DOI: http://dx.doi.org/10.26483/ijarcs.v16i6.7374

ISSN No. 0976-5697

Volume 16, No. 6, November-December 2025

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

SOFTWARE-DEFINED NETWORKING: A COMPREHENSIVE EXPLORATION OF ITS TRENDS, CHALLENGES, AND OPPORTUNITIES

Rabea M.Ali
Department of Computer Science and IT
Dr.Babasaheb Ambedkar Marathwada University
Chhatrapati Sambhajinagar, India

Manasi Ram Baheti
Department of Computer Science and IT
Dr.Babasaheb Ambedkar Marathwada University
Chhatrapati Sambhajinagar, India

Syed Ahteshamuddin Quadri
Department of Computer Science and IT
Dr.Babasaheb Ambedkar Marathwada University
Chhatrapati Sambhajinagar, India

Pratibha Dapke
Department of Computer Science and IT
Dr.Babasaheb Ambedkar Marathwada University
Chhatrapati Sambhajinagar, India

Samadhan M. Nagare
Department of Computer Science and Information Technology
Dr.Babasaheb Ambedkar Marathwada University
Chhatrapati Sambhajinagar, India

Abstract: Software-defined networking (SDN) is an emerging network architecture that decouples the control plane from the data plane, enabling centralized programmability and management of networks. While SDN offers benefits like flexibility, scalability, and automation, it also introduces new security vulnerabilities. This literature review analyzes the current state of research on SDN security in three key domains – Internet of Things (IoT) environments, cloud computing, and traditional enterprise networks. A systematic review methodology was followed to search, select, and review 53 relevant studies published in the past 5 years. The analysis focuses on identifying common SDN threat vectors, security solutions proposed leveraging SDN programmability and evaluating their effectiveness based on results from simulations, testbed experiments, and initial real-world implementations. Key findings of the review include lack of authentication, susceptibility to DDoS attacks, and flow rule conflicts as major security issues in SDN across domains. Dynamic traffic monitoring, access control, policy orchestration, and virtualized security functions are commonly proposed techniques to enhance SDN security. However, limitations exist in robustness testing at scale, emerging paradigms like fog computing, and quantitatively comparing SDN security with legacy networks. As SDN adoption expands, focused efforts are needed to address these research gaps through innovations in data-driven security, coordinated security policy, and emphasizing SDN controller security. This review provides valuable insights into the current state of SDN security research and informs future efforts needed in this important area.

Keywords: Software-Defined Networking, Network Security, Internet of Thing, Cloud Computing, DDoS Attack Mitigation

I. INTRODUCTION

All Software-defined networking (SDN) represents a new paradigm in network architecture and management. This section provides an in-depth analysis of the conceptual framework and operational mechanisms underlying SDN. SDN architecture consists of three distinct layers the application plane, control plane, and data plane. The application plane manages network applications and provides services to end-users. It abstracts the underlying physical infrastructure. The plane controls make centralized decisions on traffic forwarding rules and network configuration configuration. It provides programmable control capabilities. The data plane consists of networking devices like switches and routers that forward traffic based on rules set by the control plane [2][5][53]. Communication between the different planes in SDN is enabled through open interfaces: Southbound APIs that enable communication between control and data planes, e.g. OpenFlow, OVSDB; Northbound APIs that enable communication between application and control planes, e.g. REST APIs; and East/Westbound APIs that enable communication between SDN controllers for inter-domain networking as shown in figur1. Some key concepts central to SDN architecture are:

Separation of control logic from underlying routers and switches; Centralization of network intelligence and state in the control plane; Programmability of the network by external applications via APIs; Abstraction and virtualization of lower-level infrastructure; and Support for policy-based management based on business needs. By separating the control and data planes, SDN introduces new capabilities while also altering traditional network security assumptions and practices. The implications of this on network security will be analyzed in the following sections.

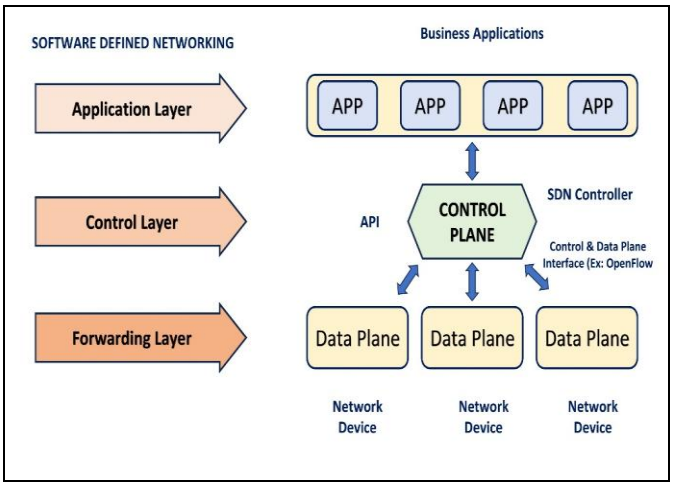

Figure 1. for SDN Architecture

As SDN adoption grows across diverse domains including enterprise networks, data centers, and the Internet of Things (IoT), a comprehensive analysis of its security implications is imperative [41]. This paper presents a systematic literature review on SDN security research focused on three key application areas – IoT, cloud computing, and traditional enterprise networks. The goal of this review is to analyze the current state of knowledge on SDN security in order to identify challenges, solutions, and research gaps. Both opportunities and risks resulting from fundamental SDN concepts like centralized control, programmability, and decoupled data/control planes are examined. The paper summarizes proposed techniques, frameworks, and mechanisms to secure SDN-based deployments against various threats. A critical analysis of the strengths and limitations of different security approaches is presented. Key knowledge gaps are identified to guide future research toward more secure, resilient SDN architectures and applications across domains. This review intends to provide a structured insight into securing next-generation networks transformed by the SDN paradigm. This review will contribute an up-to-date academic perspective on securing one of the most disruptive networking technologies of this era – SDN. It will serve as a knowledge base and research roadmap for students, security professionals, and network architects working in this rapidly evolving domain. The paper is organized as follows. Section 2 discusses related work and provides a perspective on SDN security in IoT. Section 3 describes the methodology used to collect papers from resources for the literature review. Section 4 presents a discussion and analysis of the gaps in studies, future research directions, and comparisons. The last section concludes the paper.

