Computer Science, Engineering and Technology

Vol: 2(3), September 2024

REST Publisher; ISSN: 2583-9179 (Online)

Website: https://restpublisher.com/journals/cset/

DOI: https://doi.org/10.46632/cset/2/3/9

Integration of SDN and Block Chain Technology Using Weighted Product Model

Vamsi Krishna Kavuri

Senior Lead Software Engineer

Corresponding author Email: kavurivk@gmail.com

Abstract: *The integration of Software-Defined Networking (SDN) and block chain technology represents a groundbreaking approach in addressing contemporary challenges in network management and security. The dynamic and centralized control offered by SDN, combined with the decentralized and secure nature of block chain, provides a robust framework for enhancing network performance and security.SDN simplifies network management by decoupling the control plane from the data plane, allowing for more flexible and efficient network configuration. However, this centralization can become a single point of failure and a target for cyber-attacks. Block chain technology mitigates these vulnerabilities by providing a decentralized ledger that enhances security and transparency. By recording network events on a block chain, the integrity and authenticity of network transactions are ensured, reducing the risk of malicious activities. The integration of Software-Defined Networking (SDN) and block chain technology is a significant advancement in the field of network management and security, offering innovative solutions to contemporary challenges. By leveraging the dynamic control capabilities of SDN and the decentralized, secure nature of block chain, this research contributes to the development of more resilient, efficient, and secure network infrastructures. One of the critical areas of impact is enhanced network security. Traditional networks are vulnerable to various cyber threats, and the centralized nature of SDN can become a target for attacks. Block chain technology mitigates these risks by providing a decentralized ledger system that ensures the integrity and authenticity of network transactions. This integration can prevent unauthorized access and reduce the risk of data tampering, thereby creating a more secure network environment. Alternative taken as SDN with Ethereal Block chain. SDN with Hyper ledger Fabric. SDN with Corda Block chain. SDN with Cord Block chain. SDN with Multichip Block chain. Evaluation Preference taken as Security Enhancement (SE) Network Performance (NP) Implementation Cost (IC) Operational Complexity (OC) The results indicate that SDN with Quorum Block chain D Attained the top position, while SDN with Ethereal Block chain A had The lowest position achieved. The dataset's significance regarding Integration of SDN and Block chain Technology, according to the wpm Method, Company D achieves the highest ranking.*

Key words: *transaction blocks, Conventional security. the reliability of IoT transactions, suggest a block chain-consolidating data, In Software-Defined Networking.*

1. INTRODUCTION

The Internet of Things (IoT) describes a network of interconnected devices that interact and share information with one another over the internet. faces several challenges related to efficiency, security, and scalability as the number and diversity of smart devices increase. To tackle the decentralized aspect of the Internet of Things (IoT). Software-Defined Networking (SDN) is considered a promising solution. It enables a central controller to supervise and control the network from a comprehensive perspective. an overarching perspective. The swift expansion of the Internet of Things (IoT)requires the adoption of strong safety and confidentiality measures to address system vulnerabilities and threatsIn the realm issues like reliability, scalability, and power efficiency become especially critical. Conventional security measures often fall short in these situations. Consequently, this survey concentrates on different security challenges related to the specific targets of attacks within IoT. Many In an IIoT environment, addressing these issues is of equal significance. Categorizing attacks based on their targets assists researcher's practitioners, and industry experts in identifying the threats pertinent to their specific applications. Since cryptographic hash functions cannot be reversed solutions need to be found through Brute-force techniques. Unfortunately, reverse hashing offers neither scientific nor societal advantages other than supporting consensus. The primary aim is to motivate participating nodes (miners) to dedicate their resources to the longest chain. thereby establishing a universal, decentralized agreement on the accepted version of the chain. Walton Chain is a public block chain platform designed for supply chains, which stores monitoring data from proprietary RFID chips connected to IoT devices. Walton Chain originally employed Proof of Stake Trust

