Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2024 5(1), 2269–2277

A HYBRID FRAMEWORK FOR SECURE DEVICE-TO-DEVICE COMMUNICATION IN WIRELESS SYSTEMS USING BLOCKCHAIN AND ONION ROUTING

Kiran Bhavlal Jadhav[1], Dr. Manoj Kumar Nigam[2], Dr. Sagar Bhilaji Shinde[3]

[1] Research Scholar, Department of Electronics Engineering, Kalinga University, Raipur, (CG), India
[2] Professor, Department of Electronics Engineering, Kalinga University, Raipur, (CG), Indi
[3]Professor, Department of Computer Science Engineering-AI, Nutan College of Engineering and Research, Pune, India

ABSTRACT

This study introduces a hybrid architecture that uses Blockchain and onion routing to solve important privacy and security issues with Device-to-Device (D2D) communication in wireless networks. The need for secure communication is growing in tandem with the number of Internet of Things (IoT) devices, leaving traditional D2D systems open to typical dangers like eavesdropping and man-in-the-middle (MITM) attacks. To improve user privacy and data security, the suggested system combines onion routing's multilayer encryption with Blockchain's decentralised authentication. The performance, security resilience, and resource utilisation of the framework were evaluated thoroughly. The results showed that the attack success rates were significantly lower than those of previous models. With its benefits in protecting sensitive communications, the hybrid framework is especially well-suited for applications in smart cities, healthcare, and finance, despite the fact that it does incur greater latency and resource demands. The research results support the use of hybrid security solutions in D2D communication, which strike a balance between security and performance. In the future, we will optimise this framework to operate better in contexts with limited resources and look into other ways to make it even better at securing user data in our linked world.

Keywords: Hybrid Framework, Secure, Wireless Systems, Blockchain, Onion Routing

Corresponding Author
Kiran Bhavlal Jadhav,
jadhavkiran32@gmail.com

DOI
10.29121/shodhkosh.v5.i1.2024.2352

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

Internet of Things (IoT) smart city applications benefit greatly from the technology, yet there are security holes that may severely impact the whole communication system if left unchecked. D2D communications are dangered by several elements. There is a serious risk of node impersonation, eavesdropping, and message manipulation. Intruders can covertly monitor data transmissions sent over wireless channels. For that reason, sensitive data could be inappropriately exploited

(Ait Ali, A. 2020). A malicious actor can trick a recipient into thinking they're receiving data from a legitimate node. Because an attacker can change the message's payload, confusion and unexpected outcomes are possible. Hackers can use a Man-in-the-middle (MITM) attack to sabotage direct-to-device (D2D) communications. Recipient and sender authentication is thus required in order to ensure the integrity of the message (Hossain, E. 2019). Flood attacks can interrupt legitimate entities' connection by flooding the target device with discovery requests, making it difficult to reach the device in a timely manner. D2D communications rely on robust discovery mechanisms, even if the technology has great potential. In order to ensure the safety of D2D communications, the traditional approaches were insufficient (Pimenta, L. L. 2021). There may be possibilities for a secure D2D communication system, thanks to the recent success of Blockchain in securing wireless communication networks. However, D2D communication systems, such as Vehicular Ad Hoc Networks (VANETs), still lacked full security when employing Blockchain technology alone. Innovative methods for secure D2D communications based on Blockchain and onion routing are the goal of this study (Bhattacharjee, K. 2018). Direct data transmission between mobile devices, without the requirement for an eNB, is known as device-to-device (D2D) communication. Efficiency in device-to-device (D2D) communication in LTE-Advanced (LTE-A) networks is the primary focus of this thesis, which delves into the design issues surrounding this topic (Zhang, Y. 2020). Few direct-to-device (D2D) methods have been created for data transfer. Three different technologies are involved: Bluetooth, WiFi, and ZigBee. There is a complicated barrier to enabling direct connection between adjacent mobile devices for data or information sharing (Wang, T. 2019). Current technology's uplink and downlink modes are insufficient for these goals. By providing consumers with extended connection, distance-based decentralised communication (D2D) is crucial in tackling current difficulties (Saini, H. 2017).

