Blockchain-Enabled Secure Device-to-Device Communication in Software-Defined Networking

Debashis Das*, Uttam Ghosh†, Nate Evans‡, and Sachin Shetty§

*†Department of CS and DS, Meharry Medical College, TN, USA
‡Oak Ridge National Laboratory, Knoxville, TN, USA
§Old Dominion University, VA, USA
debashis.das@ieee.org*, ghosh.uttam@ieee.org†, evansn@ornl.gov‡, sshetty@odu.edu§

2024 IEEE International Conference on Communications Workshops (ICC Workshops) | 979-8-3503-0405-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCWORKSHOPS59551.2024.10615611

***Abstract*—The Internet of Things (IoT) continues to increase the demand for seamless communication among IoT devices. The rapid growth of IoT devices has led to an exponential increase in device-to-device (D2D) communication within the Software-Defined Networking (SDN), though it enables a flexible architecture for managing network resources. However, traditional security models face challenges (e.g., Security, privacy, and trust) in addressing the dynamic and decentralized nature of these communications. Despite of these challenges, this paper proposes a novel approach that leverages blockchain technology to enhance the security, privacy, and trustworthiness of D2D communication within an SDN environment. The proposed approach integrates blockchain nodes in sDN components to establish a decentralized ledger for transparent and verifiable records. Smart contracts enforce authentication rules to ensure that only authenticated devices can access the network and engage in transactions securely. It also automates the security policies to ensure temper resistance execution using the cryptographic mechanism for data integrity and authentic communication. The Implementation of the proposed algorithms validates the resilience of the proposed approach against cyberattacks. Overall, the proposed approach enables efficient and secure D2D communication for resilient SDN infrastructure in IoT ecosystems.**

***Index Terms*—Blockchain, software-defined networking, communication, device security, and smart contracts.**

I. Introduction

The swift proliferation of the Internet of Things (IoT) devices [1] has catalyzed an unprecedented surge in device-to-device (D2D) communication, particularly within the dynamic landscape of software-defined networking (SDN) architectures. These devices can range from everyday objects like household appliances and wearable devices to industrial machinery and smart infrastructure components. D2D communication can continue to communicate with each other even when internet connectivity is unavailable. D2D communication [2] facilitates real-time interactions between devices to enable faster response times and more immediate feedback. This is particularly important for SDN-enabled applications such as home automation, industrial control systems, and emergency response systems where timely communication is critical. D2D communication can enhance privacy by allowing devices to exchange sensitive data directly without passing through potentially insecure network intermediaries. This direct communication reduces the risk of data interception or eavesdropping [3].

However, D2D communication introduces vulnerabilities such as unauthorized access, data breaches, and malware propagation due to the direct exchange of data between devices. Privacy issues also arise from the potential exposure of sensitive information during D2D interactions [4]. The dynamic and decentralized nature of these communications strains conventional security measures, raising concerns about privacy breaches, data integrity, and trust in the evolving SDN landscape [5]. The impact of the challenges lies in the potential compromise of security, privacy, and data integrity within the rapidly evolving landscape of D2D communication in SDN architectures [6]. Traditional security models can not keep up with the exponential growth of devices that are connected [7]. There is a need for a novel approach to completely change how we protect these dynamic and decentralized communications [8]. This research focuses on addressing these challenges faced by traditional security paradigms to redefine the contours of security, privacy, and trust in the intricate web of D2D communication [9].

In response to these challenges, this paper proposes a novel D2D communication framework using Blockchain [10] to enhance the security, privacy, and trustworthiness of D2D communication within SDN environments. Blockchain's decentralized ledger not only promises a robust foundation for transparent transaction verification but also introduces the concept of smart contracts. [11]. The paper presents an identity generation mechanism and provides a secure authentication mechanism for devices engaged in D2D communication. In essence, this paper envisions a future where blockchain technology becomes integral to addressing the intricate security challenges posed by the burgeoning D2D communication landscape within SDN architectures. This work not only responds to the current imperatives of securing IoT-driven communications but also pioneers a path toward a more secure, private, and trust-oriented future. Moreover, Blockchain can be integrated with SDN to enhance the security, transparency, and integrity of D2D communication in various applications, including healthcare, finance, and IoT.