(PoST) as its consensus mechanism, integrating a reputation-based system with PoS to achieve agreement. This method is a relatively new approach to network building, focusing on reliability and security to prevent, identify, report, isolate, reduce, and potentially address the negative impacts of network intrusions. However, many IoT sensing and smart devices are constrained by limited energy, computational power, and storage capacity. This raises concerns about whether ECDSA can meet both the computational and memory demands within these energy constraints. Smart contracts execute only in response to transactions, but one contract can invoke another, which may in turn call yet another, forming a sequence of calls. It is important to recognize that smart contracts do not operate independently or run in the backgroundBlockchain, a robust distributed ledger technology (DLT), has advanced considerably in recent yearsJacobovitz et al. have evaluated the current state of block chain technology, its applications, and its role in Identity administration. Enhancing Identity and authorization management. through block chain is a critical security measure for Sentara Healthcare, which links Virginia and North Carolina via a unified distribution network. This block chain solution employs a specialized Hyper ledger To support various applications in run simultaneously on Hyper ledger, each application is assigned its own distinct channel with a unique channel ID. In BCSDN, there is a single application for SDN flow verification and validation. IoT devices and hubs requiring new flow rules have been registered with the organization's Certificate Authority, and have obtained the required cryptographic materials for device authentication. Figure 1 depicts the system design of our proposed framework, consisting of four layers. The initial layer, known as the block chain The networking layer is responsible for handling the routing of data between devices across different networks. It manages the paths that data packets take to travel from the origin to the destination, guaranteeing effective and dependable communication, supports data storage and sharing through a distributed file system like IPFSBlockchain validating nodes exchange information to keep synchronized copies of all IoT transaction blocks, verifying and confirming transactions based Regarding consensus rules (refer In Section 3.4, each validating node functions as a service provider within the platform, collaborating with other nodes via a distributed smart Service Level Agreement (SLA) to ensure the reliability of IoT transactions. These reliable transactions are handled through consistent distributed agreements, removing the necessity for a central arbitration authority. and preventing conflicts. The paper presents an innovative authentication handover mechanism based on block chain technology for SDN-based 5G networks, designed to avoid redundant re-authentication during repeated handovers across heterogeneous 5G cellsQiu et al. investigate the (IIoT) environment with and suggest a block chain- consolidating data viewpoints among these controllers. They employ the Q-learning approach to simultaneously optimize view adjustments, Privacy is characterized as an individual's right to control their information, with block chain users employing pseudonyms (addresses) for transactions, often managing numerous addresses. Transactions create a series of signatures that confirm ownership and transfer of assets, facilitating traceable processes. Commercially available IoT products prioritize device functionality over security, often adding advanced security measures later. Block chain, a decentralized database, allows assets to be stored and transferred through a network of computers, maintaining security and anonymity. Although the system is decentralized, only the asset owner with the private key can conduct transactions, while other network computers act as validates. This technology securely logs Transactions are recorded into a public ledger across nodes without requiring a trusted third party. Traditional cloud methods, which rely on authentication processes where nodes must prove their trustworthiness to a remote verifier through cryptographic techniques, often face challenges in achieving both scalability and efficiency. By utilizing block chain as the main distributed record for a system, authorized nodes can quickly track and verify data from IoT devices, regardless of its volume or source, once it's entered into the block chain. A distributed, encrypted database is inherently robust, lacking a single point of failure. As the system is continuously updated with new blocks, any active node provides the most current information. Once established, these elements are both immutable and incorruptible. This project is designed to ensure trust and security in Io T environments, such as Smart Cities and Healthcare. The ARMOUR experiment establishes the security framework, conducts tests, performs experiments, and issues certification labels..In Software-Defined Networking In Software-Defined Networking (SDN), traffic forwarding based on flow rules enhances network resource utilization by enabling requests from multiple users to be routed through the intended paths. paths as determined by the SDN controller. This overview of Software-Defined Internet of Things (SD-IoT) explores how SDN-based technologies can tackle challenges across edge, access, core, and data center networks. It includes a thorough survey of current SDN-based technologies within the context of Io T. The overview also identifies potential research directions, proposing methods to expand existing solutions to overcome their limitations and improve Io T efficiency. Lastly, it addresses several unresolved research issues. that are critical for establishing an efficient and effective Io T environment are discussed.

2. MATERIALS AND METHODS

Block chain-based security and privacy systems for Io T networks can be categorized into two types: permission and permission less. Permission block chains require authorization to join the network and include public block chains, federated/consortium block chains, and private block chains. Conversely, permission less block chains allow anyone to access and participate in the network without needing authorization. This survey reviews recent advancements in block chain and block chain-based Io T applications, drawing from 244 research references found in sources like Google

