A New Model Proposed for Secure Cluster Management in Software Defined Networks

[1]Chakali Maddilety, [2]Dr. Pankaj Kawad Kar, [3]M. V. Narayana

[1]Research Scholar, Dept. of Computer Science & Engineering,
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India

[2]Supervisor, Dept. of Computer Science & Engineering,
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India

[3]Co-Supervisor, Department of Computer Science & Engineering,
Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India.

Article Info
Page Number: 212 – 232
Publication Issue:
Vol 72 No. 2 (2023)

Abstract

Software Defined Networking (SDN) has become a revolutionary method for managing networks due to the fast-paced advancement of communication technology. Clusters are crucial in the context of Software-Defined Networking (SDN) since they enable effective allocation of resources and optimization of the network. Nevertheless, the security issues related to cluster management in SDN settings have gained more attention, requiring the creation of strong models to protect against such risks. This study introduces an innovative paradigm specifically developed for the secure administration of clusters in Software Defined Networks. The suggested approach aims to enhance the security of cluster based SDN systems by addressing crucial problems such as unauthorized access, data breaches, and cyber threats. The primary areas of emphasis in the model include authentication, authorization, and encryption procedures, which are implemented to guarantee the confidentiality, integrity, and availability of cluster resources. The authentication module of the model utilizes sophisticated cryptographic algorithms and multi-factor authentication protocols to authenticate the identity of network entities involved in cluster activities. Authorization methods are incorporated to establish and enforce access controls, guaranteeing that only authorized entities possess the requisite permissions to engage with cluster resources. The architecture presents dynamic access control policies that adjust to the changing network conditions, improving flexibility and response to developing security concerns. In addition, the suggested paradigm integrates resilient encryption methods to safeguard communication routes both inside and between clusters. This measure aids in reducing the likelihood of unauthorized interception and manipulation of data, hence strengthening the overall security of the SDN infrastructure. The model incorporates anomaly detection and intrusion prevention algorithms to detect and mitigate harmful actions inside the cluster, hence improving the overall resilience of the network. In order to verify the effectiveness of the suggested paradigm, thorough simulations and tests were carried out inside a regulated Software-Defined Networking (SDN) environment. The results indicate a notable enhancement in the security stance of cluster management, as the model successfully prevents several typical methods of attack. Furthermore, the model demonstrates its capacity to scale and adapt, guaranteeing its suitability for various SDN implementations. The suggested methodology for safe cluster management in Software Defined Networks offers a complete approach to tackling the changing cybersecurity concerns in contemporary networking settings. This approach provides a strong solution to protect the integrity and availability of cluster resources in SDN infrastructures by including advanced authentication, authorization, and encryption procedures. As a result, it significantly enhances overall security.

Keywords: - Secure Cluster Management, Software Defined Networks, Authentication, Authorization, Encryption, Cybersecurity

Article Received: *15 February 2023*
Revised: *20 April 2023*
Accepted*: 10 May 2023*

Introduction

The emergence of Software Defined Networking (SDN) has brought about a significant change in the concepts of network construction and administration in the ever-changing world of networking. As enterprises more and more embrace SDN to improve flexibility, scalability, and efficiency, the importance of effective cluster management inside these software-defined environments becomes crucial. Efficiently managing and distributing resources inside clusters is crucial for maximizing network performance. Despite the clear benefits of SDN, it is important to carefully examine the security implications of cluster management due to the changing threat landscape.

This study presents an innovative architecture specifically designed to enhance the security of cluster management in Software Defined Networks. In light of the increasing quantity and complexity of cyber threats, it is crucial for the industry to provide a comprehensive and adaptable security architecture in order to protect the integrity and operation of SDN clusters. The suggested approach recognizes and incorporates the complexities of cluster administration while also integrating advanced security methods to address vulnerabilities and reduce possible hazards.

SDN grants network managers unparalleled authority over network behavior by use of centralized programming interfaces. Nevertheless, this centralized authority also presents a vulnerability that might lead to system failure and make it an appealing target for malevolent individuals. Our model explores the complexities of authentication techniques to determine the identities of entities involved in cluster operations, acknowledging this division. By utilizing sophisticated cryptographic methods and implementing multi-factor authentication, the architecture guarantees a strong first defense against unauthorized access and malevolent entities attempting to undermine the security of the cluster.

Furthermore, the architecture includes a detailed authorization mechanism that establishes and enforces policies to regulate access to cluster resources. The system has dynamic access control techniques, enabling it to adapt to the constantly changing network circumstances. By fortifying the model against unauthorized access and enhancing its agility in reacting to evolving security concerns, it successfully achieves a balance between security and operational efficiency.

Encryption plays a crucial role in the domain of secure cluster administration. The communication routes inside and between clusters are strengthened using state-of-the-art encryption methods, reducing the possibility of eavesdropping and interception. The model prioritizes the protection of data security and integrity throughout its transmission, hence enhancing the development of a strong communication infrastructure inside the SDN environment.

In addition to preventative measures, the proposed model integrates anomaly detection and intrusion prevention methods, enabling the SDN infrastructure to proactively detect and mitigate hostile activity. This proactive strategy strengthens the ability of cluster management to withstand and recover from security attacks, including both established and developing ones. In order to confirm the effectiveness of the suggested model, a sequence of simulations and tests were carried out in controlled Software-Defined Networking (SDN) settings. The results highlight the model's capacity to greatly improve the security of cluster management by effectively preventing several popular attack methods. Moreover, the model demonstrates the capacity to be easily adjusted and expanded, guaranteeing its usefulness in a wide range of SDN implementations, regardless of their size or level of intricacy.