Contribution: The paper makes significant contributions to addressing the challenges posed by the dynamic and decentralized nature of D2D communication within SDN architectures. The key contributions include:

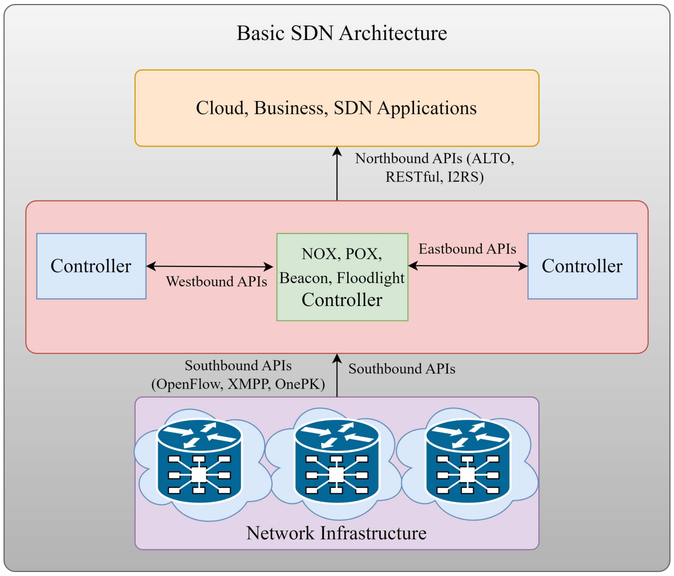

Fig. 1: An overview of basic SDN architecture.

• The paper introduces the integration of blockchain technology into SDN environments to establish a transparent and decentralized ledger for secure transaction verification, data integrity, and authentication in D2D communication.
• The paper also depicts a transparent transaction verification mechanism for the authenticity of D2D communication transactions and enhancement of the overall trustworthiness of the communication process.
• The paper proposes the use of smart contracts to automate and enforce security policies within the proposed approach to streamline the execution of security protocols.
• The paper introduces cryptographic hashes to verify the integrity of data exchanged in D2D communication.

Paper Organization: The remaining part of the paper is structured as follows. Section II explores the fundamentals of SDN architectures and provides an in-depth overview of blockchain technology. Section III outlines the proposed framework and describes the implementation of smart contracts and the decentralized ledger for transaction recording. In Section IV, performance analysis of the proposed approach is discussed. Finally, Section V concluded the paper with relevant future directions.

II. Background and Related Works

A. Software-Defined Networking

Software-Defined Networking (SDN) represents a paradigm shift in network architecture, providing a dynamic and programmable approach to network management [12]. Fig. 1 shows the basic architecture of SDN. Unlike traditional networking, where the control plane and data plane functions are tightly integrated within network devices, SDN decouples these functions. In SDN, the control plane is centralized and managed by a software-based controller, while the data plane remains distributed among network devices.

1) Challenges in Securing D2D Communication within SDN: While SDN brings numerous advantages, securing D2D communication within this architecture presents unique challenges [13], [14]:

Dynamic Nature D2D communication is inherently dynamic, with devices forming ad-hoc connections based on contextual factors. Traditional security models designed for static network infrastructures struggle to adapt to this dynamic nature, making it challenging to enforce consistent security policies.

Decentralization SDN's centralized control is juxtaposed with the decentralized nature of D2D communication [15]. As devices communicate directly with each other, ensuring end-to-end security becomes complex, requiring mechanisms that go beyond the centralized controller.

Privacy Concerns D2D communication often involves sensitive data exchange. Privacy concerns arise as traditional security mechanisms may lack the granularity needed to protect individual device communications, potentially leading to unauthorized access.

Scalability As the number of IoT devices increases, Scalability becomes a concern. Traditional security approaches may struggle to scale efficiently, potentially leading to performance bottlenecks.

B. Blockchain Technology

Blockchain is a distributed and decentralized ledger technology that enables secure, transparent, and tamper-resistant record-keeping [16]. It consists of a chain of blocks, where each block contains a list of transactions, and these blocks are linked using cryptographic hashes. The decentralized nature of blockchain ensures that no single entity has control over the entire network.