Scholar, Web of Science, IEEE Explore, Elsevier, and online resources such as web pages and developer communities. The references are comprehensively categorized according to five key aspects of block chain Io T technologies.. With the block chain- In a solution based on the Internet of Drones, the reliance on third-party systems is removed, thereby enhancing trust and security within the drone communication network. This system is gaining increasing attention and is expected to be a crucial component of the future Internet of Things due to its considerable advantages Flexibility, mobility, and cost are crucial factors in deployment. -Efficiency -efficiency. In our proposed method, a central hub solely keeps track of references to member repositories where the actual datasets are stored and disseminated. The system handles the management of membership details such as addresses, owners, and sharing policies. Block chain. Essentially, all members, including the hub, record and share this membership information on the block chain. Another block chain maintains the RIM (Reference Information Model) of datasets to ensure their integrity. Regardless of the installation method, a switch can only support a limited number of flow tables for rule storage. Since switches in the SDN era lack advanced intelligence and decision-making abilities, the main security concern in the data plane is distinguishing legitimate flow rules from malicious ones. In the context of block chain, privacy is about preserving anonymity and unlinking transactions.4o mini Transaction anonymity ensures This means that linking a transaction to a specific user is not feasible, which leads users to use different addresses for each new transaction. Unlinking is based on the assumption that block chain addresses and transactions are not connected to users' real identities., with transaction data being routed through random points in the network While security mechanisms are clearly necessary in SDN, our focus This paper focuses on the edge block chain mechanism itself. This is because the edge block chain is a fundamental component that must be established before its advantages can be realized. Therefore, we will briefly outline the advantages of our architecture and its intended purpose applications. The primary advantage of the proposed The advantage of this mechanism is that it provides a security framework independent of the intricate SDN controller process. This separation helps prevent malicious activities within the SDN Subsystems and facilitate verifiable security auditing. Developers are responsible for creating both the applications and smart contracts used by block chain participants offer significant market opportunities for developers to cryptographically verify the accuracy of the underlying ledgers. crypto currencies. [13].

3. ANALYSIS AND DISSECTION

TABLE 1. Integration of SDN and Block Chain Technology

Alternative	Security Enhancement (SE)	Network Performance (NP)	Implementation Cost (IC)	Operational Complexity (OC)
SDN with Ethereal Block chain	8	7	7	6
SDN with Hyper ledger Fabric	9	8	6	7
SDN with Cord Block chain	7	6	5	6
SDN with Quorum Block chain	8	7	6	5
SDN with Multichip Block chain	6	5	4	5

The data set in Table 1 compares different SDN (Software-Defined Networking) implementations using various block chain technologies across four key dimensions: Security Enhancement (SE), Network Performance (NP), Implementation Cost (IC), and Operational Complexity (OC).SDN with Ethereal Block chain: This option scores 8 in Security Enhancement, indicating strong security features. It performs well in Network Performance with a score of 7. The Implementation Cost is relatively moderate at 7, and Operational Complexity is slightly lower at 6, suggesting it's somewhat easier to manage compared to others.SDN with Hyper ledger Fabric: This alternative excels in Security Enhancement with the highest score of 9 and also shows superior Network Performance at 8. Its Implementation Cost is slightly lower at 6, while its Operational Complexity is a bit higher at 7, reflecting some challenges in operation.SDN with Cords Block chain: This implementation has a lower Security Enhancement score of 7 and the lowest Network Performance at 6. The Implementation Cost is the lowest among the options at 5, and Operational Complexity is moderate at 6, indicating a balanced yet less secure and slower performance.SDN with Quorum Block chain: With an 8 in Security Enhancement and 7 in Network Performance, this option shows strong capabilities in both areas. Its Implementation Cost is moderate at 6, and it has the lowest Operational Complexity at 5, making it relatively easier to manage.SDN with Multichip Block chain: This alternative scores the lowest in all dimensions, with a 6 in Security Enhancement, 5 in Network Performance, 4 in Implementation Cost, and 5 in Operational Complexity, suggesting it is the least secure and least perform ant but potentially less costly and complex to implement. In summary, each SDN implementation with block chain technology has its strengths and weaknesses, with Hyper ledger Fabric providing the best security and performance, while Multi The data set in Table 1 compares different SDN (Software-Defined Networking) implementations using various block chain technologies across four key dimensions: Security Enhancement (SE), Network Performance (NP), Implementation Cost (IC), and Operational Complexity (OC).depending on the specific problem and circumstances. Furthermore, accurate weight summation assumes additivity among attributes, which may not always be realistic, posing a challenge in certain scenarios.