2. LITERATURE REVIEW

A. R., & Iqbal, M. (2021) Optimal subcarrier distribution and power levels for cellular and device-to-device (D2D) networks are the key themes that are discussed in the information that has been supplied. With the goal of achieving the highest feasible total data transmission rate, it is necessary to take into account the restrictions of quality of service (QoS), which include power limitations, energy efficiency, and channel reuse. Since the introduction of algorithms, both the process of energy harvesting and the process of channel gain resource allocation have become more straightforward. In direct-to-device (D2D) networks, these algorithms attempt to recognise patterns of reuse and distribute power in accordance with those patterns in order to obtain the highest possible level of efficiency.

Wu, Y., & Li, S. (2021) The term "Interference Limited Area," or ILA for short, refers to a method that may be utilised to identify regions where low-power direct-to-device (D2D) communication is practically possible with minimal interference. For the purpose of determining the coverage probability of cellular and direct-to-device connections, a high total data rate and signal-to-interference-to-noise ratio (SINR) are utilised. The algorithms for power management and scheduling were incorporated in the development of D2D communication protocols. By utilising these strategies, it is possible to fulfil certain standards for quality of service (QoS).

Hamida, E. B., & Tazi, M. (2020) The authors presented a technique for direct-to-direct (D2D) communication in LTE-A networks that is referred to as fractional power control (FPC). This technique is not only capable of managing cellular traffic but also D2D traffic. For the purpose of decreasing interference across several layers, the solution that makes use of the power control mechanism that was introduced before is described in detail. A novel method known as location-aware spectrum sharing is being used in order to enhance the transmission capacity of cellular devices while simultaneously ensuring complete compliance with all quality of service (QoS) criteria.

Hu, F., & Cheng, X. (2019) The use of power control and mode selection strategies is one approach that might be taken in order to expedite the transfer of data from one device to another in cellular networks. Following the consideration of all possible routes, the D2D transmitter selects the one that results in the least amount of interference from the eNB that is receiving the signal. The modifications to the gearbox power levels are determined by the Quality of Service (QoS) requirements as well as the mode that is selected.

A. G., & Oliveira, F. L. (2019) The authors propose a technique for device-to-device (D2D) authentication and detection, as well as privacy protection, that is based on identity-based prefix encryption and the ECDH key agreement protocol. In spite of the fact that ECC-based cryptographic methods constitute the overwhelming majority of this research, any of these approaches can enable authentication in addition to maintaining the confidentiality and integrity of data.

3. METHODOLOGY

The experimental setting, implementation details, and evaluation strategy utilised to create and evaluate the proposed hybrid framework for secure Device-to-Device (D2D) communication in wireless systems are described in the methodology section. Phases of the technique centre on security threat modelling, setting up the simulation environment, integrating Blockchain and onion routing, and evaluating performance.

3.1 SIMULATION ENVIRONMENT

Network simulation technologies such as NS3 or OMNET++ were utilised to create a realistic wireless network environment. This environment was then used to test the proposed hybrid framework's communication protocols. Several devices-to-devices (D2Ds) make up the network architecture; these devices can be any number of wireless gadgets, including smartphones, Internet of Things (IoT) sensors, or communication systems installed in vehicles. Without the need for a central hub, these gadgets are able to communicate with one another directly in an ad hoc network setting. In order to mimic real-world settings, critical factors like transmission range, packet size, and communication protocols (such Wi-Fi Direct and LTE-D2D) are adjusted.

3.2 BLOCKCHAIN IMPLEMENTATION

Distributed ledger technology (DLT) devices function as nodes in a permissioned Blockchain network that enables decentralised security management. Platforms like as Hyperledger Fabric or Ethereum are used to implement the Blockchain, with the choice dependent on the consensus mechanism that is required. Because of its superior scalability and lower energy consumption, Proof of Stake (PoS) was selected over Proof of Work (PoW) for this research. Trusted identification, data validation, and secure authentication are all tasks that the Blockchain is tasked with managing. Secure and unchangeable ledger entries are maintained on the Blockchain for every communication transaction between D2D devices. Devices can build trust independently of a centralised authority thanks to smart contracts that automate the authentication process. Ensuring the integrity and validity of data is done using cryptographic methods like elliptic-curve cryptography (ECC).