II. RELATED WORK

In this section, we've thoroughly explored previous studies on SDN security in IoT, cloud, and traditional networks. We're providing a comprehensive overview of the current knowledge, divided into three sections: SDN security in IoT, cloud, and traditional networks. Each section analyzes methodologies, study findings, and implications for future research. Our aim is to enhance understanding of SDN security challenges and opportunities in these contexts.

The integration of Software-Defined Networking (SDN) within Internet of Things (IoT) environments has garnered significant research attention in recent years. Keshav Sood et al. [23] addressed the issue of heterogeneity in SDN-based IoT networks which impact QoS and security. They proposed a methodology to categorize controllers and monitor response times to mitigate effects of heterogeneity. This mathematical model provides centralized, adaptive control to enhance QoS and security. Michael Baddeley et al. [24] focused on tackling latency and reliability challenges of SDN deployment in low-power IoT networks. They proposed Atomic-SDN architecture using synchronous flooding and a middleware layer for SDN control automation. Evaluation showed improved performance compared to other SDN solutions in terms of latency, reliability and power consumption. Tryfon Theodorou et al. [25] developed CORAL-SDN protocol to provide centralized, programmable control in Wireless Sensor Networks. They highlighted how dynamic network configuration aids scalability, mobility, and security. Real-world implementation demonstrated feasibility and performance gains. In contrast with conventional distributed control, the papers commonly propose centralized SDN controllers to monitor and programmatically control IoT networks. This facilitates dynamic optimization, access control, and integrated security. However, synchronous flooding, middleware layers, or new protocols are required to overcome control latency and overhead issues in resource-constrained IoT environments. Trupti Lotlikar et al. [26] examined DDoS attacks targeting IoT devices and proposed integrating IoT with SDN as a mitigation approach. C. Tselios et al. [27] discussed using blockchain to enhance trust in SDN-based IoT networks. Perekebode Amangele et al [28] presented a hierarchical machine learning framework for anomaly detection in SDN-IoT networks. Common SDN vulnerabilities highlighted across papers include lack of authentication between controllers and switches, vulnerabilities in controllers and APIs, flow rule conflicts, and susceptibility to DDoS attacks due to centralized control planes. Proposed security solutions follow a pattern of leveraging SDN's programmability for dynamic monitoring, access control, traffic engineering, and implementing security middleboxes. Machine learning and blockchain are emerging techniques utilized for threat detection and authentication. Federated reinforcement learning has been applied for autonomous traffic shaping in SDN-based IoT networks [48]. Approaches like Trust List [44] and identity-based mobility [43] aim to manage connections and restrict attacks in IoT edge networks. TCP multi-path selection using SDN has been investigated for handling growing IoT traffic to web services [46].

Yuki Yoshida et al. [47] evaluated using IoT devices as SDN apparatus and developed a path-selection method utilizing individual path traffic statistics and packet length. Experiments assessed the throughput and response time of this technique for web services showing superior performance over traditional approaches.

Kallol Krishna Karmakar et al [36] proposed an SDN-based security framework for IoT networks to restrict access and enforce granular flow policies. Experimental evaluations using malware attacks demonstrated the robustness of this architecture. Intidhar Bedhief et al [37] introduced an SDN-Docker architecture to handle heterogeneity in IoT networks and protocols. Experiments showed the ability to efficiently handle diverse devices and traffic flows validating the proposed framework.

Pankaj Thorat et al [38] leveraged machine learning techniques and SDN for detecting and preventing DoS attacks at IoT gateways. The ensemble approach combining multiple algorithms achieved approximately 98% accuracy.

Tao Li, Christoph Hofmann et al[39] proposed using SDN programmability to identify compromised switches through end-host reports and reroute traffic through reliable channels in IIoT networks. Prototype implementation demonstrated the solution's ability to promptly and reliably detect malicious forwarding devices.

Chaitanya Aggarwal et al[40] discussed integrating SDN and edge computing to enhance security and access control for IoT devices. The strategic use of traffic engineering, load balancing and stringent access policies were highlighted.

Anichur Rahman et al. [41] introduced a hierarchical architecture using SDN and blockchain for energy-efficient and secure IoT networks. Extensive simulations validated the framework's capabilities in ensuring secure communication and optimizing efficiency.

Gustavo Caiza et al[42] formulated and implemented an SDN/IoT testbed to evaluate the impact of SDN on Industry 4.0 applications. The testbed design comprising process, SDN and application layers was presented in detail.

Walaa F. Elsadek[43] proposed an identity-based mobility management solution using SDN overlay networks to address limitations of existing protocols. Preliminary results showcase efficient join delays validating the approach.

Kotaro Kataoka et al[44] introduced a Trust List and blockchain-based system to automatically enforce access policies and restrict attacks from rogue IoT devices in edge networks. A simulation illustrated the system's real-world functionality.

Ping Du et al[45] presented a context-aware IoT architecture using SDN and NFV with a software-defined forwarding plane to handle IoT traffic. Use cases in smart homes, cities and healthcare demonstrated the practical applicability.

Yuki Yoshida et al [46] evaluated using IoT devices as SDN apparatus and developed a path-selection method utilizing individual path traffic statistics and packet length. Experiments assessed the throughput and response time of this technique for web services showing superior performance over traditional approaches.

Younggi Kim et al [47] introduced a federated reinforcement learning approach for autonomous traffic shaping in SDN-IoT networks. Experiments using inverted pendulum platforms demonstrated streamlined learning and advantages of SDN-based control.

Shahzad et al[49] presented the FLIP framework integrating SDN and DPI for efficient data aggregation from large-scale IoT networks. Assessments showed the ability to automatically optimize networks and meet user requirements. Peter Bull et al. [50] proposed an SDN gateway placed at the edge of IoT networks to monitor traffic, modify QoS and restrict attacks. Comparative evaluations against standard models demonstrated enhanced security and detection of flood attacks.

Hamed Mohseni et al[51] introduced a cross-layer SDN-based mobility management scheme to reduce handover delays and latency for time-sensitive IoT applications. Evaluations showed decreased handoffs and mobility management delays. Yasin lnag et al[52] proposed an SDN-based IoT architecture to enhance sensor data transmission efficiency. Assessments focused on packet loss and latency with respect to network hops and topology.