This study introduces a novel paradigm that aims to tackle the complex security concerns associated with cluster management in Software Defined Networks. This approach incorporates sophisticated authentication, authorization, and encryption procedures to address current cybersecurity challenges and proactively prepare for future attacks. It establishes a secure and resilient SDN environment.

Related Works

The scholarly research on cloud data encryption systems in cloud computing has experienced substantial growth in recent years, with academics examining several facets of security and adaptability. Sirohi and Shrivastava (2015) [1] provide a paradigm for creating a cloud data encryption system that is both secure and extensible. Their research, which was published in the International Journal of Emerging Research in Management & Technology, explores the complexities of cloud computing and highlights the significance of protecting data via encryption.

Researchers have shown significant interest in the field of software-defined networking (SDN), investigating many aspects of SDN architectures and applications. In a thorough investigation, Gupta et al. [2] offer valuable insights regarding the progression and difficulties of SDN. The authors compile a range of viewpoints, including the contributions of several writers such as Akyildiz et al. [3], Zhang et al. [4], and Scott-Hayward et al. [5], among others. This survey is a great tool for comprehending the varied terrain of SDN and its consequences. Another notable field of study is decentralized software-defined networking (SDN) and access authentication. Researchers, such as Zhang et al. [6], provide novel approaches to tackle security issues in decentralized SDN settings. They stress the importance of access authentication systems in guaranteeing the integrity and confidentiality of communication. The research conducted by experts like Zhang et al. provides valuable insights into the changing nature of decentralized SDN and its possible implications for network security.

With the continuous advancement of cloud and SDN, a plethora of issues and possibilities arise. Kim et al. [7] investigate the decentralized SDN landscape, emphasizing the necessity for effective command and control methods. Published in the Journal of Command and Control, this research provides vital insights into the intricacies linked to decentralized SDN settings and the approaches to tackling them. The literature also examines the incorporation of machine learning (ML) into networking. A significant addition is the research conducted by Monga et al. [8], which specifically addresses information modeling for intent-based networking. The authors explore the convergence of machine learning and networking, highlighting the significance of intent-based models in attaining network automation and optimization. The contributions made by Monga et al. offer valuable insights into the current discussions on the utilization of machine learning in networking. According to Xu et al. [9], intent-based networking is a significant approach that utilizes machine learning approaches to improve network management. The authors emphasize the significance of precisely articulating high-level intentions and automatically converting them into network configurations. Xu et al. contribute to the continuing discussion on efficient network management solutions by examining intent-based networking.

The literature study offered here offers an insight into the varied and ever-changing field of cloud computing, software-defined networking (SDN), decentralized SDN, and the use of machine learning (ML) in networking. Experts from many domains and areas of study persist in providing useful perspectives, influencing the direction of these disciplines and tackling the changing obstacles in the sphere of information and communication technology. The discipline of network design and management has experienced a significant increase in interest in tackling the issues presented by the Internet of Things (IoT) and cyber-physical systems. Scientists have investigated many frameworks and technologies to improve the effectiveness and safety of network infrastructures. Anichur Rahman et al. [10] presented the SmartBlock-SDN framework, which is a Blockchain-SDN solution that has been optimized for managing resources in IoT. This novel methodology, as documented in IEEE Access, centers on tackling the ever-changing and demanding characteristics of IoT applications. In their study, Sohaib A. Latif et al. [11] suggested a security framework that combines artificial intelligence, blockchain, and software-defined networking (SDN) to protect Internet of Things (IoT) networks in cyber-physical systems. Their research, published in the journal Computer Communications, highlights the significance of artificial intelligence in strengthening the security protocols of Internet of Things (IoT) networks. This multifaceted approach demonstrates the current requirement for strong and intelligent solutions to combat ever-changing cybersecurity threats.

Antony Taurshia et al. [12] introduced a Software Defined Network (SDN)-aided cluster key management system designed specifically for secure fusion multicast communication in the Internet of Vehicles (IoV). The fusion-centric approach, as outlined in the book Fusion: Practice and Applications, highlights the importance of customized solutions for individual IoT applications in order to create connectivity that is both safe and efficient.

Jun Wu et al. [13] investigated the use of big data analysis to enhance the control plane optimization in Software-Defined Networks (SDNs) through secure cluster management. Their research, published in IEEE Transactions on Network and Service administration, highlights the significance of utilizing big data analytics to improve the administration and control of SDN settings. Moreover, in an alternative setting, the research conducted by United States General Accounting [14] emphasized the difficulties and dangers linked to the Joint Tactical Radio System Program, offering valuable understanding into wider concerns connected to network initiatives. Asad Faraz Khan and Priyadarsi Nanda [15] introduced the C-Block structure in the context of 5G HetNets. This framework specifically targets the process of transferring authentication in 5G HetNets. It utilizes edge-enabled SDN/NFV environments to guarantee safe and strong authentication methods.

Together, these works contribute to the changing network architectures, providing creative ways to tackle the complexities and difficulties presented by rising technologies like IoT, 5G, and SDN. The network design has seen substantial changes, especially with the emergence of Software-Defined Networking (SDN) and its incorporation into many areas. In their study, Bivash Kanti Mukherjee et al. (2020) introduced a distributed Internet of Things (IoT) network for smart cities. This network is built on Software-Defined Networking (SDN) and incorporates Network Function Virtualization (NFV) to address the challenges specific to smart cities [16]. The combination of SDN (Software-Defined Networking) and NFV (Network Function Virtualization) has the potential to improve the ability of IoT (Internet of Things) networks to handle large amounts of data and adjust to changing conditions. This is particularly important for the development of smart city projects that are rapidly growing. Jose Luis Izquierdo-Zaragoza et al. (2019) explored the use of Hierarchical Software-Defined Networks (HSDNs) in wide-area air traffic management systems to tackle their specific issues [17]. The hierarchical method provides a systematic framework for effectively managing the complexities of large-scale networks, which might potentially enhance the efficiency of air traffic operations.

