networking. In the wake of an abridgment on blockchain advancement, we examined extant work on blockchain-centered ID in SDN under different ID techniques and approaches. Rooted in this examination, we observed that blockchain-centered ID in SDN can be 3-fold: applying blockchain for secure data preservation for off-chain ID without authentication, off-chain ID by using blockchain for both authentication and secure data sharing, and on-chain ID with the aid of SCs and/or consensus with secure blockchain-centered data storage. Next, we elaborately examined the assessed works by categorizing them in terms of ID technique/approach, blockchain components, blockchain schema, etc. to assess the tendencies and hiatus in blockchain-centered ID in SDN. Finally, we examined the potentials and hardships of blockchain-centered ID in SDN.

This review supplies effective knowledge to the extant literature by providing tendencies and hiatus in blockchain-centered ID in SDN. Likewise, researchers can rapidly apply this assessment as a manual to formulate coming-time research problems rooted in the insights made centered upon the hardships examined to do research in blockchain-centered ID in SDN.

The below insights can be given for the hardships examined.

- With the aim of overcoming the security vulnerabilities of blockchain, several counter-measures can be applied. 51% vulnerability can be reduced by using alternative consensus approaches, namely proof-of-stake, where validators are selected centered upon the amount of stake. Smart contract vulnerabilities can be reduced by using a formal verification method to thoroughly check SCs for vulnerabilities before they are applied to the blockchain. Even after applying, they need to be audited frequently. Double-spending attacks can be reduced by using an appropriate consensus technique that makes it hard to perform double-spending for malicious endpoints. Furthermore, eclipse attacks on blockchain can be minimized by secure peer discovery mechanisms, minimizing the risk of a single entity controlling connections.
- The additional infrastructure cost associated with the fusion of blockchain and SDN for ID is unavoidable. However, operational costs can be reduced by several approaches. First, SCs and transactions can be optimized to minimize the computational cost. Moreover, a communication cost-aware consensus approach can be selected where possible to reduce the communication burden.
- The negative effect on ID on account of forks and rollbacks can be reduced by using a consensus approach such as proof-of-authority, which is resistant to them. Moreover, in ID, recovery plans need to be stated so as to handle situations where forks and rollbacks can occur in the blockchain. Furthermore, critical ID can be redundantly stored off-chain and cross validated against those in blockchain to detect any discrepancies.
- In energy-constrained SDN environments, an energy-efficient green consensus approach such as green proof-of-work may be applied. Moreover, energy waste can be alleviated by applying dedicated hardware resources designed for blockchain mining purposes. Furthermore, erratic blockchains that have parallel calculation potential and high scalability can be applied to escalate energy sustainability. Moreover, light-weight consensus approaches such as preferential delegated-proof-of-stake can be used

instead of resource-intensive consensus mechanisms like PoW to improve the scalability and number of transactions per second [137]. Moreover, researchers have used hybrid versions of private, permissioned, or public blockchains to overcome the latency issues, where private blockchains can be used for high-speed processing of intrusion detection data, while public blockchains can be used to store immutable data. Alternatively, hybrid permissioned blockchains can be utilized to improve the attack detection performance [138]. Moreover, latency issues in blockchain-centered intrusion detection can be reduced by using sharding techniques and then validating the shards optimally using an optimization-based technique [139]. Finally, by off-chain storage of data that are not directly utilized or of low importance for intrusion detection, the latency and scalability issues arising from blockchain can be drastically reduced.

- With the aim of overcoming the additional latency introduced by blockchain, several propositions can be put forward. First, blockchain can be assisted with parallel off-chain storage for non-critical data, reducing the burden on the blockchain and making it operate faster on account of less load. Moreover, if blockchain itself is applied for ID in SDN, SCs can be optimized for latency. Prioritization of data flows can be applied to prioritize critical transactions, allowing them to be used for ID with low latency. Furthermore, blockchain parameters, namely block size, cryptocurrency limits, etc., can be adjusted to get low latency.

Blockchains have been utilized in SDN to detect intrusions on- or off-chain, where the purity, confidentiality, genuineness, and so on of data are protected using blockchain. In the coming time, research can investigate the joint optimization of SDN-related controller parameters and blockchain parameters for more efficient use of blockchain-centered ID in SDN. Furthermore, coming research can incorporate forwarding standardizations for applying blockchain with SDN for ID. In addition, it will be very fascinating to judge the conduct of current blockchain-centered network IDs in SDN under quantum computing attacks, and researchers should consider mechanisms to make these blockchain-centered IDs in SDN resist them.



## References


[1] B. Mantur, A. Desai, and K.S. Nagegowda, "Centralized control signature-based firewall and statistical-based network intrusion detection system (NIDS) in software defined networks (SDN)," in *Proc. Emerging Research Comput. Inform. Commun. Appl. (ERCICA 2015)*, Bangalore, India: Springer, Jan. 2015, vol. 1, pp. 497-506, doi: 10.1007/978-81-322-2550-8_48

[2] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "Machine Learning Based Link Stability Prediction for Routing in Software Defined Vehicular Networks," in *Proc. 20th Academic Sessions*, Matara, Sri Lanka: University of Ruhuna, Jun. 2023, Art. no. 60, doi: http://ir.lib.ruh.ac.lk/xmlui/handle/iruor/13317

[3] D.V. Medhane, A.K. Sangaiah, M.S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6143-6149, Feb. 2020, doi: 10.1109/JIOT.2020.2977196

[4] H. V. Vo, D.H. Nguyen, T.T. Nguyen, H.N. Nguyen, and D.V. Nguyen, "Leveraging AI-Driven Realtime Intrusion Detection by Using WGAN and XGBoost," in *Proc. 11th Int. Symp. Inform. Commun. Tech.*, Hanoi, Vietnam: ACM, Dec. 2022, pp. 208-215, doi: 10.1145/3568562.3568660

[5] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," *Comput. Electr. Eng.*, vol. 107, Apr. 2023, Art. no. 108626, doi: 10.1016/j.compeleceng.2023.108626