In summary, SDN shows promise for centralized control, dynamic configuration, and security policy enforcement in IoT environments. However, solutions must account for resource constraints, heterogeneity, and vulnerabilities introduced by SDN. Further research is needed in multi-controller cooperation, failover mechanisms, and large-scale validation.

III. Methodology

A systematic approach was followed to search, select, and analyze research studies for this literature review. The first step was conducting a comprehensive search of major databases including IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar. The search was limited to English-language peer-reviewed conference and journal papers published in the past 5 years. The focus was on studies concentrating on SDN security in one or more of the domains - Internet of Things (IoT), cloud computing, and traditional enterprise networks. Search queries included relevant keywords and combinations such as "SDN security", "SDN vulnerabilities", "SDN cloud security", "SDN controller security", etc. This initial search resulted in over 200 articles. The papers were screened based on relevance by reviewing titles, abstracts, and keywords to shortlist 65 most pertinent articles. These were further evaluated by going through the full texts to finally select 53 high-quality studies aligned to the review scope

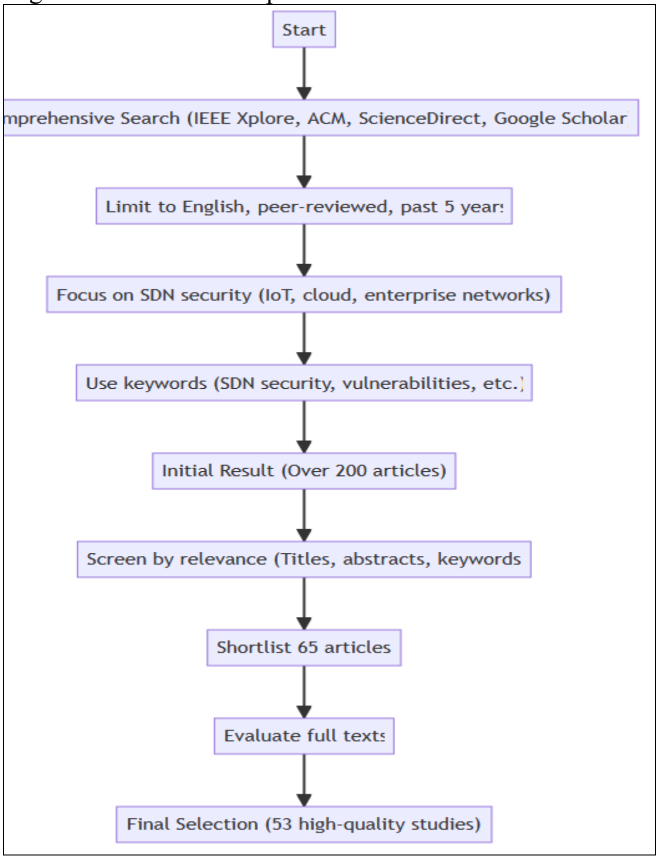
Start
mprehensive Search (IEEE Xplore, ACM, ScienceDirect, Google Scholar
Limit to English, peer-reviewed, past 5 year:
Focus on SDN security (IoT, cloud, enterprise networks)
Use keywords (SDN security, vulnerabilities, etc.]
Initial Result (Over 200 articles)
Screen by relevance (Titles, abstracts, keywords
Shortlist 65 articles
Evaluate full text:
Final Selection (53 high-quality studies)

Figure 2. Flowchart of the Systematic Literature Review Process on SDN Security

The full texts of selected articles were thoroughly read, analyzed, and summarized to identify the specific SDN security issues examined, solutions proposed, experimental methodologies used, results obtained, and conclusions presented. Key technical details, metrics, and findings were highlighted. The selected articles were categorized into themes based on the network environment - SDN security in IoT, cloud computing, and traditional networks. Within each theme, the approaches were compared, and limitations were noted. Aspects like threat models, evaluation setups, metrics, and validity of results were given importance during analysis. Key insights from the literature were synthesized to identify common security vulnerabilities in SDN architectures, propose taxonomies of threats and countermeasures, analyze trends and gaps in existing solutions, and provide recommendations for future research. Queries were rerun periodically to include any new studies published within the timeframe satisfying the criteria. In summary, a systematic methodology was followed to search, filter, critically review, analyze, and synthesize SDN security research literature for key insights.

IV. DISCUSSION

The reviewed studies demonstrate the significant potential of SDN to transform network security through centralized, programmable control and policy orchestration. New protocols like CORAL-SDN [25] and architectures like Atomic-SDN [24] aim to address control latency and overhead issues in resource-constrained IoT environments. SDN facilitates dynamic security monitoring, rapid threat response, and adaptive access control across diverse networks [23][26][27]. Integrating SDN with machine learning enables anomaly detection [28] while blockchain integration enhances provenance and auditability [27]. However, SDN also introduces new vulnerabilities that persist, including lack of authentication between controllers and switches [36], susceptibility to DDoS attacks [33], and flow rule conflicts [20]. While approaches leveraging traffic engineering [40], edge computing [40][50], and network segmentation [17] help reduce attack surfaces, innovative solutions are still needed. Emerging techniques like machine learning, blockchain, and fog computing add complexity and infrastructure requirements that may limit deployments [28][41][44]. Most proposals remain preliminary designs lacking extensive robustness testing and validation at scale. Evaluations are constrained to simulations, emulations, and small testbeds with limited diversity [6][10][14]. There is a dearth of large-scale, real-world studies across complex IoT, cloud or enterprise deployments. Quantitative comparative analyses with legacy network security solutions are rare [52], making ROI determination difficult. With increasing heterogeneity and distribution in IoT and cloud ecosystems, holistic SDN security solutions are still scarce [37][45]. Critical aspects like controller security [38], inter-domain coordination [37], and failover mechanisms [23] require further research. Emerging paradigms like moving target defense, deception tactics, and automated threat intelligence sharing can potentially improve resilience [18][49]. In summary, while SDN represents a promising approach to programmatically orchestrate security, pragmatic challenges around scalability, validation, incremental deployment, and integration with complementary technologies need to be addressed through extensive applied research and trials. Prudent integration of machine learning, edge computing, and blockchain with SDN can help maximize benefits while minimizing complexity. SDN security is still an open research area requiring multi-disciplinary innovations to realize its potential while overcoming limitations.