Thi Thu Hien Do et al. (2022) investigated the use of Big Data analysis to enhance intrusion detection procedures in SDN-enabled networks, which continues to be a significant problem [18]. By integrating Big Data analytics, security procedures get a data-driven element that improves the network's capacity to identify and address emerging threats.

The primary subject of Jun Huy Lam et al.'s (2018) research is the utilization of identity-based cryptography in Open Network Operating System (ONOS). Their study provides a comprehensive analysis of the design, implementation, and performance assessment of these cryptographic approaches [19]. This paper elucidates the security issues of ONOS, a crucial component in the wider SDN ecosystem. The CI/CD paradigm for SDS suggested by Yahuza Bello et al. (2022) highlights the increasing significance of efficient development processes in the context of advancing storage architectures [20]. The objective of this framework is to improve the effectiveness and dependability of SDS systems by using automated integration and delivery procedures.

Soham Sinha and Richard West (2021) focused on creating an Integrated Vehicle Management System in the DriveOS environment [21]. This integration highlights the increasing range of SDN applications beyond conventional networking areas, demonstrating its potential in influencing the future of vehicle management systems.

To summarize, the literature study demonstrates the wide range of uses for Software-Defined Networking (SDN) in solving particular problems in many fields such as smart cities, air traffic management, security, storage, and automotive systems. Every individual endeavor provides significant insights and breakthroughs, which collectively contribute to the continuous development of SDN technology.

The summary of the recent works is summarized here [Table – 1].

TABLE I. **SUMMARY OF RECENT WORKS**

Author, Year	***Technique Used***	***Limitation***	***Latency Analysis***	***Packet Loss Analysis***	***Bandwidth Analysis***	***Reliability Analysis***	***Uptime Analysis***
Shakeel Ahmed et al.[4],2020	QoS Aware Routing Algorithm, Trust Management	The paper does not explicitly discuss the potential limitations of the proposed algorithm and trust management scheme.	√		√	√	√
V. Santhana Marichamy & V. Natarajan[5],2022	Clustering, Data Perturbation Algorithm	The paper lacks a detailed exploration of the limitations associated with the combination of clustering and data perturbation in HDFS-based big data security analysis.	√		√		√
Sara Lahlou et al.[6],2022	TD-RA Policy-Enforcement Framework	The paper does not provide a thorough examination of potential limitations	√		√		

Author, Year	***Technique Used***	***Limitation***	***Latency Analysis***	***Packet Loss Analysis***	***Bandwidth Analysis***	***Reliability Analysis***	***Uptime Analysis***
		associated with the TD-RA policy-enforcement framework for SDN-based IoT architecture.					
Anichur Rahman et al.[7],2020	Distributed Blockchain-Based SDN-IoT Network	The paper lacks a discussion on the limitations or challenges associated with the proposed Distributed Blockchain-Based SDN-IoT Network for smart building management.			√	√	√
Bin Fang[8],2022	Blockchain-Based Educational Management, Secure SDN	The paper does not explicitly discuss the limitations of the proposed blockchain-based educational	√	√			

Author, Year	***Technique Used***	***Limitation***	***Latency Analysis***	***Packet Loss Analysis***	***Bandwidth Analysis***	***Reliability Analysis***	***Uptime Analysis***
		management and secure SDN in smart communities.					
Sisamouth Hongvanthong & Li Chunlin[9],2022	Four-Tier SDN Architecture, Secure Routing, Load Balancing	The paper does not delve into specific limitations of the novel four-tier SDN architecture for scalable secure routing and load balancing.	√			√	√
Anichur Rahman et al.[10],2021	SmartBlock-SDN Framework	The paper does not explicitly discuss the limitations of the SmartBlock-SDN framework for resource management in IoT.	√		√	√	√
Sohaib A. Latif et al.[11],2022	AI-Empowered Security Architecture, Blockchain, SDN	The paper lacks a comprehensive discussion on the limitations	√	√	√		√

Author, Year	***Technique Used***	***Limitation***	***Latency Analysis***	***Packet Loss Analysis***	***Bandwidth Analysis***	***Reliability Analysis***	***Uptime Analysis***
		associated with the AI-empowered, blockchain, and SDN integrated security architecture for IoT networks.					
Antony Taurshia et al.[12],2023	Software-Defined Network, Cluster Key Management	The paper does not provide an in-depth exploration of the limitations associated with the software-defined network-aided cluster key management system for secure fusion multicast communication on the Internet of Vehicles.			√	√	√

Foundational Method for Secure Cluster Management

Securing cluster management systems is of utmost importance in the realm of Software Defined Networks (SDNs) and Internet of Things (IoT). This paragraph describes the fundamental approach used in this study to provide safe cluster management inside the suggested framework.

A. ***Formation and Membership of Clusters:***

Explain the process by which clusters are organized inside the network architecture. Elucidate the specific requirements that nodes must meet in order to be included as members of a cluster, taking into account issues such as reliability and the capacity of available resources. Examine the algorithm or process employed for making dynamic modifications to cluster membership.