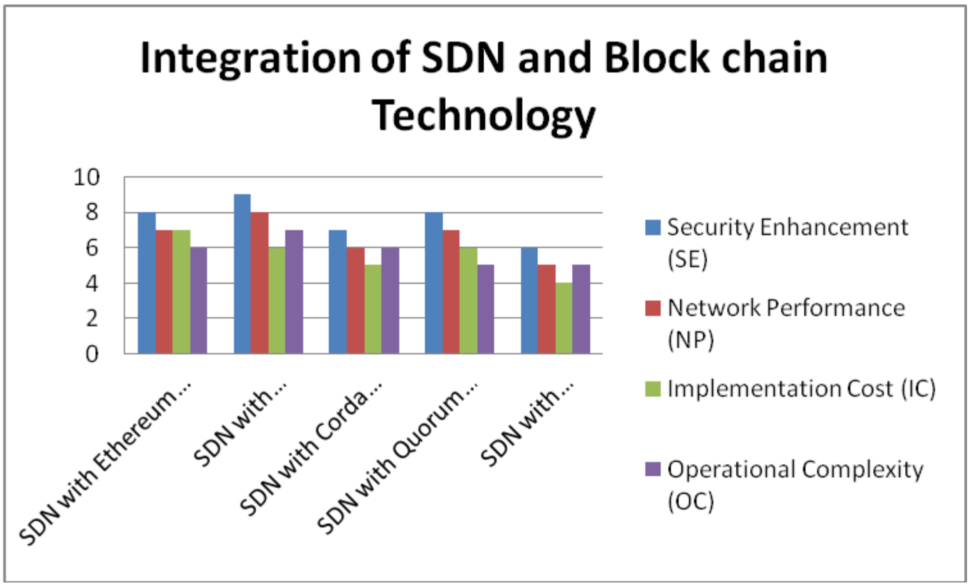

FIGURE 1. Integration of SDN and Block chain Technology

The data set in figure 1 compares different SDN (Software-Defined Networking) implementations using various block chain technologies across four key dimensions: Security Enhancement (SE), Network Performance (NP), Implementation Cost (IC), and Operational Complexity (OC).SDN with Ethereal Block chain: This option scores 8 in Security Enhancement, indicating strong security features. It performs well in Network Performance with a score of 7. The Implementation Cost is relatively moderate at 7, and Operational Complexity is slightly lower at 6, suggesting it's somewhat easier to manage compared to others.SDN with Hyper ledger Fabric: This alternative excels in Security Enhancement with the highest score of 9 and also shows superior Network Performance at 8. Its Implementation Cost is slightly lower at 6, while its Operational Complexity is a bit higher at 7, reflecting some challenges in operation.SDN with Cords Block chain: This implementation has a lower Security Enhancement score of 7 and the lowest Network Performance at 6. The Implementation Cost is the lowest among the options at 5, and Operational Complexity is moderate at 6, indicating a balanced yet less secure and slower performance.SDN with Quorum Block chain: With an 8 in Security Enhancement and 7 in Network Performance, this option shows strong capabilities in both areas. Its Implementation Cost is moderate at 6, and it has the lowest Operational Complexity at 5, making it relatively easier to manage.SDN with Multichip Block chain: This alternative scores the lowest in all dimensions, with a 6 in Security Enhancement, 5 in Network Performance, 4 in Implementation Cost, and 5 in Operational Complexity, suggesting it is the least secure and least perform ant but potentially less costly and complex to implement. In summary, each SDN implementation with block chain technology has its strengths and weaknesses, with Hyper ledger Fabric providing the best security and performance, while Multi The data set in Table 1 compares different SDN (Software-Defined Networking) implementations using various block chain technologies across four key dimensions: Security Enhancement (SE), Network Performance (NP), Implementation Cost (IC), and Operational Complexity (OC).depending on the specific problem and circumstances. Furthermore, accurate weight summation assumes additively among attributes, which may not always be realistic, posing a challenge in certain scenarios.

TABLE 2. Performance value

SDN with Ethereum Blockchain	0.8889	0.875	0.5714	0.8333
SDN with Hyperledger Fabric	1	1	0.6667	0.7143
SDN with Corda Blockchain	0.7778	0.75	0.8	0.8333
SDN with Quorum Blockchain	0.8889	0.875	0.6667	1
SDN with Multichain Blockchain	0.6667	0.625	1	1

The performance values provided in the data set reflect the relative strengths and weaknesses of different SDN (Software-Defined Networking) implementations using various block chain technologies across four key dimensions: Security Enhancement (SE), Network Performance (NP), Implementation Cost (IC), and Operational Complexity (OC).The first row shows the values: 0.8889, 0.875, 0.5714, and 0.8333. These numbers represent performance metrics for SDN with Ethereal Block chain. The high value in Security Enhancement (0.8889) and Network Performance (0.875) indicates strong capabilities in these areas, although Implementation Cost (0.5714) is relatively lower, and Operational Complexity (0.8333) is moderate. The second row has values of 1, 1, 0.6667, and 0.7143, representing SDN with Hyper ledger Fabric. The perfect scores in Security Enhancement and Network Performance (1) highlight its leading position in these aspects. However, Implementation Cost (0.6667) and Operational Complexity (0.7143) are moderately high, suggesting some challenges in deployment and maintenance. For SDN with Coda Block chain, the values are 0.7778, 0.75, 0.8, and 0.8333. These figures indicate decent performance across Security Enhancement (0.7778), Network Performance (0.75), and Operational Complexity (0.8333), but Implementation Cost (0.8) is slightly higher, indicating moderate expenses.SDN with Quorum Block chain scores 0.8889, 0.875, 0.6667, and 1. The values reveal strong Security Enhancement and Network Performance, with the highest Operational Complexity score (1), which indicates a potentially higher challenge in operational deployment. Lastly, SDN with Multichip Block chain shows values of 0.6667, 0.625, 1, and 1. The high Implementation Cost (1) and Operational Complexity (1) make it the most challenging in these aspects, despite having lower scores in Security Enhancement (0.6667) and Network Performance (0.625).In summary, Hyper ledger Fabric and Quorum Block chain demonstrate the highest performance in Security Enhancement and Network Performance, while Multichip Block chain presents the highest challenges in Implementation Cost and Operational Complexity.