The existing literature on securing SDN-based networks, while insightful, presents several limitations and gaps. A majority of the proposals are in preliminary stages or are prototypes without substantial real-world validation, emphasizing the need for larger-scale deployments. The increasing complexity introduced by IoT and cloud environments often goes unaddressed in many solutions primarily aimed at enterprises or data centers, calling for more context-aware designs. An over-reliance on simulations, emulations, and testbeds, lacking variety in evaluation environments and traffic patterns, could lead to performance overestimations. Abbott Ho et al. [36] pinpoint the under-exploration of ML-based security applications in SDN, suggesting the potential for enhanced detection rates through innovative data-driven methods. The literature also reveals the need for more research into inter-domain security and coordination among multiple controller domains, as indicated by Y. Xiang et al. [37]. Furthermore, the robustness of controllers against exploits and attacks needs assessment, a concern raised by X. Huang et al. [38]. Lastly, as A. Braga et al. [39] note, there's a distinct absence of granular dynamic risk assessment methodologies that integrate diverse security data sources.

Table 1. Comparison of limitations and gaps across reviewed studies.

Study	Focus	Approach	Benefits	Limitations
Sood et al. [23]	Heterogeneity in SDN-IoT	Categorize controllers, monitor response times	Enhanced QoS and security via centralized, adaptive control	Limited large-scale validation
Baddeley et al. [24]	Latency and reliability in low-power IoT	Atomic-SDN architecture with flooding and middleware layer	Improved performance vs other SDN solutions	Overhead issues remain in resource constrained devices
Theodorou et al. [25]	Centralized control in wireless sensor networks	CORAL-SDN protocol	Dynamic configuration enhances scalability, mobility, security	Needs extensive real-world testing
Lotlikar et al. [26]	DDoS attacks by IoT devices	Integrate IoT and SDN	Leverages SDN programmability for security monitoring and response	Susceptible to emerging threats
Tselios et al. [27]	Trust in SDN-IoT	Use blockchain for decentralized authentication and logging	Enhanced provenance and auditability	Computationally intensive, lacks robust testing
Amangele et al. [28]	Anomaly detection in SDN-IoT	Two-tier hierarchical machine learning	Reduces edge device load, maintains accuracy	Prone to overfitting, narrow focus
Karmakar et al. [36]	Access control and policy enforcement	SDN framework with authentication and permission system	Withstood malware attacks demonstrating robustness	Limited topology size for evaluation

Bedhief et al. [37]	Heterogeneous protocols in IoT	SDN-Docker architecture	Handled diverse devices and traffic flows	Did not explore performance optimization
Thorat et al. [38]	DDoS attack detection and prevention	Ensemble ML approach at IoT gateway	~98% accuracy in identifying attacks	Limited analysis of misclassifications
Li et al. [39]	Secure IIoT data transmission	Identify compromised switches via host reports	Prompt and reliable detection enables prevention	Further functionality enhancements needed
Aggarwal et al. [40]	IoT device security	Integrate SDN and edge computing	Advanced access control through traffic engineering	Complexity in integrating edge computing and SDN
Rahman et al. [41]	Energy efficiency and security	SDN and blockchain framework	Ensured secure communication, optimized efficiency	Simulated environment lacks real-world validation
Caiza et al. [42]	Evaluate SDN for Industry 4.0 applications	Formulated and implemented SDN/IoT testbed	Detailed design supports scalability, security for industry use cases	Limited to demo applications in controlled setting
Elsadek [43]	Session mobility in SDN-IoT	SDN overlay network for mobility management	Efficient join delays validating approach	Needs evaluation across diverse mobility patterns
Kataoka et al. [44]	Access control in IoT edge networks	Blockchain-based trust system and SDN	Prevents large scale botnet attacks	Complexity of integrating blockchain with SDN
Du et al. [45]	Forwarding and processing IoT data	Context-aware architecture using SDN and NFV	Handles sensor data effectively, supports diverse apps	Additional optimization needed for industrial-scale deployments
Yoshida et al. [46]	Incorporating IoT devices in SDN control	TCP multi-path selection based on traffic	Improved web service performance over traditional networks	Limited flexibility in path switching schemes
Kim et al. [47]	Autonomous traffic shaping in SDN-IoT	Federated reinforcement learning approach	Streamlined learning, validated SDN-based control advantages	Sensitive to neural network parameters and architecture
Shahzad et al. [49]	Data aggregation in large-scale IoT	FLIP framework integrating SDN and DPI	Automated user-centric network optimization	Lacks comparision to alternatives beyond baseline
Bull et al. [50]	Securing IoT edge networks	SDN gateway for monitoring and restricting attacks	Enhanced security with low-cost hardware	Tradeoff between security and performance
Mohseni et al. [51]	Mobility management in SDN-IoT	Cross-layer mobility management scheme	Reduced latency and handoffs	Needs extensive evaluation across diverse mobility patterns
Inag et al. [52]	Sensor data transmission efficiency	SDN-based IoT architecture	Centralized monitoring and routing optimization	Did not explore alternative approaches for comparison
Bhushan et al. [1]	DDoS attack detection in cloud	Shared flow tables across switches	Improved attack resistance with lower overhead	Evaluation limited to simulations
De Jesus et al. [2]	Cloud security	Collaborative framework combining policies	Rapid threat response enabled by SDN	Bugs can impact network-wide
Chowdhary et al. [3]	Securing cloud in educational institutions	Science DMZ testbed	Flexible and scalable security monitoring	Narrow focus on academic environments
Djouani et al. [4]	IoT security and scalability	Integrate cloud, SDN and IoT	Enhanced confidentiality and access control	Lacks implementation details
Ghosh et al. [5]	Cloud networking and security	SDN-based information-centric cloud network	Optimized resource allocation, ensured data privacy	Needs comprehensive security analysis
Gao et al. [6]	Assessing vulnerabilities in cyber physical systems	Testbed integrating cloud, SDN	Highly adaptable and scalable architecture	Focused on simulation, lacks real-world testing
Abdulqadder et al. [7]	Securing 5G networks	Leverage SDN, NFV and cloud	Ensured user privacy while detecting attacks	Complex system requiring extensive tuning
Chi et al. [8]	Intrusion prevention in cloud	Dynamically filter intrusions using SDN	Significantly enhanced IDS effectiveness	Performance impact needs quantification
Meyer et al. [9]	In-vehicle communication security	SDN-based anomaly detection	Comprehensive security monitoring and response	Vehicle-specific dependencies may limit generalizability
Bhushan et al. [10]	DDoS attack detection in SDN clouds	Symmetric distance metric reduces overhead	Effective attack detection validated experimentally	Limited experimental scale and conditions
Zhou et al. [11]	DDoS attack detection in SDN clouds	Similar to Bhushan et al. [10]	Low overhead distributed denial of service attack detection	Repeats limitations of Bhushan et al. [10]
Jarraya et al. [12]	Cost optimization for cloud network security	Multi-stage optimization framework	Addresses scalability limitations	Implementation and testing details lacking
Jeong et al. [13]	Performance in virtualized cloud data centers	Packet rewriting approach using SDN switches	Near native throughput with lower resource overhead	Needs additional testing across configurations
Patel et al. [14]	Cloud network services and security	Integrate SDN, NFV and OpenStack	Enhanced network security and service quality	Lacks implementation specifics and evaluation
Anitha et al. [15]	Secure VM migration in cloud	SDN-based access control framework	Preserves confidentiality and integrity	Narrow focus limits applicability
Tamanna et al. [16]	DDoS defense in cloud environments	Leverage SDN programmability	Enables traffic engineering and attack isolation	High-level conceptual discussion only
Li et al. [17]	Access control in cloud environments	Stateful firewall based on SDN data plane	Precise access control with lower overhead	Needs extensive robustness testing
Smith-Perrone	Automated DDoS attack	Hybrid cloud solutions	Support diverse platforms and providers	Lacks technical details