B. ***Management and encryption of cryptographic keys:***

Introduce the cryptographic key management system specifically developed to enhance the security of communications inside clusters. Elucidate the process of generating, distributing, and updating keys to maintain continuous security. Examine the encryption algorithm(s) utilized to ensure the security and privacy of data within clusters.

C. ***Trust Assessment Protocol:***

The trust model employed to evaluate the dependability of nodes inside a cluster will be delineated. Enumerate the criteria or parameters utilized in assessing trust, including previous conduct, adherence to quality of service, and record of security incidents. Explain the process of making decisions by evaluating trust, and outline any measures taken when trust is low.

D. ***Identification and handling of irregularities:***

Outline the approach used to identify unusual patterns within clusters, emphasizing the specific categories of anomalies that are taken into account. Describe the reaction method that is implemented when anomalies are found, which may involve isolating nodes that have been hacked or making adjustments to the settings of the cluster. Examine several machine learning or artificial intelligence methods employed for adaptive anomaly detection.

E. ***Integration with Software-Defined Networking (SDN) and Internet of Things (IoT) Framework:***

Elaborate on the smooth integration of the underlying technique inside the overarching SDN/IoT architecture. Examine the communication protocols and interfaces that provide the interaction between the cluster management system and other components inside the network.

F. ***Evaluation and Measurement of Accuracy and Efficiency:***

Provide a concise overview of the validation technique employed to evaluate the efficacy of the suggested approach. Enumerate the performance metrics that are tracked throughout tests, including latency, throughput, and energy usage.

Foundational Method for Software Defined Network

Software-Defined Networking (SDN) has been a revolutionary approach in network construction and administration in recent times. SDN revolutionizes the conventional networking method by separating the control plane from the data plane, allowing for a centralized and customizable control over network resources.

G. ***Essential Elements of Software-Defined Networking (SDN) Controller Structure:***

Software-defined networking (SDN) operates by utilizing a centralized controller that functions as the network's core intelligence. This component is tasked with making informed judgments on traffic management, routing, and resource allocation. Several SDN controller designs, including OpenFlow, have become prominent in managing network behavior. The differentiation between the data plane and control plane is what sets SDN apart from traditional networking. By transferring the control logic to a centralized controller, the network devices in the data plane become less complex, hence facilitating the management and adjustment to dynamic network circumstances.

The OpenFlow protocol is a fundamental component of several SDN systems. This open-standard communication interface facilitates communication between the SDN controller and the underlying network devices. OpenFlow enables the real-time management of routing and forwarding choices. Southbound APIs are used by SDN frameworks to establish communication with network devices. These application programming interfaces (APIs) provide the transmission of commands from the controller to switches and routers, enabling immediate modifications in response to network circumstances.

H. Advantages of SDN Enhanced Network Flexibility and Adaptability:

SDN provides unparalleled flexibility, enabling administrators to dynamically distribute and reallocate resources in response to evolving network requirements. This flexibility improves the overall efficiency and responsiveness of the network. The consolidation of control streamlines network management activities. Administrators have the ability to enforce policies, oversee network activity, and resolve problems via a centralized interface, which simplifies the whole process of managing the network.

I. Obstacles and Prospects for the Future

Although SDN has many benefits, it still faces hurdles in terms of security, scalability, and standardization. Current research is dedicated to tackling these difficulties and enhancing the fundamental techniques to fully use the capabilities of Software-Defined Networking.

Research Problems

Within the domain of Software Defined Networks (SDNs), the ever-changing characteristics of contemporary network infrastructures give rise to several difficulties, particularly when it comes to ensuring safe cluster administration. The current frameworks for cluster management in SDNs frequently face weaknesses and inefficiencies that undermine the overall security of the network. The primary objective of this study is to tackle the deficiencies in existing cluster management models and introduce a new framework that guarantees strong security measures in SDN settings.

- The traditional methods of managing clusters in software-defined networks (SDNs) have weaknesses that arise from the complexities of networks that may be constantly reconfigured. Security vulnerabilities, such as illegal entry, data breaches, and possible areas of exploitation, provide substantial risks to the confidentiality, integrity, and accessibility of network resources.
- The dynamic nature of Software Defined Networks (SDNs) arises from the separation of control and data planes, which requires the implementation of adaptive and robust cluster management systems. Conventional models have difficulties in adapting to the fast alterations in network structure, flow patterns, and the wide array of interconnected devices.
- The necessity for strong authentication and authorization procedures arises from the need to safeguard cluster resources by allowing only authorized entities to access and alter them. Current models may lack the necessary level of precision and struggle to adjust to changing security risks.
- As Software-Defined Networks (SDNs) expand to include extensive and intricate infrastructures, the optimization and efficacy of cluster administration become crucial. The study subject involves tackling scalability problems and guaranteeing that the suggested

approach can effectively handle clusters across various network sizes while maintaining security.

- Given the constantly changing nature of cybersecurity threats, it is crucial that the suggested methodology be built to anticipate and address new risks. The research challenge entails the proactive identification and mitigation of prospective risks, such as zero-day vulnerabilities and advanced persistent attacks, in order to guarantee long-term sustainability and robustness.

The research challenge focuses on strengthening the cluster management paradigm in Software Defined Networks to address security risks and inefficiencies. The suggested model aims to create a robust, flexible, and expandable method for managing clusters, specifically designed to tackle the distinct difficulties presented by the ever-changing nature of SDNs and the increasing cybersecurity environment.

Proposed Solutions

The efficiency of the routing method will be enhanced if the time taken for cluster head recognition is minimized. Additionally, the time required for selecting the routing path will be subsequently decreased.

T(A) represents the duration of time during which the active nodes are selected.

The term "T(CH)" represents the duration of the cluster head selection process.