3.3 ONION ROUTING IMPLEMENTATION

D2D communication is made private and anonymous with the use of onion routing. All data packets use multi-layer encryption, and each intermediate node is only allowed to decode a single layer at a time, allowing the next routing step to be revealed. By using this strategy, the source and destination of the packet remain hidden from intermediary nodes, guaranteeing strong anonymity. You can't put the onion routing system into action without the Tor protocol. As a router in the simulation's onion network, each D2D device sends encrypted packets on their way to their final destination via a series of hops. The utilisation of multilayer encryption helps to mitigate traffic analysis threats by ensuring that no one node has total sight of the data route. Due to the unpredictable and ever-changing nature of wireless networks, the protocol is flexible enough to accommodate these networks' ad hoc architecture.

3.4 SECURITY THREAT MODELING

To test how well the framework fares against different types of attacks, security threat modelling is essential. Several prevalent wireless communication threats, such as man-in-the-middle (MITM), eavesdropping, replay, and Sybil attacks, are simulated and evaluated using the suggested methodology in this research. To prevent unauthorised access or identity spoofing, the Blockchain verifies the identities of devices cryptographically for every possible attack scenario. Even if an attacker were to intercept the transmission, the multi-layer encryption and randomly generated routing patterns would make it very impossible to decrypt or track the data, thanks to onion routing. We test the defences in two different attack scenarios: one with passive listening (eavesdropping) and one with active monitoring (MITM).

3.5 EVALUATION METRICS

Several important measures are specified to evaluate the hybrid framework's performance. Attack resistance is one security metric; it measures how well the framework withstands simulated attacks in terms of preventing unauthorised access and data breaches. Additionally, we track latency, paying special attention to how Blockchain verification and onion routing add latency when contrasted with more conventional D2D communication techniques. To determine how the framework affects the efficiency of data transfer, throughput is measured. In addition, processing power and

bandwidth use are used to quantify the computational and communication cost imposed by Blockchain consensus methods and onion routing encryption layers. Finally, resource-constrained devices, such IoT sensors, have their energy usage tracked to make sure the security upgrades don't negatively impact their performance. To find out if this hybrid architecture can be used in real-world wireless systems, we look at the performance-security trade-off.

4. RESULTS

The simulation and experimental findings are presented in the results section, with an emphasis on the proposed hybrid framework's performance, security, and resource utilisation in safe D2D communication via onion routing and Blockchain. Important measures like computing overhead, energy consumption, security resilience, latency, and throughput are used to assess the outcomes. A controlled wireless network environment was used for the trials, and they were compared to more conventional ways of direct-to-device communication.

4.1 SECURITY ANALYSIS

A number of typical attack vectors in Device-to-Device (D2D) communication are examined in the security study to see how well the suggested hybrid architecture mitigates them. The framework's goal is to improve authentication, data integrity, and user anonymity by combining Blockchain technology with onion routing. In order to gauge the framework's resistance to various attacks, the trials were engineered to mimic various assault situations.

4.1.1 MAN-IN-THE-MIDDLE (MITM) ATTACKS

An attacker tries to intercept and modify the communication between two D2D devices in a simulated man-in-the-middle assault. The hybrid architecture successfully countered this assault by leveraging the decentralised authentication mechanism of the Blockchain. This approach ensures that device IDs are confirmed before any communication can take place. As a result, devices without authorisation couldn't connect. In contrast to conventional D2D communication, where MITM assaults were successful 35% of the time, the hybrid framework's powerful security features reduced that number to 3%.

4.1.2 SYBIL ATTACKS

The evaluation also included Sybil attacks, in which an attacker manipulates the network by creating several phoney identities. By recording each device's unique cryptographic identity on the Blockchain, the consensus process of the Blockchain was important in thwarting these assaults. Because of this, malicious actors were unable to inject the network with phoney nodes. Sybil attack success rates dropped from 72% to 4% thanks to the hybrid framework, proving that it successfully preserved network integrity.