et al. [18]	detection			
Bousselham et al. [19]	Securing vehicular cloud networks	Distributed SDN architecture with ECDSA	Protection against various attacks	Vehicle-specific dependencies may limit generalizability
Pisharody et al. [20]	SDN cloud security	Architecture for conflict detection, resolution	Addresses key SDN cloud concerns	Lacks implementation specifics and evaluation
Yan et al. [21]	DDoS defense in cloud data centers	Analysis of SDN-based DDoS protection	Insights into attack types and mitigation techniques	Does not propose new techniques
Jeuk et al. [22]	Service function chaining in cloud	Cloud identifier metadata and UCCaaS	Flexible and selective policy enforcement	Practical challenges integrating UCCaaS with NSH

A. Challenges and Limitations in SDN-IoT Integration

The integration of Software-Defined Networking (SDN) with the Internet of Things (IoT) has been the subject of numerous studies, focusing on specific aspects and proposing various approaches. However, a common thread across these studies is the identification of challenges and limitations inherent to this integration.

- Heterogeneity and Scalability: Sood et al. [23] highlighted the challenges posed by heterogeneity in SDN-IoT networks. While their approach offers enhanced QoS and security, it lacks large-scale validation, indicating potential scalability issues.
- Resource Constraints: Baddeley et al. [24] addressed latency and reliability in low-power IoT devices. Despite the improved performance, the overhead issues in resource-constrained devices remain unresolved.
- Real-world Applicability: Theodorou et al. [25] emphasized the benefits of centralized control in wireless sensor networks. However, their solution requires extensive real-world testing to ascertain its feasibility.
- Emerging Threat Landscape: Lotlikar et al. [26] and Thorat et al. [38] focused on DDoS attacks targeting IoT devices. While their approaches leverage SDN's programmability, they might be susceptible to new and evolving threats.
- Computational Overhead: Tselios et al. [27] discussed enhancing trust using blockchain. This approach, though promising, can be computationally intensive and lacks robust testing.
- Model Overfitting: Amangele et al. [28] proposed a machine learning-based approach for anomaly detection. Such models, while effective, can be prone to overfitting and may have a narrow focus.
- Performance Optimization: Bedhief et al. [37] introduced an SDN-Docker architecture to handle diverse IoT devices. The study did not delve into performance optimization, leaving room for further exploration.
- Complex Integrations: Aggarwal et al. [40] and Kataoka et al. [44] discussed the challenges of integrating SDN with edge computing and blockchain, respectively. These integrations introduce complexities that need to be addressed.
- Simulation vs. Real-world Testing: Rahman et al. [41] and Gao et al. [6] relied on simulated environments, which might not capture the intricacies of real-world IoT networks.
- Narrow Focus: Several studies, such as Chowdhary et al. [3] and Anitha et al. [15], have a specific focus, limiting their broader applicability.
- Repetitive Research: Zhou et al. [11] presented findings similar to Bhushan et al. [10], indicating potential redundancies in the research landscape.
- Lack of Technical Details: Some studies, like Smith-Perrone et al. [18], provide high-level discussions without delving into technical specifics.

B. Future Solutions for SDN-IoT Integration

- Adaptive Scalability Solutions: Develop SDN architectures that can dynamically adapt to the scale of IoT networks, ensuring consistent performance even as the number of devices grows exponentially.
- Resource-Efficient Protocols: Design lightweight SDN protocols tailored for resource-constrained IoT devices. These protocols should prioritize minimal overhead while maintaining security and performance.
- Hybrid Centralization: While centralized SDN controllers offer many benefits, a hybrid approach combining centralized and decentralized elements might address vulnerabilities and provide more resilience against certain threats.
- Advanced Threat Detection: Integrate advanced machine learning and AI techniques to continuously learn from network traffic, enabling real-time detection of both known and emerging threats.
- Holistic Blockchain Integration: Instead of merely using blockchain for trust or authentication, explore its potential for decentralized network management, ensuring data integrity and device accountability in the IoT network.
- Real-world Testbeds: Establish large-scale real-world testbeds for SDN-IoT solutions, moving beyond simulations to validate solutions in diverse and dynamic environments.
- Unified Frameworks: Develop comprehensive frameworks that integrate SDN, edge computing, blockchain, and other technologies, ensuring seamless interoperability and optimized performance.
- Self-Optimizing Networks: Design SDN controllers that can autonomously optimize network configurations based on real-time traffic, device health, and other parameters.
- Enhanced Mobility Management: Given the dynamic nature of IoT devices (e.g., vehicular networks), advanced mobility management solutions using SDN can ensure consistent connectivity and low latency.
- Open-source Collaborations: Encourage open-source collaborations to develop, test, and refine SDN-IoT solutions, fostering a community-driven approach to address challenges.
- Standardization Efforts: Engage in global standardization efforts to define best practices, protocols, and architectures for SDN in IoT, ensuring consistency and interoperability across solutions.
- User-Centric Design: Given the diverse applications of IoT, from smart homes to industrial setups, SDN solutions should prioritize user needs, ensuring solutions are intuitive, user-friendly, and cater to specific application requirements.