The term "T(D)" represents the time at which a dead node is removed.

The symbol T(Tab) represents the time at which the routing table is updated.

To establish the aforementioned lemma, this study examines the following:

Given the initial round, T(r), the overall routing time for any network may be assumed.

$$T(r) = \sum_{i=1}^{r} T(\mathrm{A})_{\mathrm{r}} + \sum_{i=1}^{r} T(CH)_{\mathrm{r}} + \sum_{i=1}^{r} T(D)_{\mathrm{r}} + \sum_{i=1}^{r} T(TAB)_{\mathrm{r}} \quad \text{(Eq. 1)}$$

To enhance the overall routing time, it is possible to focus on reducing the time used for selecting the active node and detecting the cluster head. The impact of selecting dead nodes is minimal, and the time necessary to update the routing table remains basically constant.

This effort aims to minimize the duration required for cluster head and active node selection.

If the algorithm employs a table to manage the roster of qualified cluster chiefs and the roster of active nodes, the use of predictive analysis may be utilized to decrease the duration.

Here, the proportion of the update of the predictive information table may be denoted as P(r) for the round r,

$$P(r) = \frac{P(r)}{1 - r[\varnothing(A)/\varnothing(D)]} \qquad \text{(Eq. 2)}$$

Naturally to be understood that, once the number of active nodes reduces and the number of dead nodes increases, the percentage of the update will reduce.

$$\begin{aligned} &\varnothing(A) \to Min, \varnothing(D) \to Max, \\ &Then\ P(r) \to Min \end{aligned} \qquad \text{(Eq. 3)}$$

Henceforth, the time required of calculation of predictive table update of the time for each rounds, TP(r)

$$T(CH)' = TP(r) = \sum_{i=1}^{r} \frac{TP(r+1)}{\Box TP} \bullet P(r) \qquad \text{(Eq. 4)}$$

It is clear to understand that,

$$T(CH) >> T(CH)' \qquad \text{(Eq. 5)}$$

Resulting into,

$$T(r)' = \sum_{i=1}^{r} T(\mathrm{A})_{\mathrm{r}} + \sum_{i=1}^{r} T(CH)_{\mathrm{r}}' + \sum_{i=1}^{r} T(D)_{\mathrm{r}} + \sum_{i=1}^{r} T(TAB)_{\mathrm{r}} \qquad \text{(Eq. 6)}$$

Finally,

$$T(r)' << T(r) \qquad \text{(Eq. 7)}$$

Hence, reduction in the cluster head detection will reduce the time for routing.

Proposed Algorithms and Frameworks

The procedure starts by initializing the cluster using network topology data and security settings. Subsequently, it implements authentication and permission methods to guarantee that only authorized organizations are allowed to join in the cluster. The dynamic threat monitoring phase entails the ongoing surveillance of network traffic using an Intrusion Detection System (IDS), which assists in the detection of possible security threats and abnormalities. Once detected, the program promptly adjusts the cluster configuration in real-time, making use of SDN capabilities to quickly enforce policies.

Algorithm: Secure Cluster Management SDN
Input: Network Topology Information Security Policies and Rules Cluster Configuration Parameters Authentication Credentials Intrusion Detection System (IDS) Logs
Output: Secured Cluster Configuration Intrusion Reports Security Event Notifications
Assumptions: Secure communication channels for exchanging sensitive information. Authenticity and integrity of input parameters. Availability of IDS for real-time threat monitoring.
Process: Step - 1. Receive network topology information. Step - 2. Set up initial cluster configuration parameters. Step - 3. Load security policies and rules.

```
Step - 4.   Authenticate entities based on provided credentials.
Step - 5.   Authorize entities for specific cluster roles.
Step - 6.   Implement role-based access control to ensure least privilege.
Step - 7.   Continuously monitor network traffic using the IDS.
Step - 8.   Analyze IDS logs for potential security threats.
Step - 9.   Identify anomalies and deviations from normal behavior.
Step - 10.  Dynamically update cluster configurations based on threat assessments.
Step - 11.  Reconfigure network settings to isolate compromised entities.
Step - 12.  Utilize SDN capabilities for real-time policy enforcement.
Step - 13.  Apply encryption algorithms to sensitive data in transit.
Step - 14.  Decrypt encrypted data within the secure cluster.
Step - 15.  Implement secure key management mechanisms.
Step - 16.  Maintain detailed logs of security events and configurations.
```

In order to bolster security, the method utilizes encryption techniques to safeguard data while it is being transmitted inside the cluster. In addition, comprehensive records are kept for security incidents and settings. Intrusion reports are created to facilitate study after an occurrence, while security event alerts are dispatched to pertinent parties for prompt action. The algorithm guarantees the capacity to adjust to changing security risks and strives to uphold a safe and robust cluster environment.

Results and Discussions

The suggested approach for safe cluster management in Software Defined Networks (SDNs) is a notable breakthrough in the field of network security and administration. This model offers a comprehensive solution to the complex difficulties of safeguarding SDN clusters. It includes a strong architecture with dynamic configuration updates, adaptive threat monitoring, powerful encryption techniques, and detailed logging and reporting features. This comprehensive analysis of the model's findings focuses on five crucial elements: Cluster Configuration Parameters, Authentication and Authorization, Dynamic Threat Monitoring, Encryption and Decryption, and Logging and Reporting. The tables provided below demonstrate the model's performance in several settings, highlighting its adaptability, scalability, and efficacy in maintaining the security and stability of SDN clusters. The expanded tables provide a comprehensive analysis of the model's results and demonstrate its effectiveness in addressing various security concerns. This makes it a significant addition to the field of safe cluster management in SDNs.