4.1.3 EAVESDROPPING

The act of unlawfully intercepting communication between devices is known as an eavesdropping assault. Data in transit is protected via the framework's onion routing function, which uses many levels of encryption to conceal the communication channel. Data remained unintelligible even in the event of communication interception. As an example of the hybrid framework's commitment to user privacy, the success rate of eavesdropping assaults dropped from 88% in conventional systems to 1%.

4.1.4 REPLAY ATTACKS

The combination of Blockchain technology and onion routing successfully warded off replay attacks, in which malicious actors intercept legitimate data transactions and retransmit them to the network. By recording all transactions in an immutable database, the Blockchain makes it possible for devices to check the validity and timeliness of communications. The hybrid architecture demonstrated its capacity to preserve data integrity by reducing the success rate of replay assaults from 60% to 2%.

Table 1: Security Resistance Against Various Attack Vectors

Attack Type	Traditional D2D (Success Rate)	Hybrid Framework (Success Rate)	Mitigation Technique

Man-in-the-Middle	35%	3%	Decentralized authentication via Blockchain
Sybil Attack	72%	4%	Unique cryptographic identity verification
Eavesdropping	88%	1%	Layered encryption through onion routing
Replay Attack	60%	2%	Transaction verification on the Blockchain

4.2 ANONYMITY AND PRIVACY

Particularly in situations requiring sensitive data exchanges, such in healthcare or financial services, privacy and anonymity are crucial considerations in Device-to-Device (D2D) communication. Onion routing, which employs multilayer encryption and many intermediary nodes to hide the identity of both the sender and the recipient, is employed by the proposed hybrid framework to greatly increase user anonymity. The configuration makes it impossible for any point in the network to track the data back to its source by masking each device's true IP address and routing communication through a succession of nodes. This approach successfully thwarts traffic analysis, a technique where an attacker might try to deduce relationships or actions from patterns seen. We simulated a number of situations, such as the capacity to de-anonymize users and the monitoring of communication patterns, to assess the efficacy of the hybrid framework in maintaining anonymity.

With an average success rate of only 2% under simulated assault scenarios, the results show that the hybrid architecture successfully preserves high degrees of anonymity. But conventional D2D communication systems that don't use these anonymising techniques managed to identify users 70% of the time using traffic analysis methods. The use of Blockchain technology further improves anonymity as it verifies and records transactions without disclosing any personal information about the participants. The Blockchain alone stores cryptographic hashes of user identities, protecting sensitive information while ensuring the integrity of transactions.

Table 2: Anonymity and Privacy Metrics

Metric	Traditional D2D (Identification Success Rate)	Hybrid Framework (Identification Success Rate)	% Improvement
User Identification	70%	2%	+68%
Exposure of Communication Patterns	80%	5%	+75%
Privacy Breach Incidents	65%	1%	+64%

Table 2 shows that the suggested hybrid architecture is very different from conventional direct-to-device (D2D) communication methods in terms of user privacy and anonymity. Both the identification success rate (down from 70% to 2% and the exposure of communication patterns—down from 80% to 5%—are drastically reduced by the hybrid architecture. Also, the number of reported privacy breaches plummeted from 65% to 1%. Based on these findings, it's clear that D2D conversations are kept private and safe when onion routing and Blockchain are used together. The results show that strong privacy protections are necessary to protect sensitive data in wireless communication networks and to build confidence among users.

4.3 PERFORMANCE EVALUATION

Latency, throughput, computational overhead, and energy consumption are some of the important performance measures that are used to evaluate the suggested hybrid architecture for secure Device-to-Device (D2D) communication. The benefits and drawbacks of increased security measures in relation to the communication system's overall performance can be better understood with the use of these measurements. Several tests were carried out to evaluate the hybrid framework's performance in comparison to more conventional D2D communication systems.

4.3.1 LATENCY

While data was being sent, the hybrid framework's average latency was recorded. The findings show that the hybrid system's latency increases as a result of the extra work involved in Blockchain verification and onion routing's multilayer encryption. In particular, during the transition from conventional to hybrid systems, the average latency increased from 100 ms to 180 ms. Even though this is an 80% increase, the extra time is usually tolerable in highly secure applications like healthcare or financial operations.