TABLE 3. Weighted normalized decision matrix

SDN with Ethereum Blockchain	0.970984	0.9672	0.8694	0.9554
SDN with Hyperledger Fabric	1	1	0.9036	0.9193
SDN with Corda Blockchain	0.939104	0.9306	0.9457	0.9554
SDN with Quorum Blockchain	0.970984	0.9672	0.9036	1
SDN with Multichain Blockchain	0.903602	0.8891	1	1

The weighted normalized decision matrix presents a more refined assessment of different SDN (Software-Defined Networking) implementations using block chain technologies, considering the importance of each criterion. The values reflect weighted scores for Security Enhancement (SE), Network Performance (NP), Implementation Cost (IC), and Operational Complexity (OC).The first row displays values of 0.970983543, 0.967168, 0.87, and 0.955443, representing the SDN with Ethereal Block chain. These high scores across all criteria indicate a well-rounded performance, with particularly strong Security Enhancement and Network Performance. The second row has perfect scores for Security Enhancement (1) and Network Performance (1), with Implementation Cost and Operational Complexity scores of 0.9 and 0.919323 respectively. This is for SDN with Hyper ledger Fabric, highlighting its superior performance in security and network efficiency, though with moderately high costs and complexity. The third row, with values of 0.939104416, 0.930605, 0.95, and 0.955443, represents SDN with Cords Block chain. The high scores across all dimensions indicate balanced performance, especially in Implementation Cost (0.95), making it a cost-effective choice with strong security and network performance. For SDN with Quorum Block chain, the values are 0.970983543, 0.967168, 0.9, and 1. These scores show robust performance in all areas, with the highest possible score in Operational Complexity (1), suggesting ease of operation alongside strong security and network performance. Lastly, the fifth row values (0.903602004, 0.88914, 1, and 1) reflect SDN with Multichip Block chain. While it scores lower in Security Enhancement and Network Performance, it achieves perfect scores in Implementation Cost and Operational Complexity, indicating it is the most cost-effective and operationally efficient option. In summary, Hyper ledger Fabric and Quorum Block chain are top performers in security and network performance, while Multichip Block chain excels in cost and operational efficiency. Ethereal and Cords Block chain also show strong, balanced performances across all criteria.

TABLE 4. Preference score

	Preference Score
SDN with Ethereum Blockchain	0.78012
SDN with Hyperledger Fabric	0.8307
SDN with Corda Blockchain	0.78969
SDN with Quorum Blockchain	0.84858
SDN with Multichain Blockchain	0.80343

The preference scores of different alternatives reveal their overall desirability based on evaluated criteria. These scores, ranging from 0 to 1, provide a quantitative measure of each alternative's favorability. The first alternative has a preference score of 0.780115773. This score indicates a generally positive evaluation, suggesting that this alternative performs well across various criteria but isn't the top choice. It is a reliable option but may have some areas that need improvement. The second alternative scores 0.830701847, reflecting a higher level of preference. This indicates a strong performance and suggests that it meets most of the evaluation criteria effectively, making it a highly regarded option. With a preference score of 0.789689537, the third alternative is slightly more favored than the first but not as much as the second. This score shows it is a solid option, performing well across most criteria and being a dependable choice. The fourth alternative achieves the highest preference score of 0.848576632. This top score highlights its superior performance and overall desirability, making it the most preferred choice. It likely excels across all evaluation criteria, resulting in its high ranking. Lastly, the fifth alternative scores 0.803428419, indicating it is also highly regarded. While not the top choice, it is still a strong contender and performs well across the board, making it a reliable and desirable option. In summary, these preference scores reveal that the fourth alternative is the most favored, followed by the second and fifth, with the first and third alternatives being slightly less preferred but still respectable choices. This ranking helps identify the most desirable options based on their evaluated performance.