1) Blockchain in Enhancing Security and Trust: Blockchain technology plays a significant role in enhancing security and trust across various applications, including D2D communication within SDN environments [17]. Here are some key aspects of how blockchain contributes to security and trust enhancement:

Transparent Transaction Verification Blockchain's transparent nature ensures that all transactions are recorded and visible to participants. In SDN, this can be applied to verify and audit transactions related to D2D communication, reducing the risk of unauthorized access.

Smart Contracts for Automation Smart contracts, self-executing code on the blockchain can automate security policies in D2D communication. These contracts can define and enforce rules, ensuring that security protocols are consistently applied without relying on a central authority.

Decentralized Identity Management Blockchain provides a decentralized approach to identity management. Each device can have a unique cryptographic identity stored on the blockchain, enhancing authentication and reducing the risk of impersonation in D2D communication.

Consensus Mechanisms for Trust The blockchain relies on consensus mechanisms to validate transactions. Consensus

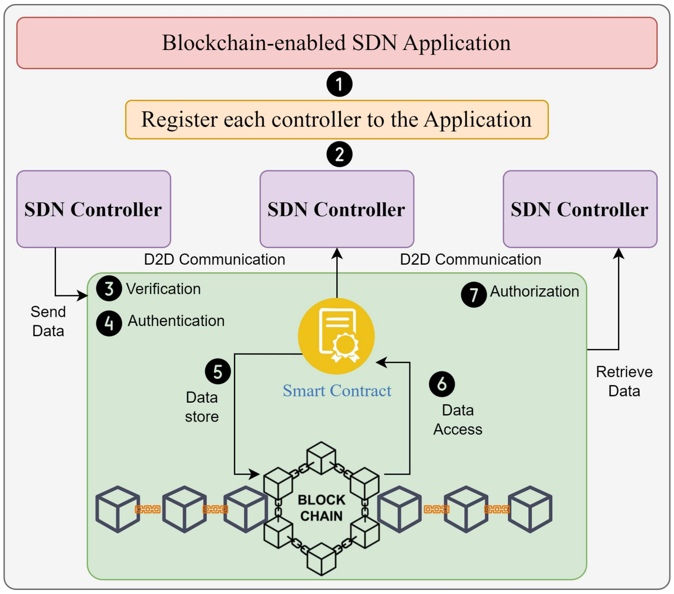

Fig. 2: Proposed blockchain-enabled D2D communication in SDN.

ensures agreement among network participants, enhancing trust in the integrity of the blockchain. This can be leveraged in SDN to establish trust among devices participating in D2D communication.

III. PROPOSED BLOCKCHAIN-ENABLED SDN FRAMEWORK

This section provides the mathematical representations of the proposed framework for understanding the integration of blockchain into SDN architecture. These representations help express the relationships and processes involved in creating a decentralized and secure environment. Fig. 2 shows the proposed architecture for D2D communication within in SDN network.

A. Blockchain Integration

Blockchain integration into SDN involves incorporating a blockchain layer to enhance the security and transparency of network transactions. This can be achieved by deploying blockchain nodes across the SDN infrastructure. Each SDN controller and network device can be a participant in the blockchain network. The integration process includes:

1) Blockchain Nodes in SDN Components: The set of nodes in the SDN architecture participating in the blockchain network can be represented as:

$$\text{Nodes} = \{\partial, \eta_1, \eta_2, \ldots, \eta_n\} \tag{1}$$

∂ represents the centralized control entity in the SDN architecture. It manages and oversees the network's overall operation, making decisions and controlling the flow of data. The set includes individual network devices, denoted as $\eta_1, \eta_2, \ldots, \eta_n$. These devices can be routers, switches, or any other network components in the SDN infrastructure. The variable n represents the total count of network devices in the SDN infrastructure. The specific value of n depends on the size and complexity of the network.