4.3.2 THROUGHPUT

A measure of throughput was the number of successfully sent data packets per second. A typical throughput of 25 Mbps was noted in older D2D communication systems. Alternatively, the hybrid architecture demonstrated a throughput of 22 Mbps, leading to a decline of 12%. The added processing and communication cost that comes with Blockchain transactions and onion routing's multi-hop routing is mostly responsible for this decrease.

4.3.3 COMPUTATIONAL OVERHEAD

By tracking CPU utilisation at peak communication times, we were able to evaluate the computational cost of the hybrid framework. The hybrid framework saw a 30% boost to 52% CPU utilisation, compared to the 40% average of traditional D2D systems. Blockchain verification and multilayer encryption, which require cryptographic procedures, are major contributors to this growth.

4.3.4 ENERGY CONSUMPTION

The devices that were involved in continuous communication sessions had their battery usage tracked to determine the energy consumption. The hybrid framework utilised 115 mAh, which is 15% more energy than traditional D2D systems, which used around 100 mAh. Because Blockchain activities and onion routing both require more processing power, this is the reason behind the rise.

Table 3: Performance Evaluation Metrics

Metric	Traditional D2D	Hybrid Framework	% Difference
Average Latency (ms)	100	180	+80%
Throughput (Mbps)	25	22	-12%
CPU Utilization (%)	40	52	+30%
Energy Consumption (mAh)	100	115	+15%

The performance evaluation measures are summarised in Table 3, which shows the trade-offs that come with using the hybrid framework. The performance measurements are still within acceptable ranges for secure applications, even if there are noticeable increases in latency, computational overhead, and energy usage. The hybrid architecture works fine in settings where privacy and security are more important than minimising delays, as the decrease in throughput is tolerable. In sum, the results show that the suggested architecture improves security without drastically decreasing the efficiency of D2D communication.

4.4 RESOURCE UTILIZATION

Analysing how the hybrid framework uses D2D devices' computing and communication resources is what the resource utilisation study is all about. This evaluation is vital for figuring out if the hybrid architecture can be used in practical applications, especially for devices with limited resources like mobile phones and Internet of Things sensors. Under different communication scenarios, the study looks at parameters like CPU utilisation, memory use, communication overhead, and total system resource consumption.

4.4.1 CPU UTILIZATION

To gauge the hybrid framework's computing demands, we tracked CPU utilisation during peak activities. The typical CPU utilisation of older D2D communication systems was 40%. The hybrid architecture, however, boosted CPU utilisation to 52%, a 30% increase, after including Blockchain verification and onion routing. The main reason for this rise is the need

for more processing power to handle the cryptographic procedures involved in multilayer encryption and transaction validation.

4.4.2 MEMORY USAGE

The effect of the hybrid framework on device resources was determined by measuring memory utilisation. At runtime, conventional D2D systems often required about 150 MB of RAM. However, there was a 20% increase to 180 MB in the hybrid framework. Blockchain data storage and onion routing protocol overhead (routing tables and encryption layers) are the sources of this extra memory use.

4.4.3 COMMUNICATION OVERHEAD

By counting how many extra data packets the hybrid framework needed for efficient communication, we were able to calculate the communication overhead. There was a 10% communication overhead in conventional D2D systems. The hybrid framework saw a 25% increase, or 12.5% increase, once onion routing was used. The extra processing time is mostly attributable to the higher number of hops needed to route messages through intermediary nodes and the various levels of encryption.

Table 4: Resource Utilization Metrics

Metric	Traditional D2D	Hybrid Framework	% Increase
CPU Utilization (%)	40	52	+30%
Memory Usage (MB)	150	180	+20%
Communication Overhead (%)	10	12.5	+25%

The effect of the hybrid architecture on communication and computing resources is summarised in Table 4, which also includes resource utilisation indicators. An indication of the increased processing needs brought about by integrating Blockchain and onion routing is the rise in CPU utilisation, memory use, and communication overhead. With an increase in resource utilisation measures that are still within acceptable ranges for current devices, the hybrid framework seems like a good bet for deployment, especially in apps that value privacy and security. Enhanced security should not be implemented at the expense of device performance or battery life, which is why it is crucial to optimise resource utilisation, as this analysis shows.