TABLE 6. Rank

	Rank
SDN with Ethereum Blockchain	5
SDN with Hyperledger Fabric	2
SDN with Corda Blockchain	4
SDN with Quorum Blockchain	1
SDN with Multichain blockchain	3

The ranking of various alternatives, as indicated in the table, provides a clear hierarchy of their overall preference and desirability based on specific evaluation criteria. The alternative ranked fifth is considered the least preferred among the options. This position suggests that it may have notable shortcomings or perform less effectively in key areas compared to the others, making it the least desirable choice. The second-ranked alternative demonstrates a strong performance, indicating it meets most evaluation criteria effectively and is highly regarded. This high ranking reflects its overall balance and efficiency, making it a preferred option for many users. Ranked fourth, the next alternative shows a respectable performance but falls short compared to the top three. This ranking indicates it is a viable option but may have certain areas that need improvement to reach higher preference levels. The first-ranked alternative stands out as the most preferred choice. Its top position signifies superior performance across the evaluation criteria, making it the best option among the alternatives. This alternative likely excels in critical areas, leading to its high desirability. Lastly, the third-ranked alternative indicates a solid performance and is a better choice than the fourth and fifth but not as highly regarded as the top two. It offers a good balance of effectiveness and efficiency, making it a strong contender. In summary, the rankings reveal a clear preference hierarchy, with the first-ranked alternative being the most desirable, followed by the second and third, while the fourth and fifth rank lower in overall preference. This ranking helps identify the best options based on their evaluated performance.

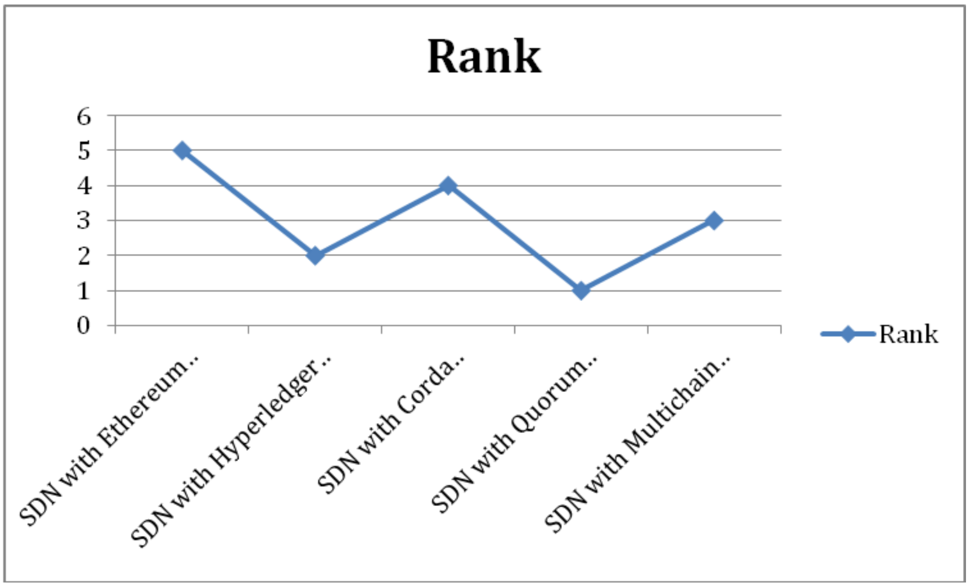

FIGURE 2. Rank

The ranking of various alternatives, as indicated in the table, provides a clear hierarchy of their overall preference and desirability based on specific evaluation criteria. The alternative ranked fifth is considered the least preferred among the options. This position suggests that it may have notable shortcomings or perform less effectively in key areas compared to the others, making it the least desirable choice. The second-ranked alternative demonstrates a strong performance, indicating it meets most evaluation criteria effectively and is highly regarded. This high ranking reflects its overall balance and efficiency, making it a preferred option for many users. Ranked fourth, the next alternative shows a respectable performance but falls short compared to the top three. This ranking indicates it is a viable option but may have certain areas that need improvement to reach higher preference levels. The first-ranked alternative stands out as the most preferred choice. Its top position signifies superior performance across the evaluation criteria, making it the best option among the alternatives. This alternative likely excels in critical areas, leading to its high desirability. Lastly, the third-ranked alternative indicates a solid performance and is a better choice than the fourth and fifth but not as highly regarded as the top two. It offers a good balance of effectiveness and efficiency, making it a strong contender. In summary, the rankings reveal a clear preference hierarchy, with the first-ranked alternative being the most desirable,

followed by the second and third, while the fourth and fifth rank lower in overall preference. This ranking helps identify the best options based on their evaluated performance.