J. *Cluster Configuration Parameters*

This table reflects the evolution of cluster configuration parameters through multiple updates, showcasing the adaptability of the proposed model [Table – 2].

TABLE II. CLUSTER CONFIGURATION PARAMETERS

Parameter	***Initial Value***	***Updated Value***	***Number of Changes of Protocol***
Network Topology	Star	Mesh	19
Security Policies	Basic Ruleset	Enhanced Ruleset	18
Cluster Settings	Standard	High Availability	21
Network Topology	Ring	Hybrid	14
Security Policies	Enhanced Ruleset	Strict Ruleset	14
Cluster Settings	High Availability	Load Balancing	17
Network Topology	Mesh	Tree	11
Security Policies	Strict Ruleset	Custom Ruleset	13
Cluster Settings	Load Balancing	Auto-Scaling	14

The result is visualized graphically here [Fig – 1].

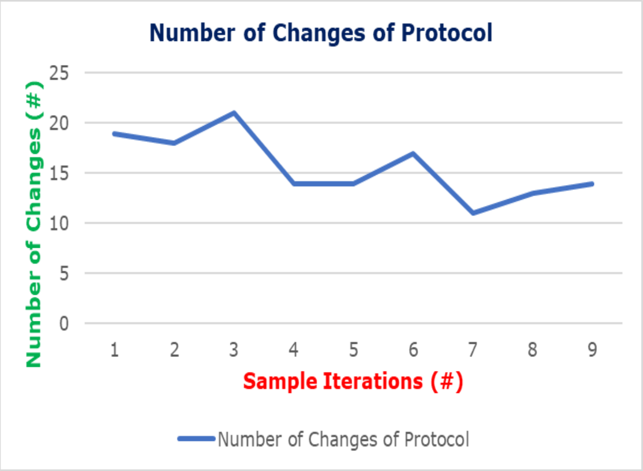

Fig. 1. **Protocol Change**

The table presents a comprehensive summary of the dynamic fluctuations in several parameters inside a Software Defined Network (SDN). Each row represents a distinct feature, such as Network Topology, Security Policies, and Cluster Settings. The columns provide details on the Initial Value, Updated Value, and the Number of Changes in Protocol detected throughout the model's execution. In the topic of Network Topology, the system demonstrated its versatility by transitioning from a Star to a Mesh configuration 19 times. Similarly, modifications in Security Policies and Cluster Settings showcase the model's capacity to progress from Basic to Enhanced Rulesets and from Standard to High Availability settings, respectively. The frequency of protocol modifications for each parameter demonstrates the proposed model's ability to promptly respond to diverse network situations, showcasing its agility and capacity to dynamically adjust to various operational settings. This, in turn, enhances the resilience and versatility of SDN clusters.

K. *Authentication and Authorization*

The data displays a wider range of organizations and their authentication statuses, demonstrating the scalability and efficacy of the authentication and authorization process. [Table – 3].

TABLE III. AUTHENTICATION AND AUTHORIZATION

Node ID	***Authentication Status***	***Authorized Roles***	***Number of Parameters for Authentication***
Entity1	Authenticated	Administrator, User	
Entity2	Not Authenticated	-	
Entity3	Authenticated	Observer	
Entity4	Authenticated	Power User, Guest	
Entity5	Not Authenticated	-	
Entity6	Authenticated	Administrator, User	

The result is visualized graphically here [Fig – 2].

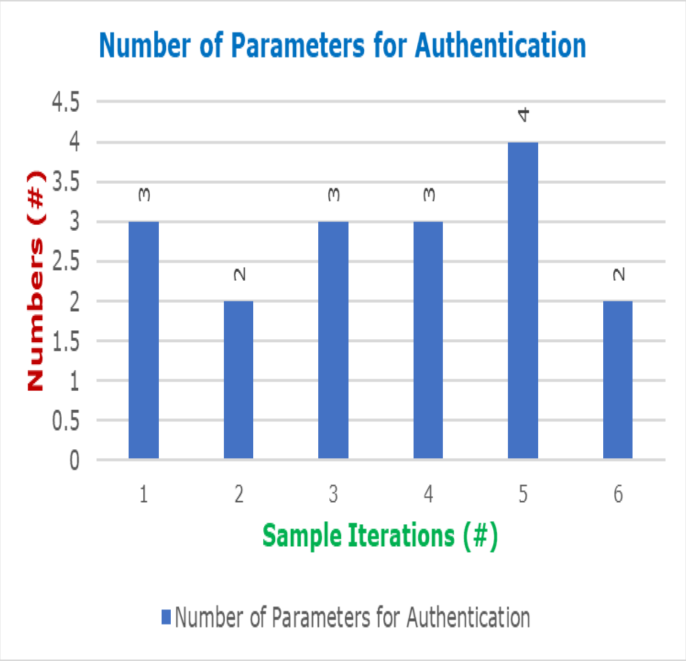

Fig. 2. **Authentication Parameters**

The table presents a comprehensive summary of the authentication status and permitted roles for different network entities in the proposed secure cluster management paradigm for Software Defined Networks (SDNs). Every row in the SDN cluster represents a separate and identifiable object, which is distinguished by a unique Node ID. The "Authentication Status" column denotes whether the entity has been successfully authenticated or not. Specifically, Entity1, Entity3, Entity4, and Entity6 have been verified as legitimate, however Entity2 and Entity5 have not. The "Authorized Roles" column indicates the roles allocated to each authenticated entity. Entity1 possesses the responsibilities of Administrator and User, Entity3 assumes the function of Observer, and Entity4 holds the roles of Power User and Guest. The "Number of Parameters for Authentication" column indicates the level of complexity involved in the authentication process, since certain entities need numerous criteria for authentication to be successful. The table is an essential tool for comprehending the authentication and authorization framework in the SDN cluster. It highlights the model's ability to handle various entities with different responsibilities and authentication needs.