2) Consensus Mechanism Integration: The integration of a consensus mechanism can be represented mathematically as a function:

$$C_M(\partial, \eta_1, \eta_2, \ldots, \eta_n) \tag{2}$$

The parameters of the function include the SDNController and individual network devices $(\eta_1, \eta_2, \ldots, \eta_n)$. These entities are participants in the consensus process. The purpose of this function is to ensure agreement among the nodes (SDNController and network devices) on the validity of transactions within the blockchain. The consensus mechanism is responsible for establishing a common understanding of the state of the blockchain.

3) Decentralized Ledger for D2D Communication: The blockchain ledger for recording transactions related to D2D communication is represented as a series of blocks linked together through cryptographic hashes as shown in equation 3. The blockchain ledger is a sequence of blocks $(\varpi_1, \varpi_2, \ldots, \varpi_n)$, where each block stores a set of transactions related to D2D communication.

$$\text{B} = \{\varpi_1, \varpi_2, \ldots, \varpi_m\} \tag{3}$$

where, Each block ϖ contains a set of transactions $(T_{i1}, T_{i2}, \ldots, T_{in})$, representing the recorded D2D communication transactions.

$$\varpi_i = \{T_{i1}, T_{i2}, \ldots, T_{in}\} \tag{4}$$

The linkage between blocks is established using cryptographic hash functions. The hash of each block $\hbar_{T_i}$ is computed by including the previous block's hash $\hbar_{T_{i-1}}$ as part of the equation 5

$$\hbar_{T_i} = \nabla(B_i, \hbar_{T_{i-1}}) \tag{5}$$

Cryptographic hash functions are algorithms that produce a fixed-size hash value from input data. In this case, the hash

Algorithm 1: Initialization

Data: For each device i: (pk_i, sk_i), Exchange, Storage.

foreach *device* i **do**
- Generate a unique public-private key pair for asymmetric cryptography: (pk_i, sk_i);
- Exchange public keys securely between devices through a secure initial pairing process or a trusted third party:
  Exchange: $pk_i \leftrightarrow pk_j$;
- Store the public keys of the devices securely:
  Storage: Device $i \rightarrow$ Secure Storage;

Algorithm 2: Data Encryption and Decryption

Data: Encryption, Session Key, Decryption.

foreach *sender device* **do**
- Encrypt the data using the recipient's public key: **Encryption (Sender):** $EncryptedData_{ij} = Encrypt(Data, pk_j)$;
- Generate an additional symmetric key (session key) for efficient encryption of large amounts of data: **Session Key:** $SessionKey_{ij} = GenerateSessionKey()$;

foreach *receiver device* **do**
- Decrypt the received data using its private key: **Decryption (Receiver):** $DecryptedData_j = Decrypt(EncryptedData_{ij}, sk_j)$;
- If a symmetric key was used, decrypt the remaining data with the session key: $RemainingData_j = Decrypt(SessionKey_{ij}, EncryptedRemainingData_{ij})$;

function is applied to the current block B_i, and the hash of the previous transaction ($\hbar_{T_i}$). The use of cryptographic hashes ensures immutability within the blockchain ledger. If any data in a previous block is altered, it would change the hash, breaking the linkage and making the tampering evident. The above explained captures the structure of the blockchain ledger for D2D communication. It emphasizes the connection between blocks through cryptographic hashes, providing a secure and tamper-resistant record of transactions. This ensures that the blockchain maintains its integrity and immutability, critical aspects for enhancing security and trust in D2D communication within SDN environments.

B. Smart Contract for Security Policies

1) Smart Contract Deployment: Smart contracts can be deployed to automate and enforce security policies within the SDN framework. These contracts, executed on the blockchain, provide a tamper-resistant and automated way to manage the security aspects of D2D communication. The automated execution of smart contracts involves programming SDN controllers to automatically execute these contracts based on predefined triggers or conditions. Let $\omega, \phi, and \varrho$ be Policy AccessControl, Policy Encryption, and Policy Authentication are specific rules within the smart contract respectively.

$$SC_{Security} = \{\omega, \phi, \varrho, \ldots\} \tag{6}$$

An optimization equation can be introduced to balance various security parameters, denoted as φ.

$$\varphi = \text{Optimize}(\alpha \cdot \omega + \beta \cdot \phi + \gamma \cdot \varrho) \tag{7}$$

where, $\alpha, \beta, and \gamma$ are weights assigned to each policy, reflecting their relative importance.