[6] Z. Chunyue, L. Yun, and Z. Hongke, "A pattern matching based network intrusion detection system," in *Proc. 2006 9th Int. Conf. Control, Autom. Robot. Vision*, Singapore: IEEE, Dec. 2006, pp. 1-4, doi: 10.1109/ICARCV.2006.345459

[7] N. Alexopoulos, E. Vasilomanolakis, N.R. Ivánkó, and M. Mühlhäuser, "Towards blockchain-based collaborative intrusion detection systems," in *Proc. Critical Inform. Infrastructures Security: 12th Int. Conf. (CRITIS 2017)*, Lucca, Italy: Springer, Oct. 2017, pp. 107-118, doi: 10.1007/978-3-319-99843-5_10

[8] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "Data Gathering Optimization in Hybrid Software Defined Vehicular Networks," in *Proc. 20th Academic Sessions*, Matara, Sri Lanka: University of Ruhuna, Jun. 2023, Art. no. 59, doi: http://ir.lib.ruh.ac.lk/xmlui/handle/iruor/13315

[9] C. Birkinshaw, E. Rouka, and V.G. Vassilakis, "Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks," *J. Netw. Comput. Appl.*, vol. 136, pp. 71-85, Jun. 2019, doi: 10.1016/j.jnca.2019.03.005

[10] R.M.A. Ujjan, Z. Pervez, and K. Dahal, "Snort based collaborative intrusion detection system using blockchain in SDN," in *Proc. 2019 13th Int. Conf. Softw. Knowl. Inf. Manag. Appl. (SKIMA)*, Island of Ulkulhas, Maldives: IEEE, Aug. 2019, pp. 1-8, doi: 10.1109/SKIMA47702.2019.8982413

[11] A. Derhab, M. Guerroumi, M. Belaoued, and O. Cheikhrouhou, "BMC-SDN: Blockchain-based multicontroller architecture for secure software-defined networks", *Wirel. Commun. Mob. Comput*, vol. 2021, pp. 1-12, Apr. 2021, doi: 10.1155/2021/9984666

[12] I.H. Abdulqadder, and S. Zhou, "SliceBlock: context-aware authentication handover and secure network slicing using DAG-blockchain in edge-assisted SDN/NFV-6G environment," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 18079-18097, Mar. 2022, doi: 10.1109/JIOT.2022.3161838

[13] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges," *Network*, vol. 3, no. 3, pp. 343-421, Aug. 2023, doi: 10.3390/network3030017

[14] D. Lee, and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multimedia Tools Appl.*, vol. 80, pp. 34517-34534, Nov. 2021, doi: 10.1007/s11042-020-08776-y

[15] G. Kaur, and C. Gandhi, "Scalability in blockchain: Challenges and solutions," *Handb. Res. Blockchain Technol.*, Academic Press, pp. 373-406, May 2020, doi: 10.1016/B978-0-12-819816-2.00015-0

[16] P.A.D.S.N. Wijesekara, "Ethical Knowledge Sharing Leveraging Blockchain: An Overview," *Sci. Eng. Technol.*, vol. 4, no. 1, pp. 112-136, Apr. 2024, doi: 10.54327/set2024/v4.i1.126

[17] A.H. Lone, and R. Naaz, "Demystifying cryptography behind blockchains and a vision for post-quantum blockchains," in *Proc. 2020 IEEE Int. Conf. Innovation Technol. (INOCON)*, Bangluru, India: IEEE, Nov. 2020, pp. 1-6, doi: 10.1109/INOCON50539.2020.9298215

[18] I.F.T. Alyaseen, "Consensus algorithms blockchain: A comparative study," *Int. J. Perceptive Cognit. Comput.*, vol. 5, no. 2, pp. 66-71, Dec. 2019, doi: 10.31436/ijpcc.v5i2.103

[19] C. Mohan, "State of public and private blockchains: Myths and reality," in *Proc. 2019 Int. Conf. Manag. Data*, New York, United States: ACM, pp. 404-411, Jun. 2019, doi: 10.1145/3299869.3314116

[20] P. Krishnan, K. Jain, K. Achuthan, and R. Buyya, "Software-defined security-by-contract for blockchain-enabled MUD-aware industrial IoT edge networks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7068-7076, Jun. 2021, doi: 10.1109/TII.2021.3084341

[21] W. Fan, Y. Park, S. Kumar, P. Ganta, X. Zhou, and S.Y. Chang, "Blockchain-enabled collaborative intrusion detection in software defined networks," in *Proc. 2020 IEEE 19th Int. Conf. Trust, Security Privacy Comput. Commun. (TrustCom)*, Guangzhou, China: IEEE, Dec. 2020, pp. 967-974, doi: 10.1109/TrustCom50675.2020.00129

[22] O. Alkadi, N. Moustafa, and B. Turnbull, "A review of intrusion detection and blockchain applications in the cloud: approaches, challenges and solutions," *IEEE Access*, vol. 8, pp. 104893-104917, Jun. 2020, doi: 10.1109/ACCESS.2020.2999715

[23] S. Al-E'mari, M. Anbar, Y. Sanjalawe, S. Manickam, and I. Hasbullah, "Intrusion Detection Systems Using Blockchain Technology: A Review, Issues and Challenges," *Comput. Syst. Sci. Eng.*, vol. 40, no. 1, pp. 87-112, Jan. 2022, doi: 10.32604/csse.2022.017941

[24] P.A.D.S.N. Wijesekara, "A study in University of Ruhuna for investigating prevalence, risk factors and remedies for psychiatric illnesses among students," *Sci. Rep.*, vol. 12, no. 1, Jul. 2022, Art. no. 12763 doi: 10.1038/s41598-022-16838-4

[25] P.A.D.S.N. Wijesekara, and Y.K. Wang, "A Mathematical Epidemiological Model (SEQIJRDS) to Recommend Public Health Interventions Related to COVID-19 in Sri Lanka," *COVID*, vol. 2, no. 6, pp. 793-826, Jun. 2022, doi: 10.3390/covid2060059