- Continuous Education and Training: As SDN-IoT solutions evolve, continuous education and training programs for network administrators, developers, and other stakeholders can ensure they are equipped to harness the full potential of these technologies.

V. CONCLUSION

This comprehensive literature review provides important insights into the current state of knowledge on securing SDN-based networks. Research so far has revealed common threat vectors stemming from the decoupled control and data planes of SDN architecture. These include lack of authentication between SDN controllers and switches, vulnerabilities in the controller platform and APIs, susceptibility to DDoS attacks due to centralized control, and flow rule conflicts. A range of solutions leveraging the programmability of SDN have been proposed and evaluated through simulations, testbeds, and smaller-scale implementations. Approaches such as dynamic traffic monitoring, access control, virtualized security functions, machine learning, blockchain, and policy orchestration demonstrate potential to enhance security monitoring, response, and resilience.However, limitations exist when it comes to large-scale robustness testing, evaluating emerging paradigms like fog computing, quantitatively comparing SDN security with legacy networks, assessing controller vulnerabilities, and inter-domain security mechanisms. As SDN sees expanded real-world deployment, these gaps need to be addressed through rigorous experimentation, innovative data-driven security applications, coordinated policy orchestration, and greater focus on securing SDN controllers and east/west interfaces.

There is also scope for novel integrations with big data analytics, edge computing, and blockchain to realize adaptive, context-aware security monitoring and response. Overall, while progress has been made, proactive efforts are still needed to enable seamless SDN adoption across diverse network domains. Targeted research to address identified limitations and gaps can unlock the full potential of SDN security.

VI. CONFLICT OF INTEREST STATEMENT

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest."

VII. AUTHOR CONTRIBUTIONS

Rabea M. Ali1 developed the conceptual model and wrote the original draft. He also performed the methodology, conducted the experiments, analyzed the results, and assisted in writing. Further, Mansi Ram validated the methodology and results and reviewed and edited the final draft. In addition, Mansi Ram supervised the research, administered the project resources, and made final revisions. The authors have read and agreed to the published version of the manuscript.

VIII. REFERENCES

[1] K. Bhushan and B. B. Gupta, "Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment," J Ambient Intell Humaniz Comput, vol. 10, no. 5, pp. 1985–1997, May 2019, doi: 10.1007/S12652-018-0800-9/METRICS.

[2] W. P. De Jesus, D. A. Da Silva, R. T. De Sousa, and F. V. L. Da Frota, "Analysis of SDN contributions for cloud computing security," Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014, pp. 922–927, Jan. 2014, doi: 10.1109/UCC.2014.150.

[3] A. Chowdhary, V. H. Dixit, N. Tiwari, S. Kyung, D. Huang, and G. J. Ahn, "Science DMZ: SDN based secured cloud testbed," 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2017, vol. 2017-January, pp. 1–2, Dec. 2017, doi: 10.1109/NFV-SDN.2017.8169868.

[4] R. Djouani, K. Djouani, F. Boutekkouk, and R. Sahbi, "A Security Proposal for IoT integrated with SDN and Cloud," Proceedings - 2018 International Conference on Wireless Networks and Mobile Communications, WINCOM 2018, Jan. 2019, doi: 10.1109/WINCOM.2018.8629727.

[5] U. Ghosh, P. Chatterjee, D. Tosh, S. Shetty, K. Xiong, and C. Kamhoua, "An SDN Based Framework for Guaranteeing Security and Performance in Information-Centric Cloud Networks," IEEE International Conference on Cloud Computing, CLOUD, vol. 2017-June, pp. 749–752, Sep. 2017, doi: 10.1109/CLOUD.2017.106.

[6] H. Gao, Y. Peng, K. Jia, Z. Wen, and H. Li, "Cyber-Physical Systems Testbed Based on Cloud Computing and Software Defined Network," Proceedings - 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2015, pp. 337–340, Feb. 2016, doi: 10.1109/IIH-MSP.2015.50.

[7] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan, and W. Dai, "Deployment of robust security scheme in SDN based 5G network over NFV enabled cloud environment," IEEE Trans Emerg Top Comput, vol. 9, no. 2, pp. 866–877, Apr. 2021, doi: 10.1109/TETC.2018.2879714.

[8] Y. Chi, T. Jiang, X. Li, and C. Gao, "Design and implementation of cloud platform intrusion prevention system based on SDN," 2017 IEEE 2nd International Conference on Big Data Analysis, ICBDA 2017, pp. 847–852, Oct. 2017, doi: 10.1109/ICBDA.2017.8078757.

[9] P. Meyer et al., "Demo: A Security Infrastructure for Vehicular Information Using SDN, Intrusion Detection, and a Defense Center in the Cloud," IEEE Vehicular Networking Conference, VNC, vol. 2020-December, Dec. 2020, doi: 10.1109/VNC51378.2020.9318351.

[10] K. Bhushan and B. B. Gupta, "Detecting DDoS Attack using Software Defined Network (SDN) in Cloud Computing Environment," 2018 5th International Conference on Signal Processing and Integrated Networks, SPIN 2018, pp. 872–877, Sep. 2018, doi: 10.1109/SPIN.2018.8474062.

[11] Z. Yongkai, Y. Hang, Z. Lijun, L. Guobao, and L. Ge, "Multiple SDN controller orchestration for financial cloud," 2016 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2016 - Proceedings, Sep. 2016, doi: 10.1109/SSIC.2016.7571809.

[12] Y. Jarraya, A. Shameli-Sendi, M. Pourzandi, and M. Cheriet, "Multistage OCDO: Scalable Security Provisioning Optimization in SDN-Based Cloud," Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015, pp. 572–579, Aug. 2015, doi: 10.1109/CLOUD.2015.82.