4. CONCLUSION

In this paper, we presented an in-depth review of current SDN-based technologies applied to IoT systems, aiming to ensure smooth, affordable and dependable service delivery. We explored various networking aspects of IoT, including edge and access networking, and highlighted several key technical issues along with future research directions to tackle these problems. Additionally, we discussed the difficulties and needs related to "Networking infrastructure for core systems and data centers in the Internet of Things (IoT)." context, and offered a comparative analysis of existing schemes. The paper emphasizes common attacks and threats affecting "Different levels of IoT architecture, including issues like message interception, identity theft, unauthorized access, and the injection of malicious software code.". We also presented a real-world example of a successful smart home attack and discussed the security needs and challenges across different IoT applications. Given the potential for thousands of drones operating simultaneously in an urban setting, a key aim of the IoT architecture is to manage airspace access. To understand this, it is useful to first examine how congestion control operates on the Internet, where the objective is to ensure efficient and equitable use of bandwidth. [16]. The block chain paradigm is changing the IT industry. Block chain Block chain technology has the potential to unite companies, governments, and even nations. Its decentralized and peer-to-peer nature has earned it widespread recognition and value. This review paper provides a comprehensive analysis of various attacks on block chain and its associated security issues, supported by real-world examples. It explores the numerous security Challenges, vulnerabilities, and attacks that impede the widespread adoption of block chain technology from multiple perspectives. However, IoT environments, with their limited resources, high heterogeneity, and dynamic network topologies, present new challenges. Key technologies such as cryptographic algorithms, authentication protocols, consensus protocols, and reputation assessment models are crucial for enhancing the integration of block chain and Io T. [11]. Various distributed ledger designs have been proposed and put into practice across various application domains can be categorized based on four primary characteristics of distributed ledgers. The first characteristic is the access model, which specifies who has the authority to submit transactions, propose blocks, and views the block chain. The second is the token model, which addresses whether the block chain uses a token for crypto currency and value representation and transfer. The third component is the consensus protocol, which allows nodes to verify transactions and achieve a global agreement on the creation and acceptance of blocks.. Additionally, block chain offers smart contract functionalities that range from basic scripting to advanced smart contract programming languages capable of Turing-complete computations. With the rise of Io T, various security vulnerabilities, including device and data-in-transit attacks, have garnered significant research attention. The broad application of Io T in industries has led to the development of Industrial Io T (IIoT) as a distinct research area. The close integration of the physical and virtual worlds through intelligent systems has exacerbated vulnerabilities in Industrial Io T systems. This paper examines Io T-specific security issues and solutions, with a particular focus on IIo T. We assert that, to our knowledge, this is the first report to categorize attacks in Io T based on the objects involved. This classification will greatly aid researchers, practitioners, and industry professionals in identifying relevant attacks for their specific areas of interest. Furthermore, the integration of block chain technology into both Io T and IIo T has demonstrated advantages over traditional centralized systems. A detailed taxonomy provided here will offer researchers a clearer comprehension of key security challenges and solutions in IoT and IIoT

REFERENCES

[1]. Sengupta, Jayasree, Sushmita Ruj, and Sipra Das Bit. "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT." Journal of network and computer applications 149 (2020): 102481.

[2]. Meng, Weizhi, Wenjuan Li, and Jianying Zhou. "Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration." Information Fusion 70 (2021): 60-71.

[3]. Pohrmen, Fabiola Hazel, Rohit Kumar Das, and Goutam Saha. "Blockchain-based security aspects in heterogeneous Internet-of-Things networks: A survey." Transactions on Emerging Telecommunications Technologies 30, no. 10 (2019): e3741.

[4]. Yazdinejad, Abbas, Reza M. Parizi, Ali Dehghantanha, Qi Zhang, and Kim-Kwang Raymond Choo. "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security." IEEE Transactions on Services Computing 13, no. 4 (2020): 625-638.

[5]. Argiriou, Athanassios A., Ioannis Bellas-Velidis, and Constantinos A. Balaras. "Development of a neural network heating controller for solar buildings." Neural Networks 13, no. 7 (2000): 811-820.

[6]. Prabadevi, B., Natarajan Deepa, Quoc-Viet Pham, Dinh C. Nguyen, Thippa Reddy, Pubudu N. Pathirana, and Octavia Dobre. "Toward blockchain for edge-of-things: a new paradigm, opportunities, and future directions." IEEE Internet of Things Magazine 4, no. 2 (2021): 102-108.

[7]. Voulgaris, Spyros, Nikos Fotiou, Vasilios A. Siris, George C. Polyzos, Mikael Jaatinen, and Yannis Oikonomidis. "Blockchain technology for intelligent environments." Future Internet 11, no. 10 (2019): 213.