[26] H.R. Ghaeini, and N.O. Tippenhauer, "Hamids: Hierarchical monitoring intrusion detection system for industrial control systems," in *Proc. 2nd ACM Workshop Cyber-Physical Syst. Security Privacy*, Vienna, Austria: ACM, Oct. 2016, pp. 103-111, doi: 10.1145/2994487.2994492

[27] A.M. Riyad, M.I. Ahmed, and R.R. Khan, "An adaptive distributed intrusion detection system architecture using multi agents," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 9, no. 6, pp. 4951-4960, Dec. 2019, doi: 10.11591/ijece.v9i6.pp4951-4960

[28] S. Anwar, J. Mohamad Zain, M.F. Zolkipli, Z. Inayat, S. Khan, B. Anthony, and V. Chang, "From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, Mar. 2017, Art. no. 39, doi: 10.3390/a10020039

[29] S. Jin, J.G. Chung, and Y. Xu, "Signature-based intrusion detection system (IDS) for in-vehicle CAN bus network," in *Proc. 2021 IEEE Int. Symp. Circuits Syst. (ISCAS)*, Daegu, Korea: IEEE, May 2021, pp. 1-5, doi: 10.1109/ISCAS51556.2021.9401087

[30] H.M.D.P.M. Herath, W.A.S.A. Weraniyagoda, R.T.M. Rajapaksha, P.A.D.S.N. Wijesekara, K.L.K. Sudheera, and P.H.J. Chong, "Automatic Assessment of Aphasic Speech Sensed by Audio Sensors for Classification into Aphasia Severity Levels to Recommend Speech Therapies," *Sensors*, vol. 22, no. 18, Sep. 2022, Art. no. 6966, doi: 10.3390/s22186966

[31] M. Hasan, "A Hybrid Real-Time Intrusion Detection System for an Internet of Things Environment with Signature and Anomaly Based Intrusion detection," *Doctoral dissertation, Dublin, National College of Ireland*, 2019.

[32] B.G. Atli, Y. Miche, and A. Jung, "Network intrusion detection using flow statistics," in *Proc. 2018 IEEE Stat. Signal Process. Workshop (SSP)*, Freiburg im Breisgau, Germany: IEEE, Jun. 2018, pp. 70-74, doi: 10.1109/SSP.2018.8450709

[33] S.K. Patel, and A. Sonker, "Rule-based network intrusion detection system for port scanning with efficient port scan detection rules using snort," *Int. J. Future Generation Commun. Netw.*, vol. 9, no. 6, pp. 339-350, Jun. 2016, doi: 10.14257/ijfgcn.2016.9.6.32

[34] H. Farsi, A. Fanian, and Z. Taghiyarrenani, "A novel online state-based anomaly detection system for process control networks," *Int. J. Critical Infrastructure Protection*, vol. 27, Dec. 2019, Art. no. 100323, doi: 10.1016/j.ijcip.2019.100323

[35] M. Niemiec, R. Kościej, and B. Gdowski, "Multivariable Heuristic Approach to Intrusion Detection in Network Environments," *Entropy*, vol. 23, no. 6, Jun. 2021, Art. no. 776, doi: 10.3390/e23060776

[36] P.A.D.S.N. Wijesekara, "Deep 3D Dynamic Object Detection towards Successful and Safe Navigation for Full Autonomous Driving," *Open Transp. J.*, vol. 16, no. 1, Oct. 2022, Art. no. e187444782208191, doi: 10.2174/18744478-v16-e2208191

[37] B. Farzaneh, M. Koosha, E. Boochanpour, and E. Alizadeh, "A new method for intrusion detection on RPL routing protocol using fuzzy logic," in *Proc. 2020 6th Int. Conf. Web Research (ICWR)*, Tehran, Iran: IEEE, Apr. 2020, pp. 245-250, doi: 10.1109/ICWR49608.2020.9122278

[38] S. Rizvi, M. Scanlon, J. McGibney, and J. Sheppard, "Deep learning based network intrusion detection system for resource-constrained environments," in *Proc. Int. Conf. Digit. Forens. Cyber Crime*, Boston, USA: Springer, Nov. 2022, pp. 355-367, doi: 10.1007/978-3-031-36574-4_21

[39] R. Gassais, N. Ezzati-Jivan, J.M. Fernandez, D. Aloise, and M.R. Dagenais, "Multi-level host-based intrusion detection system for Internet of things," *J. Cloud Comput.*, vol. 9, pp. 1-16, Nov. 2020, doi: 10.1186/s13677-020-00206-6

[40] M. Sarhan, S. Layeghy, and M. Portmann, "Towards a standard feature set for network intrusion detection system datasets," *Mobile Netw. Appl.*, vol. 27, pp. 357-370, Feb. 2022, doi: 10.1007/s11036-021-01843-0

[41] S. Bijani, and M. Kazemitabar, "HIDMN: A host and network-based intrusion detection for mobile networks," in *Proc. 2008 Int. Conf. Comput. Electr. Eng.*, Phuket, Thailand: IEEE, Dec. 2008, pp. 204-208, doi: 10.1109/ICCEE.2008.183

[42] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "An Optimization Framework for Data Collection in Software Defined Vehicular Networks," *Sensors*, vol. 23, no. 3, , Feb. 2023, Art. no. 1600, doi: 10.3390/s23031600

[43] M. Kumar, and A.K. Singh, "Distributed intrusion detection system using blockchain and cloud computing infrastructure," in *Proc. 2020 4th Int. Conf. Trends Electron. Informat. (ICOEI)*, Tirunelveli, India: IEEE, Jun. 2020, pp. 248-252, doi: 10.1109/ICOEI48184.2020.9142954

[44] P. Santikellur, T. Haque, M. Al-Zewairi, and R.S. Chakraborty, "Optimized multi-layer hierarchical network intrusion detection system with genetic algorithms," in *Proc. 2019 2nd Int. Conf. New Trends Comput. Sci. (ICTCS)*, Amman, Jordan: IEEE, Oct. 2019, pp. 1-7, doi: 10.1109/ICTCS.2019.8923067

[45] W.T. Yue, and M. Çakanyıldırım, "A cost-based analysis of intrusion detection system configuration under active or passive response," *Decision Support Syst.*, Vol. 50, No. 1, pp.21-31, Dec. 2010, doi: 10.1016/j.dss.2010.06.001

[46] S.K. Alampalayam, A. Kumar, J.H. Graham, and S. Srinivasan, "Intruder Identification and Response Framework for Mobile Ad hoc Networks," in *Proc. CATA*, Honolulu, Hawaii: ISCA, Mar. 2007, pp. 260-265.