[13] K. Jeong, R. Figueiredo, and K. Ichikawa, “PARES: Packet Rewriting on SDN-Enabled Edge Switches for Network Virtualization in Multi-Tenant Cloud Data Centers,” IEEE International Conference on Cloud Computing, CLOUD, vol. 2017-June, pp. 9–17, Sep. 2017, doi: 10.1109/CLOUD.2017.11.

[14] P. Patel, V. Tiwari, and M. K. Abhishek, “SDN and NFV integration in openstack cloud to improve network services and security,” Proceedings of 2016 International Conference on Advanced Communication Control and Computing Technologies, ICACCCT 2016, pp. 655–660, Jan. 2017, doi: 10.1109/ICACCCT.2016.7831721.

[15] H. M. Anitha and P. Jayarekha, “SDN Based Secure Virtual Machine Migration in Cloud Environment,” 2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018, pp. 2270–2275, Nov. 2018, doi: 10.1109/ICACCI.2018.8554813.

[16] T. Tamanna, T. Fatema, and R. Saha, “SDN, A research on SDN assets and tools to defense DDoS attack in cloud computing environment,” pp. 1670–1674, Feb. 2018, doi: 10.1109/WISPNET.2017.8300045.

[17] J. Li, H. Jiang, W. Jiang, J. Wu, and W. Du, “SDN-based Stateful Firewall for Cloud,” Proceedings - 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, IDS 2020, pp. 157–161, May 2020, doi: 10.1109/BIGDATASECURITY-HPSC-IDS49724.2020.00037.

[18] J. Smith-Perrone and J. Sims, “Securing cloud, SDN and large data network environments from emerging DDoS attacks,” Proceedings of the 7th International Conference Confluence 2017 on Cloud Computing, Data Science and Engineering, pp. 466–469, Jun. 2017, doi: 10.1109/CONFLUENCE.2017.7943196.

[19] M. Bousselham, A. Abdellaoui, and H. Chaoui, “Security against malicious node in the vehicular cloud computing using a software-defined networking architecture,” 2017 International Conference on Soft Computing and its Engineering Applications: Harnessing Soft Computing Techniques for Smart and Better World, icSoftComp 2017, vol. 2018-January, pp. 1–5, Feb. 2018, doi: 10.1109/ICSOFTCOMP.2017.8280084.

[20] S. Pisharody, A. Chowdhary, and D. Huang, “Security policy checking in distributed SDN based clouds,” 2016 IEEE Conference on Communications and Network Security (CNS), pp. 19–27, Feb. 2016, doi: 10.1109/CNS.2016.7860466.

[21] Q. Yan, F. R. Yu, Q. Gong, and J. Li, “Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges,” IEEE Communications Surveys and Tutorials, vol. 18, no. 1, pp. 602–622, Jan. 2016, doi: 10.1109/COMST.2015.2487361.

[22] S. Jeuk, G. Salgueiro, and S. Zhou, “Towards Cloud-Aware Policy Enforcement with Universal Cloud Classification as a Service (UCCaaS) in Software Defined Networks,” pp. 489–496, Jan. 2017, doi: 10.1109/CLOUD.2016.0071.

[23] K. Sood, K. K. Karmakar, S. Yu, V. Varadharajan, S. R. Pokhrel, and Y. Xiang, “Alleviating Heterogeneity in SDN-IoT Networks to Maintain QoS and Enhance Security,” IEEE Internet Things J, vol. 7, no. 7, pp. 5964–5975, Jul. 2020, doi: 10.1109/JIOT.2019.2959025.

[24] M. Baddeley et al., “Atomic-SDN: Is Synchronous Flooding the Solution to Software-Defined Networking in IoT?,” IEEE Access, vol. 7, pp. 96019–96034, 2019, doi: 10.1109/ACCESS.2019.2920100.

[25] T. Theodorou and L. Mamatas, “CORAL-SDN: A software-defined networking solution for the internet of things,” 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2017, vol. 2017-January, pp. 1–2, Dec. 2017, doi: 10.1109/NFV-SDN.2017.8169870.

[26] T. Lotlikar, S. Madhavan, S. Andrews, C. Mascarenhas, and J. Mathew, “DoShield Through SDN for IoT Enabled Attacks,” Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018, pp. 1499–1504, Sep. 2018, doi: 10.1109/ICECA.2018.8474665.

[27] C. Tselios, I. Politis, and S. Kotsopoulos, “Enhancing SDN security for iot-related deployments through blockchain,” 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2017, vol. 2017-January, pp. 303–308, Dec. 2017, doi: 10.1109/NFV-SDN.2017.8169860.

[28] P. Amangele, M. J. Reed, M. Al-Naday, N. Thomos, and M. Nowak, “Hierarchical Machine Learning for IoT Anomaly Detection in SDN,” 2019 International Conference on Information Technologies, InfoTech 2019 - Proceedings, Sep. 2019, doi: 10.1109/INFOTECH.2019.8860878.

[29] R. Muñoz et al., “Integration of IoT, Transport SDN, and Edge/Cloud Computing for Dynamic Distribution of IoT Analytics and Efficient Use of Network Resources,” Journal of Lightwave Technology, vol. 36, no. 7, pp. 1420–1428, Apr. 2018, doi: 10.1109/JLT.2018.2800660.

[30] L. Ogrodowczyk, B. Belter, and M. Leclerc, “IoT Ecosystem over programmable SDN infrastructure for smart city applications,” Proceedings - European Workshop on Software-Defined Networks, EWSDN , vol. 2016-October, pp. 49–51, Jun. 2017, doi: 10.1109/EWSDN.2016.17.

[31] S. Badotra, Di. Nagpal, S. N. Panda, S. Tanwar, and S. Bajaj, “IoT-Enabled Healthcare Network with SDN,” ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), pp. 38–42, Jun. 2020, doi: 10.1109/ICRITO48877.2020.9197807.

[32] M. Baddeley, R. Nejabati, G. Oikonomou, S. Gormus, M. Sooriyabandara, and D. Simeonidou, “Isolating SDN control traffic with layer-2 slicing in 6TiSCH industrial iot networks,” 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2017, vol. 2017-January, pp. 247–251, Dec. 2017, doi: 10.1109/NFV-SDN.2017.8169876.