2) Automated Execution: The automated execution of smart contracts involve programming SDN controllers to automatically execute these contracts based on predefined triggers or conditions. A mathematical representation, denoted as E_{SC} can be expressed as:

$$E_{SC} = \text{If}(Tgr_{NewD2DCommunication}, \text{Execute}(SC_{Security})) \tag{8}$$

Where Trigger NewD2DCommunication represents a condition triggering the execution of the smart contract when new D2D communication is established.

Aligning the optimization equation with the execution process, taking into account the optimized security parameters. $SC_{Security}$ encapsulates various security policies, providing a clear representation of the rules governing D2D communication. The optimization equation φ reflects a trade-off between different security policies, allowing for the fine-tuning of weights based on their relative importance. E_{SC} ensures that the smart contract is executed automatically when triggered conditions, such as $Tgr_{NewD2DCommunication}$, are met. Aligning the optimization equation with the execution process reinforces the idea that the execution of security policies is not arbitrary but follows a well-defined optimization strategy.

C. Security and Privacy Enhancements

1) Transparent Transaction Verification: All transactions related to D2D communication are recorded on the blockchain ledger. To verify a transaction, nodes in the network can refer to the blockchain ledger to ensure the transaction's authenticity. Transparent transaction verification involves leveraging blockchain technology to ensure that transactions related to D2D communication are not only recorded securely but can also be easily verified for authenticity.

$$Verification_T = \text{ReferTo}(B) \tag{9}$$

Algorithm 3: Data Authentication

Data: Message Authentication Code (MAC), Data with MAC, Calculated MAC.

foreach *sender device* **do**
- Calculate a MAC using a shared secret key: **MAC:** $MAC_{ij} = HMAC(Data, SharedKey_{ij})$;
- Send the MAC along with the data: $DatawithMAC_{ij} = (Data, MAC_{ij})$;

foreach *receiver device* **do**
- Calculate its own MAC using the received data and the shared secret key: $CalculatedMAC_j = HMAC(ReceivedData_{ij}, SharedKey_{ij})$;
- If the calculated MAC matches the received MAC, the data is considered authentic.

Algorithm 4: Device Authentication

Data: Challenge-Response, Response, Verification.

foreach *initiating device* **do**
- Send a challenge to the responding device: **Challenge-Response Authentication:** $Challenge_{ij} = GenerateChallenge();$
- The responding device signs the challenge with its private key and sends it back: $Response_{ij} = Sign(Challenge_{ij}, sk_j);$
- The initiating device verifies the signature using the responding device's public key: $Verification = Verify(Challenge_{ij}, Response_{ij}, pk_j);$

Algorithm 5: Secure Communication

Data: Secure Communication.

foreach *device* **do**
- Exchange data securely using the established encryption keys, ensuring confidentiality and integrity: **Secure Communication:** $SecureCommunication_{ij} = Encrypt(Data, SessionKey_{ij});$
- Periodic rekeying may be performed to enhance security.

Equation 9 uses the blockchain ledger B to verify the authenticity of a specific transaction, denoted as T_{D2D}. $Verification_T$ represents the process of referencing the blockchain ledger to verify the authenticity of a specific D2D communication transaction.

$Hash_T$ ensures transparency and integrity of transactions. The use of cryptographic hashes links each transaction to the previous one, making it computationally infeasible to alter past transactions.

$$Verification_T = \text{VerifyAuthenticity}(T_{D2D}) \tag{10}$$

2) Cryptographic Hashes: Here, we use cryptographic hashes to link each transaction to the previous one, ensuring transparency and making it computationally infeasible to alter past transactions $\hbar_T$. To ensure transparency and tamper resistance, cryptographic hashes are used to link each transaction to the previous one. Cryptographic hash functions are applied to each transaction to generate a unique hash value. Let $\hbar_{D2D}$ represent the hash of a D2D communication transaction.

$$\hbar_{T_{D2D}} = \nabla(T_{D2D}) \tag{11}$$

To ensure transparency and immutability, link each transaction to the previous one using cryptographic hashes.

$$Hash_{T_{D2D}} = \nabla(T_{D2D}, Hash_{T_{PreviousD2D}}) \tag{12}$$

D. Data Integrity and Authentication

Blockchain is employed to enhance data integrity and authentication in D2D communication, ensuring the reliability and security of exchanged information.