[47] S. Hossain-McKenzie, A. Chavez, N. Jacobs, C.B. Jones, A. Summers, and B. Wright, "Proactive intrusion detection and mitigation system: Case study on packet replay attacks in distributed energy resource systems," in *Proc. 2021 IEEE Power Energy Conf. Illinois (PECI)*, Urbana, USA: IEEE, Apr. 2021, pp. 1-6, doi: 10.1109/PECI51586.2021.9435231

[48] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Comprehensive Survey on Knowledge-Defined Networking," *Telecom*, vol. 4, no. 3, pp. 477-596, Aug. 2023, doi: 10.3390/telecom4030025

[49] M. Lopez-Martin, A. Sanchez-Esguevillas, J.I. Arribas, and B. Carro, "Network intrusion detection based on extended RBF neural network with offline reinforcement learning," *IEEE Access*, vol. 9, pp. 153153 - 153170, Nov. 2021, doi: 10.1109/ACCESS.2021.3127689

[50] M.A. Aladaileh, M. Anbar, I.H. Hasbullah, Y.W. Chong, and Y.K. Sanjalawe, "Detection techniques of distributed denial of service attacks on software-defined networking controller–a review," *IEEE Access*, vol. 8, pp. 143985-143995, Aug. 2020, doi: 10.1109/ACCESS.2020.3013998

[51] A. Mihoub, O.B. Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," *Comput. Electr. Eng.*, vol. 98, Mar. 2022, Art. no. 107716, doi: 10.1016/j.compeleceng.2022.107716

[52] G. Yadav, A. Allakany, V. Kumar, K. Paul, and K. Okamura, "Penetration testing framework for iot," in *Proc. 2019 8th Int. Congr. Adv. Appl. Informat. (IIAI-AAI)*, Toyama, Japan: IEEE, Jul. 2019, pp. 477-482, doi: 10.1109/IIAI-AAI.2019.00104

[53] N.I. Mowla, I. Doh, and K. Chae, "An efficient defense mechanism for spoofed IP attack in SDN based CDNi," in *Proc. 2015 Int. Conf. Inform. Netw. (ICOIN),* Cambodia: IEEE*,* Jan. 2015*,* pp. 92-97, doi: 10.1109/ICOIN.2015.7057863

[54] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Machine Learning-Aided Network Contention-Aware Link Lifetime- and Delay-Based Hybrid Routing Framework for Software-Defined Vehicular Networks," *Telecom*, vol. 4, no. 3, pp. 393-458, Jul. 2023, doi: 10.3390/telecom4030023

[55] S. Luo, Y. Lai, and J. Liu, "Selective forwarding attack detection and network recovery mechanism based on cloud-edge cooperation in software-defined wireless sensor network," *Comput. Security*, vol. 126, Mar. 2023, Art. no. 103083, doi: 10.1016/j.cose.2022.103083

[56] F.A. Alenezi, S. Song, and B.Y. Choi, "WAND: wormhole attack analysis using the neighbor discovery for software-defined heterogeneous internet of things," in *Proc. 2021 IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Montreal, Canada: IEEE, Jun. 2021, pp. 1-6, doi: 10.1109/ICCWorkshops50388.2021.9473770

[57] R.P. Nayak, S. Sethi, S.K. Bhoi, K.S. Sahoo, M. Masud, and J.F. Al-Amri, "Sybil Misbehavior Detection in Software Defined VANETs using Received Signal Strength," *Turkish Onl. J. Qualitat. Inqu.*, vol. 12, no. 5, pp. 3454-3468, Jun. 2021.

[58] M. Erritali, B. Cherkaoui, H. Ezzikouri, and A. Beni-hssane, "Detection of the Black Hole Attack on SDN-Based VANET Network," in *Proc. Distrib. Sensing Intell. Syst. (ICDSIS 2020)*, Jun. 2022, pp. 67-74, doi: 10.1007/978-3-030-64258-7_6

[59] A. Nehra, M. Tripathi, M.S. Gaur, R.B. Battula, and C. Lal, "SLDP: A secure and lightweight link discovery protocol for software defined networking," *Comput. Netw.*, vol. 150, pp. 102-116, Feb. 2019, doi: 10.1016/j.comnet.2018.12.014

[60] H. Aldabbas, and R. Amin, "A novel mechanism to handle address spoofing attacks in SDN based IoT," *Cluster Comput.*, vol. 24, no. 4, pp. 3011-3026, Jun. 2021, doi: 10.1007/s10586-021-03309-0

[61] T. Alharbi, D. Durando, F. Pakzad, and M. Portmann, "Securing ARP in software defined networks," in *Proc. 2016 IEEE 41st Conf. Local Comput. Netw. (LCN)*, Dubai, United Arab Emirates: IEEE, Nov. 2016, pp. 523-526, doi: 10.1109/LCN.2016.83

[62] Y. Hu, K. Zheng, X. Wang, and Y. Yang, "WORM-HUNTER: A Worm Guard System using Software-defined Networking," *KSII Tran. Internet Inform. Syst.*, vol. 11, no. 1, Jan. 2017, doi: 10.3837/tiis.2017.01.026

[63] R. Jin, and B. Wang, "Malware detection for mobile devices using software-defined networking," in *Proc. 2013 Second GENI Research Educ. Experiment Workshop,* Salt Lake City, USA: IEEE, Mar. 2013, pp. 81-88, doi: 10.1109/GREE.2013.24

[64] A. Mahmood, W.E. Zhang, Q.Z. Sheng, S.A. Siddiqui, and A. Aljubairy, "Trust management for software-defined heterogeneous vehicular ad hoc networks," *Secur. Priv. Trust IoT Environ.*, pp. 203-226, May 2019, doi: 10.1007/978-3-030-18075-1_10