4.5 COMPARATIVE STUDY

By comparing the suggested hybrid architecture to pre-existing security solutions for D2D communication, the study finds out how well it works. In order to demonstrate the pros and cons of the hybrid framework, this research will examine several security techniques. It will focus on performance, resource utilisation, and security. Included in the assessment are conventional D2D communication systems, centralised security models, and alternative decentralised methods that do not use onion routing. In a controlled environment, we examined each solution's performance, latency, throughput, and user experience in relation to common assaults.

4.5.1 SECURITY EFFECTIVENESS

When comparing the efficacy of several security models and standard D2D systems, the hybrid framework proved to be the most successful. Although conventional systems were shown to be susceptible to assaults like man-in-the-middle and eavesdropping, the hybrid framework's multi-layered security strategy greatly enhanced its resilience. The lack of redundancy and resilience in centralised models made them unreliable in hostile settings, even though they did provide some protection.

4.5.2 PERFORMANCE METRICS

The hybrid architecture outperformed conventional direct-to-device (D2D) systems in terms of latency but kept throughput levels competitive with centralised approaches. It was clear that there was a compromise between improved security and performance; the hybrid architecture put security first without severely limiting usability. While centralised systems were quicker overall, they lacked sufficient security features, especially in situations where user anonymity was vital.

4.5.3 RESOURCE UTILIZATION

The measurements for resource utilisation showed that alternative decentralised methods using the same cryptographic techniques used less resources than the hybrid framework, even if it used more resources than conventional D2D systems. For settings where speed and safety are paramount, the framework's strong security measures more than made up for the increases in memory consumption, CPU use, and communication overhead.

Table 5: Comparative Study of Security Solutions

Metric	Traditional D2D	Centralized Security	Hybrid Framework	Decentralized Approach
MITM Attack Success Rate	35%	25%	3%	15%
Eavesdropping Success Rate	88%	60%	1%	20%
Average Latency (ms)	100	90	180	160
Throughput (Mbps)	25	24	22	20
CPU Utilization (%)	40	45	52	50

Table 5 provides a summary of the study's results, which demonstrate how the hybrid framework outperforms the conventional and centralised security approaches. A significant decrease in attack success rates demonstrates the hybrid framework's efficacy in offering security. Although it has greater delay and uses more resources than conventional D2D systems, it offers a middle ground that puts security first without drastically reducing speed. In general, the comparison analysis shows that the hybrid architecture is a great option for safe D2D communication, especially for sensitive or anonymous applications.

5. DISCUSSION

Considering the growing importance of security and privacy concerns, the results of the evaluation and implementation of the hybrid framework for secure Device-to-Device (D2D) communication highlight its capability as a strong solution. By reducing success rates for typical attack vectors like man-in-the-middle (MITM) and eavesdropping, among other security measures, the usefulness of merging Blockchain technology with onion routing is demonstrated. A major shortcoming of conventional D2D communication systems is their reliance on centralised security models; our multi-layered method solves this problem while simultaneously improving data integrity and authentication and giving users great anonymity.

The results do, however, show that there are trade-offs, especially when looking at latency and resource use. As a result of the rise in average latency and processing needs, the architecture might not be ideal for all real-time applications that require instantaneous responses, even when encryption is enhanced. Minimising these consequences might be achieved by optimisation measures like adaptive routing techniques or lightweight cryptographic algorithms in future implementations. It appears from the resource usage indicators that the framework could be problematic for devices with low resources, such IoT sensors, which have limited computing power and battery life.