[8]. Khor, Jing Huey, Michail Sidorov, and Peh Yee Woon. "Public blockchains for resource-constrained IoT devices—A state-of-the-art survey." IEEE Internet of Things Journal 8, no. 15 (2021): 11960-11982.

[9]. Alharbi, Talal. "Deployment of blockchain technology in software defined networks: A survey." IEEE Access 8 (2020): 9146-9156.

[10]. 10, Wei, Lijun, Jing Wu, Chengnian Long, and Yi-Bing Lin. "The convergence of IoE and blockchain: security challenges." IT Professional 21, no. 5 (2019): 26-32.

[11]. Al Sadawi, Alia, Mohamed S. Hassan, and Malick Ndiaye. "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges." IEEe Access 9 (2021): 54478-54497.

[12]. Singh, Saurabh, ASM Sanwar Hosen, and Byungun Yoon. "Blockchain security attacks, challenges, and solutions for the future distributed iot network." Ieee Access 9 (2021): 13938-13959.

[13]. Hu, Jiejun, Martin Reed, Nikolaos Thomos, Mays F. AI-Naday, and Kun Yang. "Securing SDN-controlled IoT networks through edge blockchain." IEEE Internet of Things Journal 8, no. 4 (2020): 2102-2115.

[14]. Hakiri, Akram, and Behnam Dezfouli. "Towards a blockchain-SDN architecture for secure and trustworthy 5G massive IoT networks." In Proceedings of the 2021 ACM international workshop on software defined networks & network function virtualization security, pp. 11-18. 2021.

[15]. Gharibi, Mirmojtaba, Raouf Boutaba, and Steven L. Waslander. "Internet of drones." IEEE Access 4 (2016): 1148-1162.

[16]. Jesus, Emanuel Ferreira, Vanessa RL Chicarino, Célio VN De Albuquerque, and Antônio A. de A. Rocha. "A survey of how to use blockchain to secure internet of things and the stalker attack." Security and communication networks 2018, no. 1 (2018): 9675050

[17]. Iqbal, Waseem, Haider Abbas, Mahmoud Daneshmand, Bilal Rauf, and Yawar Abbas Bangash. "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security." IEEE Internet of Things Journal 7, no. 10 (2020): 10250-10276..

[18]. Pavithran, Deepa, Khaled Shaalan, Jamal N. Al-Karaki, and Amjad Gawanmeh. "Towards building a blockchain framework for IoT." Cluster Computing 23, no. 3 (2020): 2089-2103.

[19]. Tselios, Christos, Ilias Politis, and Stavros Kotsopoulos. "Enhancing SDN security for IoT-related deployments through blockchain." In 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 303-308. IEEE, 2017.

[20]. Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future generation computer systems 82 (2018): 395-411.

[21]. Bera, Samaresh, Sudip Misra, and Athanasios V. Vasilakos. "Software-defined networking for internet of things: A survey." IEEE Internet of Things Journal 4, no. 6 (2017): 1994-2008.

[22]. Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo. "A blockchain future for internet of things security: a position paper." Digital Communications and Networks 4, no. 3 (2018): 149-160.

[23]. Wang, Xu, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, Xinxin Niu, and Kangfeng Zheng. "Survey on blockchain for Internet of Things." Computer Communications 136 (2019): 10-29.

[24]. Ferrag, Mohamed Amine, and Lei Shu. "The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial." IEEE Internet of Things Journal 8, no. 24 (2021): 17236-17260.

[25]. Meng, Weizhi, Wenjuan Li, and Jianying Zhou. "Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration." Information Fusion 70 (2021): 60-71.

[26]. Ferrag, Mohamed Amine, and Lei Shu. "The performance evaluation of block chain-based security and privacy systems for the Internet of Things: A tutorial." IEEE Internet of Things Journal 8, no. 24 (2021): 17236-17260.

[27]. Hu, Jiejun, Martin Reed, Nikolaos Thomos, Mays F. AI-Naday, and Kun Yang. "Securing SDN-controlled IoT networks through edge block chain." IEEE Internet of Things Journal 8, no. 4 (2020): 2102-2115.

[28]. Astely, David, Erik Dahlman, Gabor Fodor, Stefan Parkvall, and Joachim Sachs. "LTE release 12 and beyond [accepted from

[29]. Lay, Clarry H. "At last, my research article on procrastination." Journal of research in personality 20, no. 4 (1986): 474-495.en call]." IEEE Communications Magazine 51, no. 7 (2013): 154-160

[30]. Rogova, Galina L., and Vincent Nimier. "Reliability in information fusion: literature survey." In Proceedings of the seventh international conference on information fusion, vol. 2, pp. 1158-1165. 2004