[65] A. H. Lara, and B. Ramamurthy, "OpenSec: Policy-based security using software-defined networking," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 1, pp. 30-42, Jan. 2016, doi: 10.1109/TNSM.2016.2517407

[66] Z. Hu, M. Wang, X. Yan, Y. Yin, and Z. Luo, "A comprehensive security architecture for SDN," In *Proc. 2015 18th Int. Conf. Intell. Next Generation Netw.*, Paris, France: IEEE, Feb. 2015, pp. 30-37, doi: 10.1109/ICIN.2015.7073803

[67] K. Cabaj, M. Gregorczyk, and W. Mazurczyk, "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics," *Comput. Electr. Eng.*, vol. 66, pp. 353-368, Feb. 2018, doi: 10.1016/j.compeleceng.2017.10.012

[68] J. Li, S. Qin, T. Tu, H. Zhang, and Y. Li, "Packet injection exploiting attack and mitigation in software-defined networks," *Appl. Sci.*, vol. 12, no. 3, Jan. 2022, Art. no. 1103, doi: 10.3390/app12031103

[69] J. Hou, M. Zhang, Z. Zhang, W. Shi, B. Qin, and B. Liang, "On the fine-grained fingerprinting threat to software-defined networks," *Fut. Gener. Comput. Syst.*, vol. 107, pp. 485-497, Jun. 2020, doi: 10.1016/j.future.2020.01.046

[70] J.M.S. Vilchez, I.G.B. Yahia, and N. Crespi, "Self-healing mechanisms for software defined networks," in *Proc. 8th Int. Conf. Autonomous Infrastructure Manag. Security (AIMS 2014)*, Brrno, Czech Republic: HAL, Jun. 2014, doi: https://hal.science/hal-01068045v1

[71] L. Yan, D. Li, X. Huang, Y. Ma, and K. Xie, "Certrust: An SDN-based framework for the trust of certificates against crossfire attacks in IoT scenarios," *Netw. Distrib. Syst.*, vol. 134, no. 3, pp. 2137-2162, Mar. 2023, doi: 10.32604/cmes.2022.022462

[72] F. Tariq, and S. Baig, "Machine learning based botnet detection in software defined networks," *Int. J. Secur. Appl*, vol. 11, no. 11, pp. 1-12, Oct. 2017, doi: 10.14257/ijsia.2017.11.11.01

[73] T.H. Nguyen, and M. Yoo, "Attacks on host tracker in SDN controller: Investigation and prevention," in *Proc 2016 Int. Conf. Inform. Commun. Technol. Convergence (ICTC),* Jeju, Korea: IEEE, Oct. 2016, pp. 610-612, doi: 10.1109/ICTC.2016.7763545

[74] T. Chin, K. Xiong, and C. Hu, "Phishlimiter: A phishing detection and mitigation approach using software-defined networking," *IEEE Access*, vol. 6, pp. 42516-42531, Jun. 2018, doi: 10.1109/ACCESS.2018.2837889

[75] A.L. Aliyu, A. Aneiba, M. Patwary, and P. Bull, "A trust management framework for software defined network (SDN) controller and network applications," *Comput. Netw.*, vol. 181, Nov. 2020, Art. no. 107421, doi: 10.1016/j.comnet.2020.107421

[76] P.W. Tsai, A.C. Risdianto, M.H. Choi, S.K. Permal, and T.C. Ling, "SD-BROV: An enhanced BGP hijacking protection with route validation in software-defined exchange," *Fut. Intern.*, vol. 13, no. 7, Jun. 2021, Art. no. 171, doi: 10.3390/fi13070171

[77] M. Husnain, K. Hayat, E. Cambiaso, U.U. Fayyaz, M. Mongelli, H. Akram, S. Ghazanfar Abbas, and G.A. Shah, "Preventing mqtt vulnerabilities using iot-enabled intrusion detection system," *Sensors*, vol. 22, no. 2, Jan. 2022, Art. no. 567, doi: 10.3390/s22020567

[78] E. Ficke, K.M. Schweitzer, R.M. Bateman, and S. Xu, "Analyzing root causes of intrusion detection false-negatives: Methodology and case study," in *Proc. 2019 IEEE Military Commun. Conf. (MILCOM)*, Norfolk, USA: IEEE, Nov. 2019, pp. 1-6, doi: 10.1109/MILCOM47813.2019.9020860

[79] O.H. Alhazmi, S.W. Woo, and Y.K. Malaiya, "Security vulnerability categories in major software systems," in *Proc. Commun. Netw. Inform. Security*, Cambridge, USA: ICTA Press, Oct. 2006, pp. 138-143.

[80] S. Anand, and K. Patne, "Network Intrusion Detection and Prevention," *Int. J. Research Appl. Sci. Eng. Technol. (IJRASET)*, vol. 10, no. 6, pp. 3754-3758, Jun. 2022, doi: 10.22214/ijraset.2022.44761

[81] A. Punia, and V.R. Vatsa, "Current trends and approaches of network intrusion detection system," *Int. J. Comput. Sci. Mobile Comput.*, vol. 6, no. 6, pp. 266-270, Jun. 2017.

[82] P.A.D.S.N. Wijesekara, "A Literature Review on Access Control in Networking Employing Blockchain," *Indonesian J. Comput. Sci.*, vol. 13, no. 1, pp. 734-768, Feb. 2024, doi: 10.33022/ijcs.v13i1.3764

[83] P.A.D.S.N. Wijesekara, "A Review on Deploying Blockchain Technology for Network Mobility Management," *Int. Trans. Electr. Eng. Comput. Sci.*, vol. 3, no. 1, pp. 1-33, Mar. 2024, doi: 10.62760/iteecs.3.1.2024.83

[84] P.A.D.S.N. Wijesekara, "A Review of Blockchain-Rooted Energy Administration in Networking," *Indonesian J. Comput. Sci.*, vol. 13, no. 2, pp. 1607-1642, Apr. 2024, doi: 10.33022/ijcs.v13i2.3818