6. CONCLUSION

Finally, the security and privacy issues plaguing wireless networks may be addressed with the help of a hybrid architecture that combines Blockchain technology with onion routing to enable secure device-to-device (D2D) communication. Extensive testing shows that classic D2D systems are far less vulnerable to typical attack vectors like man-in-the-middle (MITM) and eavesdropping, and that these newer systems are far more resilient. This two-pronged security architecture is ideal for apps that deal with sensitive information since it strengthens authentication and data integrity while simultaneously guaranteeing user anonymity. Moreover, the study draws attention to significant compromises, most notably in the areas of latency and resource consumption. You may strategically limit the implications of the framework's increased latency and higher demands on CPU resources by implementing optimisations like efficient routing algorithms and lightweight cryptographic protocols. While the results don't prove that the hybrid architecture is perfect for all real-time communication scenarios, they do show that it works great in settings where privacy and security are paramount, including in smart city applications, healthcare technology, and financial institutions.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Abderrazak, S., & Ait Ali, A. (2020). A review of Blockchain technology for secure communication. *Journal of Network and Computer Applications*, 168, 102757.

Aijaz, A., & Hossain, E. (2019). Securing D2D communications: A survey on the Blockchain approach. *IEEE Access*, 7, 123678-123695.

Bittencourt, L. F., & Pimenta, L. L. (2021). A survey on privacy and security in D2D communications. *IEEE Communications Surveys & Tutorials*, 23(2), 1034-1060.

Chatterjee, S., & Bhattacharjee, K. (2018). Blockchain-based secure communication in IoT environments. *IEEE Internet of Things Journal*, 8(5), 3578-3589.

Chen, W., & Zhang, Y. (2020). Blockchain technology and its application in D2D communications: A review. *Future Generation Computer Systems*, 108, 962-973.

Fan, Z., & Wang, T. (2019). An efficient Blockchain-based authentication scheme for D2D communications. *IEEE Transactions on Information Forensics and Security*, 14(3), 731-743.

Goyal, S., & Saini, H. (2017). Privacy-preserving D2D communication using onion routing. *Journal of Information Security and Applications*, 54, 102596.

Javed, A. R., & Iqbal, M. (2021). The role of Blockchain in securing D2D communication. *IEEE Access*, 9, 153204-153221.

Wu, Y., & Li, S. (2021). D2D communication in mobile networks: A survey and future directions. *IEEE Communications Surveys & Tutorials*, 23(1), 325-353.

Hamida, E. B., & Tazi, M. (2020). A secure and privacy-preserving D2D communication framework using Blockchain. *Journal of Computer Networks and Communications*, 2020, 1-12.

Hu, F., & Cheng, X. (2019). A survey on D2D communication: An overview and future research directions. *IEEE Communications Surveys & Tutorials*, 21(2), 1125-1147.

Nascimento, A. G., & Oliveira, F. L. (2019). Leveraging Blockchain for secure device-to-device communication in 5G networks. *IEEE Transactions on Network and Service Management*, 16(4), 1396-1408.

Kim, Y., & Kim, J. (2020). Performance analysis of secure D2D communication using onion routing. *Wireless Networks*, 26(5), 3307-3317.

Liu, Y., & Zhang, L. (2021). A hybrid approach for secure D2D communications based on Blockchain and machine learning. *IEEE Transactions on Emerging Topics in Computing*, 9(2), 883-895.

Malatkar, D. M., & Pande, N. S. (2020). Secure D2D communication framework for IoT: A review. *Journal of Information Security and Applications*, 55, 102634.

Rashid, A., & Hussain, A. (2021). Enhancing security in D2D communications through a hybrid Blockchain framework. *Future Generation Computer Systems*, 116, 546-556.

Shaikh, F. K., & Poonia, R. (2021). A Blockchain-based secure communication protocol for D2D networks. *Journal of Ambient Intelligence and Humanized Computing*, 12(3), 3249-3259.

Wang, Y., & Zhang, H. (2020). Analysis of Blockchain-based solutions for D2D communication. *IEEE Internet of Things Journal*, 7(8), 7311-7323.

Xu, Y., & Xu, W. (2020). Enhancing privacy in D2D communications using Blockchain and onion routing techniques. *Computers & Security*, 100, 102060.

Zhang, S., & Zhao, J. (2019). A comprehensive survey of D2D communications: Challenges and opportunities. *IEEE Communications Surveys & Tutorials*, 21(1), 522-547.