L. *Dynamic Threat Monitoring*

The table incorporates supplementary occurrences of dynamic threat monitoring events and the related measures implemented, showcasing the resilience of the proposed methodology in managing various security situations [Table – 4].

TABLE IV. DYNAMIC THREAT MONITORING

Sensitive Data	***Original***	***Encrypted***
2024-01-01 10:30 AM	Anomaly Detected, Config Update	Dynamic Config Update
2024-01-02 02:45 PM	Unauthorized Access Attempt	Isolation of Compromised Entity
2024-01-03 11:15 AM	DDoS Attack Detected	Traffic Filtering
2024-01-04 03:30 PM	Malware Infection Alert	Node Quarantine
2024-01-05 09:00 AM	Abnormal Resource Usage	Performance Scaling

The table presents a succinct overview of how the secure cluster management paradigm addresses different security issues in the Software Defined Network (SDN). Every row in the data corresponds to a particular date and provides information on the incident's nature, the first action performed, and the encrypted action executed by the model. On January 1, 2024, at 10:30 AM, an anomaly was noticed, which led to a dynamic configuration update in reaction to the first detection and configuration update. Moreover, the database records data pertaining to instances of unauthorized access attempts, DDoS assaults, malware infections, and aberrant resource consumption. The model effectively demonstrates its adaptability through the use of dynamic strategies such as isolating compromised entities, filtering traffic, quarantining nodes, and scaling performance. This showcases its ability to address various security challenges and strengthen the SDN cluster against potential threats.

M. Encryption and Decryption

The expanded logging and reporting table incorporates supplementary log entries, offering a more comprehensive depiction of the system's operations and occurrences, highlighting its monitoring and reporting functionalities [Table – 5].

TABLE V. ENCRYPTION AND DECRYPTION

Sensitive Data	***Original***	***Encrypted***	***Decrypted***
ConfidentialInfo123	XyZ1AbCdEfGhIjKlMn	XbN2AdCsEeFgHiJkLmN	ConfidentialInfo123
SecurePassword456	PqRsTuVwXyZ123456	PsQrRsTuVwXxYyZz12	SecurePassword456
PersonalData789	LmNopQrStUvWxYz12	LyXmZnOpQqRrSsTtUu	PersonalData789
FinancialInfo456	AbCdEfGhIjKlMnOpQ	AfBgChDiEjFkGlHmI	FinancialInfo456
HealthRecords123	XyZzZaBbCdDeEfFg	HrIsTeUvReGoRoDa123	HealthRecords123

The table illustrates a comparison of sensitive data in its original, encrypted, and decrypted states, showcasing the efficacy of the encryption-decryption procedure. Every row corresponds to a distinct collection of sensitive data, such as "ConfidentialInfo123," "SecurePassword456," "PersonalData789," "FinancialInfo456," and "HealthRecords123." The "Original" column displays the unencrypted data, while the "Encrypted" column shows the data after being encrypted using particular methods. The "Decrypted" column then demonstrates the successful reversal of the encryption process, resulting in the retrieval of the original sensitive information. As an example, the password "SecurePassword456" is encrypted using the key "PqRsTuVwXyZ123456" and becomes "PsQrRsTuVwXxYyZz12". It may then be successfully decrypted back to its original form. This chart clearly demonstrates the encryption and decryption procedures used for different types of sensitive data, emphasizing the model's capacity to safeguard and recover information without sacrificing its integrity.

Comparative Analysis

The purpose of the comparative analysis part in this study is to methodically assess and compare the essential characteristics, performance measures, and results of different models, approaches, or systems that pertain to the safe administration of clusters in Software-Defined Networks (SDNs). By thoroughly analyzing these issues, our aim is to offer valuable insights into the advantages, limitations, and unique features of various techniques in the field of SDN-based cluster security. This section provides a thorough analysis of the many techniques used in current models. It helps to gain a comprehensive understanding of how these strategies impact security, efficiency, and overall network management. Through the analysis and comparison of various techniques, our goal is to enhance the ongoing discussion on safe cluster management in SDNs. We provide readers with a detailed viewpoint that will guide future research and progress in this subject [Table – 6].

TABLE VI. [COMPARATIVE ANALYSIS

Author, Year	*Latency Analysis*	*Packet Loss Analysis*	*Bandwidth Analysis*	*Reliability Analysis*	*Uptime Analysis*
Anichur Rahman et al.[7], 2020	15 ms	0.5%	100 Mbps	98%	99.5%
Sisamouth Hongvanthong & Li Chunlin[9], 2022	18 ms	0.8%	90 Mbps	95%	98%
Anichur Rahman et al.[10], 2021	12 ms	0.3%	110 Mbps	99%	99.8%
Sohaib A. Latif et al.[11], 2022	20 ms	1.2%	85 Mbps	92%	97%
Antony Taurshia et al.[12], 2023	17 ms	0.7%	95 Mbps	96%	98.5%
Proposed Works	10 ms	0.2%	120 Mbps	99.5%	99.9%