[85] W. Li, Y. Wang, and J. Li, "A blockchain-enabled collaborative intrusion detection framework for SDN-assisted cyber-physical systems", *Int. J. Inform. Security*, vol. 22, pp. 1219-1230, Oct. 2023, doi: 10.1007/s10207-023-00687-x

[86] W. Li, J. Tan, and Y. Wang, "A framework of blockchain-based collaborative intrusion detection in software defined networking," in *Proc. Netw. Syst. Security: 14th Int. Conf. NSS 2020*, Melbourne, Australia: Springer, Nov. 2020, pp. 261-276, doi: 10.1007/978-3-030-65745-1_15

[87] M. Singh, G.S. Aujla, A. Singh, N. Kumar, and S. Garg, "Deep-learning-based blockchain framework for secure software-defined industrial networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 606-616, Jan. 2020, doi: 10.1109/TII.2020.2968946

[88] D. Guha Roy, and S.N. Srirama, "A blockchain-based cyber attack detection scheme for decentralized Internet of Things using software-defined network," *Softw. Practice Experience*, vol. 51, no. 7, pp. 1540-1556, May 2021, doi: 10.1002/spe.2972

[89] W. Li, Y. Wang, W. Meng, J. Li, and C. Su, "BlockCSDN: towards blockchain-based collaborative intrusion detection in software defined networking," *IEICE Trans. Inform. Syst.*, vol. 105, no. 2, pp. 272-279, Feb. 2022, doi: 10.1587/transinf.2021BCP0013

[90] W. Meng, W. Li, and J. Zhou, "Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration," *Inform. Fusion*, vol. 70, pp. 60-71, Jun. 2021, doi: 10.1016/j.inffus.2020.12.006

[91] S. Rani, H. Babbar, G. Srivastava, T.R. Gadekallu, and G. Dhiman, "Security Framework for Internet-of-Things-Based Software-Defined Networks Using Blockchain," *IEEE Intern. Things J.*, vol. 10, no. 7, pp. 6074-6081, Nov. 2022, doi: 10.1109/JIOT.2022.3223576

[92] G.S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications," *IEEE Netw.*, vol. 34, no. 2, pp. 83-91, Apr. 2020, doi: 10.1109/MNET.001.1900151

[93] H. Yang, Y. Liang, Q. Yao, S. Guo, A. Yu, and J. Zhang, "Blockchain-based secure distributed control for software defined

optical networking," *China Commun.*, vol. 16, no. 6, pp. 42-54, Jun. 2019, doi: 10.23919/JCC.2019.06.004

[94] S. Alkhli, "Sea Turtle Foraging Optimization-Based Controller Placement with Blockchain-Assisted Intrusion Detection in Software-Defined Networks," *Comput. Mat. Continua*, vol. 75, no. 3, pp. 4735-4752, Apr. 2023, doi: 10.32604/cmc.2023.037141

[95] Y. ABBASSI, and H. Benlahmer, "BCSDN-IoT: Towards an IoT security architecture based on SDN and Blockchain," *Int. J. Electr. Comput. Eng. Syst.*, vol. 13, no. 2, pp. 155-163, Feb. 2022, doi: 10.32985/ijeces.13.2.8

[96] N. Giri, R. Jaisinghani, R. Kriplani, T. Ramrakhyani, and V. Bhatia, "Distributed denial of service (DDoS) mitigation in software defined network using blockchain," in *Proc. 2019 third Int. Conf. I-SMAC (IoT Social Mobile Analytics Cloud)*, Palladam, India: IEEE, Dec. 2019, pp. 673-678, doi: 10.1109/I-SMAC47947.2019.9032690

[97] M. Almakhour, A. Wehby, L. Sliman, A.E. Samhat, and A. Mellouk, "Smart contract based solution for secure distributed sdn," in *Proc. 2021 11th IFIP Int. Conf. New Technol. Mobility Security (NTMS)*, Paris, France: IEEE, Apr. 2021, pp. 1-6, doi: 10.1109/NTMS49979.2021.9432647

[98] A. Yazdinejad, R.M. Parizi, A. Dehghantanha, and K.K.R. Choo, "P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking," *Comput. Security*, vol. 88, Jan. 2020, Art. no. 101629, doi: 10.1016/j.cose.2019.101629

[99] A. Hakiri, B. Sellami, S.B. Yahia, and P. Berthou, "A Blockchain architecture for SDN-enabled tamper-resistant IoT networks," in *Proc. 2020 Global Inform. Infrastructure Netw. Symp. (GIIS)*, Tunis, Tunisia: IEEE, Oct. 2020, pp. 1-4, doi: 10.1109/GIIS50753.2020.9248492

[100] A. Hakiri, and B. Dezfouli, "Towards a blockchain-SDN architecture for secure and trustworthy 5G massive IoT networks," in *Proc. 2021 ACM Int. Workshop Softw. Defined Netw. Netw. Function Virtualization Security*, Virtual Event, USA: ACM, Apr. 2021, pp. 11-18, doi: 10.1145/3445968.3452090

[101] B. Zhao, Y. Liu, X. Li, J. Li, and J. Zou, "TrustBlock: An adaptive trust evaluation of SDN network nodes based on double-layer blockchain," *PloS one*, vol. 15, no. 3, Mar. 2020, Art. no. e0228844, doi: 10.1371/journal.pone.0228844

[102] J. Hayes, A. Aneiba, M.M. Gaber, and R. Abozariba, "FBA-SDN: A Federated Byzantine Approach for Blockchain-based Collaborative Intrusion Detection in Edge SDN," in *Proc. 2023 IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Rome, Italy: IEEE, Jun. 2023, pp. 427-433, doi: 10.1109/ICCWorkshops57953.2023.10283805

[103] S. Abbas, N. Javaid, A. Almogren, S.M. Gulfam, A. Ahmed, and A. Radwan, "Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things," *IEEE Access*, vol. 9, pp. 139739-139754, Oct. 2021, doi: 10.1109/ACCESS.2021.3118948

[104] Z. Abou El Houda, A.S. Hafid, and L. Khoukhi, "Cochain-SC: An intra-and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract," *IEEE Access*, vol. 7, pp. 98893-98907, Jul. 2019, doi: 10.1109/ACCESS.2019.2930715