1) Data Integrity Verification: The representation of the process of verifying data integrity is denoted as V_DI.

$$Hash_{Data} = CryptographicHash(Data) \tag{13}$$

Verify the integrity of the data by comparing the calculated hash with the one recorded on the blockchain.

$$V_{DI} = \text{Verify}(Hash_{Data}, Hash_{RecordedData}) \tag{14}$$

V_DI ensures the integrity of data by comparing the cryptographic the hash of exchanged data with the one recorded on the blockchain, providing a reliable method for confirming data integrity.

2) Decentralized Identity Management: Utilizing the blockchain for decentralized identity management can enhance authentication in D2D communication. Mathematically representing the concept as I_B. Each device in the D2D communication network has a unique cryptographic identity stored on the blockchain, denoted as I_D.

$$I_B = \text{UniqueCryptographicIdentity} \tag{15}$$

I_B represents the decentralized identity management on the blockchain, providing each device with a unique cryptographic identity. This identity is then used for authentication in D2D communication.

IV. Performance Analysis

The performance analysis section of the paper is crucial in evaluating the effectiveness of the proposed blockchain-enabled SDN framework in enhancing security, privacy, and trust in D2D communication. Algorithm (1-5) shows the stepwise implementation process of the proposed method. However, this analysis involves assessing various metrics and parameters to gauge the efficiency and viability of the proposed solution.

A. Transaction Throughput: A high transaction throughput is indicative of a robust and scalable system, capable of efficiently processing a large number of transactions concurrently. This is particularly crucial in the realm of D2D communication, where real-time interactions demand swift and secure transaction processing. The evaluation of transaction throughput thus providing a comprehensive understanding of the blockchain-enabled SDN framework's ability to meet the demands of a dynamic and decentralized communication environment, ensuring a secure and timely exchange of information among interconnected devices.

B. Security: Security within the proposed blockchain-enabled SDN framework is meticulously addressed through a multi-faceted approach. The integration of blockchain technology serves as a foundational element, introducing decentralization, transparency, and cryptographic principles. Cryptographic mechanisms, including encryption and hashing, are strategically employed to secure data integrity and authenticate D2D communication. The decentralized ledger provides a transparent and immutable record of transactions, mitigating risks of unauthorized access and manipulation. The seamless integration of these security measures establishes a robust and resilient framework, fostering a secure environment for D2D communication within the SDN architecture.

C. Trust: The deployment of decentralized ledger technology introduces transparency in transaction verification, providing stakeholders with a verifiable and immutable record. Smart contracts, executed within the framework, automate security policies, contributing to a tamper-resistant execution that fosters trust in the enforcement of predefined rules. The decentralized identity management system, powered by blockchain, assures the uniqueness and integrity of device identities, enhancing trust in the authenticity of participants in D2D communication. Through these measures, the proposed framework not only enhances security but also establishes a foundation for trust among network participants, laying the groundwork for a reliable and resilient SDN environment.

D. Resilience to Attacks: Blockchain provides a transparent and secure method for authenticating devices and participants in the network. Through cryptographic keys and digital signatures, the identity of each participant can be verified without the need for a central authentication authority. This transparency builds trust among devices and entities in the network. The decentralized nature of blockchain makes it more resilient to Sybil attacks, where a malicious actor creates multiple fake identities to gain control over a network. In a blockchain-based system, achieving control would require a majority of honest nodes, making it significantly more challenging for attackers to compromise the network.

V. Conclusions

D2D communication requires security and trust as it allows devices to directly exchange data with each other through a central network infrastructure. This paper presents a new approach to make D2D communication in SDN environments more safer and secure using Blockchain. The proposed approach effectively enhances the security, privacy, and trust of D2D communication within SDN environments. Herein, Blockchain's decentralized ledger ensures transparent and tamper-proof records and enhances trust among network participants. Transparent transaction verification and immutable records build trust by providing verifiable evidence of data integrity and authenticity. Smart contracts automate security policies to ensure the execution of reliable and secure transactions among devices. Through data encryption and decryption, data authentication, and secure communication algorithms, the proposed approach provides trust and a robust authentication method for securing D2D interaction with SDN. Looking ahead, future research could focus on further optimizing resource utilization and scalability and efficiency of the proposed blockchain-enabled SDN framework.