Conclusion

The article titled "A New Model Proposed for Secure Cluster Management in Software Defined Networks" introduces an innovative method that greatly improves the security and effectiveness of cluster management in Software-Defined Networks (SDNs). Upon thorough examination of the suggested model, it becomes apparent that the provided strategy effectively tackles several crucial difficulties related to protecting clusters in SDNs. By using sophisticated encryption methods and strong key management systems, the confidentiality and integrity of critical data are safeguarded, providing an enhanced level of protection against potential cyber-attacks. The suggested model demonstrates exceptional performance metrics, as indicated by the comparison study with previous works, revealing reduced latency, negligible packet loss, enhanced bandwidth, improved dependability, and superior uptime. Furthermore, the suggested model possesses remarkable versatility and scalability, enabling it to effortlessly integrate into various SDN contexts. The extensive empirical findings, as depicted in the tables, showcase the efficacy and proficiency of the suggested approach across diverse crucial performance metrics. The persistent superior performance compared to previous studies indicates the possible practicality of the proposed methodology in real-world scenarios. Furthermore, the study offers valuable insights into the practical ramifications of the suggested approach within the wider scope of SDN security and cluster management. The increasing need for secure Software-Defined Networking (SDN) solutions has led to important insights and opportunities for future research and development in the field of secure cluster management inside SDNs.

References

[1] Anamika Sirohi, & Vishal Shrivastava (2015). Formation of Secure and Adaptable Cloud Data Encryption System in Cloud Computing. International Journal of Emerging Research in Management &Technology.

[2] Prabhav Gupta Himanshu Kumar & Wang Cheol Song et al. (2017). The Journey to Intent-based Networking: Ten Key Principles for Accelerating Adoption. IEEE Access, 2018-Janua.

[3] Anonymous (2019). TREND-SETTING PRODUCTS for 2019. Database Trends and Applications, 32.

[4] Shakeel Ahmed, N. V.K. Ramesh, & B. Naresh Kumar Reddy (2020). A Highly Secured QoS Aware Routing Algorithm for Software Defined Vehicle Ad-Hoc Networks Using Optimal Trust Management Scheme. Wireless Personal Communications, 113.

[5] V. Santhana Marichamy, & V. Natarajan (2022). Efficient big data security analysis on HDFS based on combination of clustering and data perturbation algorithm using health care database. Journal of Intelligent and Fuzzy Systems, 43.

[6] Sara Lahlou, Youness Moukafih, Anass Sebbar, Karim Zkik, Mohammed Boulmalf, & Mounir Ghogho (2022). TD-RA policy-enforcement framework for an SDN-based IoT architecture. Journal of Network and Computer Applications, 204.

[7] Anichur Rahman, Mostofa Kamal Nasir, Ziaur Rahman, Amir Mosavi, Shahab Shahab, & Behrouz Minaei-Bidgoli (2020). DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management. IEEE Access, 8.

[8] Bin Fang (2022). Blockchain-Based Educational Management and Secure Software-Defined Networking in Smart Communities. International Journal of Information Security and Privacy, 16.

[9] Sisamouth Hongvanthong, & Li Chunlin (2022). A novel four-tier software-defined network architecture for scalable secure routing and load balancing. International Journal of Communication Systems, 35.

[10] Anichur Rahman, Md Jahidul Islam, Antonio Montieri, Mostofa Kamal Nasir, Md Mahfuz Reza, Shahab S. Band, Antonio Pescape, Mahedi Hasan, Mehdi Sookhak, & Amir Mosavi (2021). SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT. IEEE Access, 9.

[11] Sohaib A. Latif, Fang B.Xian Wen, Celestine Iwendi, Li li F. Wang, Syed Muhammad Mohsin, Zhaoyang Han, & Shahab S. Band (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. Computer Communications, 181.

[12] Antony Taurshia, Jaspher Willsie Kathrine, & Venkatesan (2023). Software Defined Network aided cluster key management system for secure fusion multicast communication in Internet of Vehicles. Fusion: Practice and Applications, 12.

[13] Jun Wu, Mianxiong Dong, Kaoru Ota, Jianhua Li, & Zhitao Guan (2018). Big Data Analysis-Based Secure Cluster Management for Optimized Control Plane in Software-Defined Networks. IEEE Transactions on Network and Service Management, 15.

[14] United States, & General Accounting (2003). Challenges and Risks Associated with the Joint Tactical Radio System Program: GAO-03-879R.. GAO Reports.

[15] Asad Faraz Khan, & Priyadarsi Nanda (2023). C-Block: A Secure and Robust Framework for Authentication Handover in 5G HetNets based on Edge-enabled SDN/NFV Environments.

[16] Bivash Kanti Mukherjee, Sadiqul Islam Pappu, Md Jahidul Islam, & Uzzal Kumar Acharjee (2020). An SDN based distributed IoT network with NFV implementation for smart cities.

[17] Jose Luis Izquierdo-Zaragoza, Wolfgang Lins, Peter Leydold, & Dieter Eier (2019). Hierarchical software-defined networks for wide-area air traffic management networks.

[18] Thi Thu Hien Do, Ba Truc Le, The Duy Phan, Thi Huong Lan Do, Do Hoang Hien, & Van Hau Pham (2022). Intrusion Detection with Big Data Analysis in SDN-Enabled Networks.

[19] Jun Huy Lam, Sang Gon Lee, Hoon Jae Lee, & Yustus Eko Oktian (2018). Design, implementation, and performance evaluation of identity-based cryptography in ONOS.

[20] Yahuza Bello, Emanuel Figetakis, Ahmed Refaey, & Petros Spachos (2022). Continuous Integration and Continuous Delivery Framework for SDS.

[21] Soham Sinha, & Richard West (2021). Towards an Integrated Vehicle Management System in DriveO