[105] Z. Abou El Houda, A.S. Hafid, and L. Khoukhi, "Mitfed: A privacy preserving collaborative network attack mitigation framework based on federated learning using sdn and blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 4, pp. 1985-2001, Jan. 2023, doi: 10.1109/TNSE.2023.3237367

[106] I. Aliyu, M.C. Feliciano, S. Van Engelenburg, D.O. Kim, and C.G. Lim, "A blockchain-based federated forest for SDN-enabled in-vehicle network intrusion detection system," *IEEE Access*, vol. 9, pp. 102593-102608, Jul. 2021, doi: 10.1109/ACCESS.2021.3094365

[107] I.H. Abdulqadder, S. Zhou, I.T. Aziz, D. Zou, X. Deng, and S.M.A. Akber, "An effective lightweight intrusion detection system with blockchain to mitigate attacks in SDN/NFV enabled cloud," in *Proc. 2021 6th Int. Conf. Convergence Technol. (I2CT)*, Maharashtra, India: IEEE, Apr. 2021, pp. 1-8, doi: 10.1109/I2CT51068.2021.9417961

[108] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M.A. Ferrag, M. Mukherjee, and F.A. Khan, "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, Jul. 2019, Art. no. 3119, doi: 10.3390/s19143119

[109] E. Fenil, and P. Mohan Kumar, "ShChain_3D-ResNet: Sharding Blockchain with 3D-Residual Network (3D-ResNet) Deep Learning Model for Classifying DDoS Attack in Software Defined Network," *Symmetry*, vol. 14, no. 6, Jun. 2022, Art. no. 1254, doi: 10.3390/sym14061254

[110] M. Pourvahab, and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," *IEEE Access*, vol. 7, pp. 99573-99588, Jul. 2019, doi: 10.1109/ACCESS.2019.2930345

[111] I.H. Abdulqadder, S. Zhou, D. Zou, I.T. Aziz, and S.M.A. Akber, "Bloc-sec: Blockchain-based lightweight security architecture for 5G/B5G enabled SDN/NFV cloud of IoT," in *Proc. 2020 IEEE 20th Int. Conf. on Commun. Technol. (ICCT)*, Nanning, China: IEEE, Dec. 2020, pp. 499-507, doi: 10.1109/ICCT50939.2020.9295823

[112] A. Finogeev, M. Deev, D. Parygin, and A. Finogeev, "Intelligent SDN Architecture With Fuzzy Neural Network and Blockchain for Monitoring Critical Events," *Appl. Artificial Intell.*, vol. 36, no. 1, Nov. 2022, Art. no. 2145634 doi: 10.1080/08839514.2022.2145634

[113] Z. Abou El Houda, A. Hafid, and L. Khoukhi, "Brainchain-a machine learning approach for protecting blockchain applications using sdn", in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dublin, Ireland: IEEE, Jun. 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148808

[114] S. Rathore, B.W. Kwon, and J.H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *J. Netw. Comput. Appl.*, vol. 143, pp. 167-177, Oct. 2019, doi: 10.1016/j.jnca.2019.06.019

[115] P. Kumar, R. Kumar, A. Kumar, A.A. Franklin, and A. Jolfaei, "Blockchain and deep learning empowered secure data sharing framework for softwarized UAVs," in *Proc. 2022 IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Seoul, Korea: IEEE, May. 2022, pp. 770 - 775, doi: 10.1109/ICCWorkshops53468.2022.9814485

[116] R. Jmal, W. Ghabri, R. Guesmi, B.M. Alshammari, A.S. Alshammari, and H. Alsaif, "Distributed Blockchain-SDN Secure IoT System Based on ANN to Mitigate DDoS Attacks," *Appl. Sci.*, vol. 13, no. 8, Apr. 2023, Art. no. 4953, doi: 10.3390/app13084953

[117] R. Kumar, P. Kumar, A. Kumar, A.A. Franklin, and A. Jolfaei, "Blockchain and deep learning for cyber threat-hunting in software-defined industrial IoT," in *Proc. 2022 IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Seoul, Korea: IEEE, May. 2022, pp. 776-781, doi: 10.1109/ICCWorkshops53468.2022.9814706

[118] I.H. Abdulqadder, D. Zou, and I.T. Aziz, "The DAG blockchain: A secure edge assisted honeypot for attack detection and multi-controller based load balancing in SDN 5G," *Future Generation Comput. Syst.*, vol. 141, pp. 339-354, Apr. 2023, doi: 10.1016/j.future.2022.11.008

[119] J. Arshad, M.A. Azad, M. Mahmoud Abdellatif, M.H. Ur Rehman, and K. Salah, "COLIDE: A collaborative intrusion detection framework for Internet of Things," *IET Netw.*, vol. *8*, no. 1, pp. 3-14, Jan. 2019, doi: 10.1049/iet-net.2018.5036

[120] P.A.D.S.N. Wijesekara, "Blockchain and Artificial Intelligence for Big Data Analytics in Networking: Leading-edge Frameworks," *J. Eng. Sci. Technol. Rev.*, vol. 17, no. 3, pp. 125-143, May 2024, doi: 10.25103/jestr.173.16

[121] M.H. Bhuyan, D.K. Bhattacharyya, and J.K. Kalita, "Network anomaly detection: methods, systems and tools," *IEEE Commun. Surveys Tutorials*, vol. *16*, no. 1, pp. 303-336, Jun. 2013, doi: 10.1109/SURV.2013.052213.00046

[122] P.A.D.S.N. Wijesekara, "Load Balancing in Blockchain Networks: A Survey," *Int. J. Electr. Electron. Eng. Telecommun.*, vol. 13, no. 4, pp. 260-276, Jul. 2024, doi: 10.18178/ijeetc.13.4.260-276

[123] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for IoT devices," *IEEE Internet Things J.*, vol. *8*, no. 3, pp. 1817-1829, Aug. 2020, doi: 10.1109/JIOT.2020.3017377

[124] P.A.D.S.N. Wijesekara, "Network Virtualization Utilizing Blockchain: A Review" *J. Appl. Research Electr. Eng.*, vol. 3, no. 2, pp. 136-158, Oct. 2024, doi: 10.22055/jaree.2024.46144.1110

[125] D. Puthal, S.P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-authentication for scalable blockchain in resource-constrained distributed systems," in *Proc. 2019 IEEE Int. Conf. Consum. Electron. (ICCE),* Las Vegas, USA: IEEE*,* Jan. 2019, pp. 1-5, doi: 10.1109/ICCE.2019.8662009

[126] P.A.D.S.N. Wijesekara, W.M.A.K. Sangeeth, H.S.C. Perera, and N.D. Jayasundere, "Underwater Acoustic Digital Communication Channel for an UROV," in *Proc. 5th Annu. Research Symp. (ARS2018)*, Hapugala, Sri Lanka: University of Ruhuna, Jan. 2018, Art. no. E17.