Acknowledgement

This work was supported by the National Science Foundation, under award number 2219741.

References

[1] D. Das, S. Banerjee, and U. Biswas, *Cloud-Based Smart IoT Architecture and Various Application Domains*. Cham: Springer International Publishing, 2020, pp. 199–226. [Online]. Available: https://doi.org/10.1007/978-3-030-40037-8_11

[2] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, U. Biswas, and W. Mansoor, "Security, trust, and privacy management framework in cyber-physical systems using blockchain," in *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*. IEEE, 2023, pp. 1–6.

[3] A. Iqbal, A. Nauman, R. Hussain, I. L. Khan, A. Khaqan, S. Shuja, and S. W. Kim, "Device discovery in d2d communication: Scenarios and challenges," *CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 75, no. 1, pp. 1735–1750, 2023.

[4] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain for intelligent transportation systems: Applications, challenges, and opportunities," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18 961–18 970, 2023.

[5] D. Das, S. Banerjee, K. Dasgupta, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain enabled sdn framework for security management in 5g applications," in *Proceedings of the 24th International Conference on Distributed Computing and Networking*, 2023, pp. 414–419.

[6] D. Carrascal, E. Rojas, J. M. Arco, D. Lopez-Pajares, J. Alvarez-Horcajo, and J. A. Carral, "A comprehensive survey of in-band control in sdn: Challenges and opportunities," *Electronics*, vol. 12, no. 6, p. 1265, 2023.

[7] D. Das, K. Dasgupta, and U. Biswas, "A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems," *Computers and Electrical Engineering*, vol. 105, 2023.

[8] K. Park, S. Sung, H. Kim, and J.-i. Jung, "Technology trends and challenges in sdn and service assurance for end-to-end network slicing," *Computer Networks*, p. 109908, 2023.

[9] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, W. Mansoor, and U. Biswas, "Design of an automated blockchain-enabled vehicle data management system," in *2022 5th International Conference on Signal Processing and Information Security (ICSPIS)*, 2022, pp. 22–25.

[10] T. Wang, H. Yang, and Q. Li, "Collaborative d2d cache system based on sdn network," in *2023 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, 2023, pp. 1–4.

[11] S. Windarta, S. Suryadi, K. Ramli, B. Pranggono, and T. S. Gunawan, "Lightweight cryptographic hash functions: Design trends, comparative study, and future directions," *IEEE Access*, pp. 82 272–82 294, 2022.

[12] D. Marikyan, S. Papagiannidis, O. F. Rana, and R. Ranjan, "Blockchain adoption: A study of cognitive factors underpinning decision making," *Computers in Human Behavior*, vol. 131, p. 107207, 2022.

[13] Y. Yu, J. Zhang, H. Lin, and Q. Fang, "A green energy efficient d2d cooperative communication," in *2023 4th International Conference on Electronic Communication and Artificial Intelligence*, 2023, pp. 62–65.

[14] K. K. Eren and K. Küçük, "Improving intrusion detection systems for iot devices using automated feature generation based on ton_iot dataset," in *2023 8th International Conference on Computer Science and Engineering (UBMK)*, 2023, pp. 276–281.

[15] D. D. Ningombam, S.-s. Hwang, and S. Shin, "Decentralized resource allocation for multicast d2d communications using stochastic geometry," in *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, 2019, pp. 703–706.

[16] M. S. Farooq, S. Riaz, and A. Alvi, "Security and privacy issues in software-defined networking (sdn): A systematic literature review," *Electronics*, vol. 12, no. 14, p. 3077, 2023.

[17] M. B. Jimenez, D. Fernandez, J. E. Rivadeneira, L. Bellido, and A. Cardenas, "A survey of the main security issues and solutions for the sdn architecture," *IEEE Access*, vol. 9, pp. 122 016–122 038, 2021.