[33] N. Sambandam, M. Hussein, N. Siddiqi, and C. H. Lung, “Network Security for IoT Using SDN: Timely DDoS Detection,” DSC 2018 - 2018 IEEE Conference on Dependable and Secure Computing, Jan. 2019, doi: 10.1109/DESEC.2018.8625119.

[34] S. Ali and M. Ghazal, “Real-time Heart Attack Mobile Detection Service (RHAMDS): An IoT use case for Software Defined Networks,” Canadian Conference on Electrical and Computer Engineering, Jun. 2017, doi: 10.1109/CCECE.2017.7946780.

[35] Rule-Based Translation of Application-Level QoS Constraints into SDN Configurations for the IoT.” https://www.researchgate.net/publication/331978414_Rule-Based_Translation_of_Application-Level_QoS_Constraints_into_SDN_Configurations_for_the_IoT (accessed Jul. 28, 2023).

[36] K. K. Karmakar, V. Varadharajan, S. Nepal, and U. Tupakula, “SDN-Enabled Secure IoT Architecture,” IEEE

Internet Things J, vol. 8, no. 8, pp. 6549–6564, Apr. 2021, doi: 10.1109/JIOT.2020.3043740.

[37] I. Bedhief, M. Kassar, and T. Aguili, "SDN-based architecture challenging the IoT heterogeneity," 2016 3rd Smart Cloud Networks and Systems, SCNS 2016, Mar. 2017, doi: 10.1109/SCNS.2016.7870558.

[38] P. Thorat and N. Kumar Dubey, "SDN-based Machine Learning Powered Alarm Manager for Mitigating the Traffic Spikes at the IoT Gateways," Proceedings of CONECCT 2020 - 6th IEEE International Conference on Electronics, Computing and Communication Technologies, Jul. 2020, doi: 10.1109/CONECCT50063.2020.9198356.

[39] T. Li, C. Hofmann, and E. Franz, "Secure and Reliable Data Transmission in SDN-based Backend Networks of Industrial IoT," Proceedings - Conference on Local Computer Networks, LCN, vol. 2020-November, pp. 365–368, Nov. 2020, doi: 10.1109/LCN48667.2020.9314854.

[40] C. Aggarwal and K. Srivastava, "Securing IOT devices using SDN and edge computing," Proceedings on 2016 2nd International Conference on Next Generation Computing Technologies, NGCT 2016, pp. 877–882, Mar. 2017, doi: 10.1109/NGCT.2016.7877534.

[41] A. Rahman et al., "SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT," IEEE Access, vol. 9, pp. 28361–28376, 2021, doi: 10.1109/ACCESS.2021.3058244.

[42] G. Caiza, S. Chiliquinga, S. Manzano, and M. V. Garcia, "Software-Defined Network (SDN) Based Internet of Things within the context of low-cost automation," IEEE International Conference on Industrial Informatics (INDIN), vol. 2020-July, pp. 587–591, Jul. 2020, doi: 10.1109/INDIN45582.2020.9442180.

[43] W. F. Elsadek, "Toward hyper interconnected iot world using SDN overlay network for NGN seamless mobility," Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, vol. 0, pp. 460–463, Jul. 2016, doi: 10.1109/CLOUDCOM.2016.0078.

[44] K. Kataoka, S. Gangwar, and P. Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN," IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings, vol. 2018-January, pp. 296–301, May 2018, doi: 10.1109/WF-IOT.2018.8355139.

[45] P. Du, P. Putra, S. Yamamoto, and A. Nakao, "A context-aware IoT architecture through software-defined data plane," Proceedings - 2016 IEEE Region 10 Symposium, TENSYMP 2016, pp. 315–320, Jul. 2016, doi: 10.1109/TENCONSPRING.2016.7519425.

[46] Y. Yoshida and Y. Ito, "Application of TCP Multi-Pathization Method with SDN by IoT Devices to Web Service," 9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018, pp. 402–404, Nov. 2018, doi: 10.1109/ICTC.2018.8539508.

[47] Y. Kim and Y. Lee, "Automatic Generation of Social Relationships between Internet of Things in Smart Home Using SDN-Based Home Cloud," Proceedings - IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2015, pp. 662–667, Apr. 2015, doi: 10.1109/WAINA.2015.93.

[48] H. K. Lim, J. B. Kim, S. Y. Kim, and Y. H. Han, "Federated Reinforcement Learning for Automatic Control in SDN-based IoT Environments," International Conference on ICT Convergence, vol. 2020-October, pp. 1868–1873, Oct. 2020, doi: 10.1109/ICTC49870.2020.9289245.

[49] S. Shahzad and E. S. Jung, "FLIP-FLexible IoT Path Programming Framework for Large-scale IoT," Proceedings - 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing, CCGRID 2020, pp. 881–888, May 2020, doi: 10.1109/CCGRID49817.2020.00014.

[50] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, "Flow based security for IoT devices using an SDN gateway," Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016, pp. 157–163, Sep. 2016, doi: 10.1109/FICLOUD.2016.30.

[51] H. Mohseni and B. Eslamnour, "Handover Management for Delay-sensitive IoT Services on Wireless Software-defined Network Platforms," Proceedings of 3rd International Conference on Internet of Things and Applications, IoT 2019, Apr. 2019, doi: 10.1109/IICITA.2019.8808840.

[52] Y. Inag, M. Demirci, and S. Ozemir, "Implementation of an SDN Based IoT Network Model for Efficient Transmission of Sensor Data," UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering, pp. 682–687, Sep. 2019, doi: 10.1109/UBMK.2019.8907119.

[53] M. Tawfik, N. M. Al-Zidi, B. Alsellami, A. M. Al-Hejri and S. Nimbhore, "Internet of Things-Based Middleware Against Cyber-Attacks on Smart Homes using Software-Defined Networking and Deep Learning," 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST), 2021, pp. 7-13, doi: 10.1109/ICCMST54943.2021.00014.

[54] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[55] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[56] K. Elissa, "Title of paper if known," unpublished.

[57] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[58] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[59] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[60] Electronic Publication: Digital Object Identifiers (DOIs):

[61] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467. **(Article in a journal)**

[62] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670. **(Article in a conference proceedings)**