[127] G. Yang, H. Jin, M. Kang, G.J. Moon, and C. Yoo, "Network monitoring for SDN virtual networks," In *IEEE INFOCOM 2020-Conf. Comput. Commun.*, Toronto, Canada: IEEE, Jul. 2020, pp. 1261-1270, doi: 10.1109/INFOCOM41043.2020.9155260

[128] H. Hasanova, U.J. Baek, M.G. Shin, K. Cho, and M.S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *Int. J. Netw. Manage.*, vol. *29*, no. 2, Mar. 2019, Art. no. e2060, doi: 10.1002/nem.2060

[129] C. Seneviratne, P.A.D.S.N. Wijesekara, and H. Leung, "Performance analysis of distributed estimation for data fusion using a statistical approach in smart grid noisy wireless sensor networks," *Sensors*, vol. 20, no. 2, Jan. 2020, Art. no. 567, doi: 10.3390/s20020567

[130] J. Marchang, G. Ibbotson, and P. Wheway, "Will blockchain technology become a reality in sensor networks?," in *Proc. 2019 Wireless Days (WD)*, Manchester, UK: IEEE, Apr. 2019, pp. 1-4, doi: 10.1109/WD.2019.8734268

[131] L. Yang, Y. Song, S. Gao, A. Hu, and B. Xiao, "Griffin: Real-time network intrusion detection system via ensemble of autoencoder in SDN," *IEEE Trans. Netw. Serv. Man.*, vol. *19*, no. 3, pp. 2269-2281.

[132] A. Alkhamisi, I. Katib, and S.M. Buhari, "Blockchain-Based Control Plane Attack Detection Mechanisms for Multi-Controller Software-Defined Networks," *Electronics*, vol. *13*, no. 12, Jun. 2024, Art. no. 2279, doi: 10.3390/electronics13122279

[133] P. Ramadass, R. shree Sekar, S. Srinivasan, S.K. Mathivanan, B.D. Shivahare, S. Mallik, N. Ahmad, and W. Ghribi, "BSDN-HMTD: A blockchain supported SDN framework for detecting DDoS attacks using deep learning method," *Egyptian Informat. J.*, vol. *27*, Sep. 2024, Art. no. 100515, doi: 10.1016/j.eij.2024.100515

[134] W.S. Khorseed, and A.H. Hamad, "Inter and Intra Domain DDoS Attack Mitigation for Software Defined Network Based on Hyperledger Fabric Blockchain Technology," *Ingén. Sys. d'Inform.*, vol. *29*, no. 1, pp. 301-311, Feb. 2024, doi: 10.18280/isi.290130

[135] M. Fartitchou, I. Lamaakal, Y. Maleh, K. El Makkaoui, Z. El Allali, P. Pławiak, F. Alblehai, and A. A. Abd El-Latif, "IOTASDN: IOTA 2.0 smart contracts for securing software-defined networking ecosystem," *Sensors*, vol. *24*, no. 17, Sep. 2024, Art. no. 5716, doi: 10.3390/s24175716

[136] P.P. Pawar, D. Kumar, B. Ananthan, A.S. Pradeepa, and A.S. Selvi, "An efficient ddos attack detection using attention based hybrid model in blockchain based SDN-IOT," in *Proc. 2024 3rd Int. Conf. Artificial Intell. Internet Things (AIIoT)*, Vellore, India: IEEE, May 2024, pp. 1-5, doi: 10.1109/AIIoT58432.2024.10574596

[137] V. Bachani, and A. Bhattacharjya, "Preferential delegated proof of stake (PDPoS)—modified DPoS with two layers towards scalability and higher TPS," *Symmetry*, vol. *15*, no. 1, Dec. 2022, Art. no. 4, doi: 10.3390/sym15010004

[138] S.R. Khonde, and V. Ulagamuthalvi, "Hybrid intrusion detection system using blockchain framework," *EURASIP J. Wireless Commun. Netw.*, vol. *2022*, no. 1, Jun. 2022, doi: 10.1186/s13638-022-02089-4

[139] X. Cai, S. Geng, J. Zhang, D. Wu, Z. Cui, W. Zhang, and J. Chen, "A sharding scheme-based many-objective optimization algorithm for enhancing security in blockchain-enabled industrial internet of things," *IEEE Trans. Ind. Informat.*, vol. *17*, no. 11, pp. 7650-7658, Jan. 2021, doi: 10.1109/TII.2021.3051607

[140] B. Hu, C. Zhou, Y.C. Tian, Y. Qin, and X. Junping, "A collaborative intrusion detection approach using blockchain for multimicrogrid systems," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. *49*, no. 8, pp. 1720-1730, Apr. 2019, doi: 10.1109/TSMC.2019.2911548

[141] A. Heidari, N.J. Navimipour, and M. Unal, "A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones," *IEEE Internet Things J.*, vol. *10*, no. 10, pp. 8445-8454, Jan. 2023, doi: 10.1109/JIOT.2023.3237661

[142] S. Algarni, F. Eassa, K. Almarhabi, A. Algarni, and A. Albeshri, "BCNBI: A blockchain-based security framework for northbound interface in software-defined networking," *Electronics*, vol. *11*, no. 7, Mar. 2022, Art. no. 996, doi: 10.3390/electronics11070996