Trust Requirements and Mechanisms in Peer-to-Peer Energy Markets

Boitumelo Leotlela[2][0009-0008-5863-9356] Lehlogonolo Ledwaba[2][0000-0002-7292-2835] Marijke Coetzee[1][0000-0002-9157-3079]

[1] North-West University, Potchefstroom 2531, South Africa
[2]Council of Scientific and Industrial Research, Meiring Naude Rd, Pretoria, 0184, South Africa
{tleotlela, lledwaba4}@csir.co.za, marijke.coetzee@nwu.ac.za

Abstract. Peer-to-peer (P2P) energy markets are emerging as a promising solution to address the challenges faced by traditional energy systems. However, the decentralised nature of these markets necessitates robust trust mechanisms to ensure secure and reliable energy transactions. This paper presents a comprehensive review of trust requirements and trust-building mechanisms in P2P energy markets. It explores the role of blockchain technology, zero-trust architecture, and reputation systems in establishing trust among market participants. It identifies several trust requirements, including security, privacy, transparency, fairness, and reputation. The study further highlights the limitations of existing works and proposes future research directions to enhance trust and security in P2P energy markets. By addressing these limitations, the full potential of P2P energy trading can be unlocked, contributing to a more sustainable and resilient energy future.

Keywords: Blockchain**,** IoT, Peer-to-peer energy market, Reputation, Security, Trust, Zero-trust architecture.

1 Introduction

South Africa's energy sector faces major challenges, including over-reliance on coal, persistent load shedding, and corruption that has eroded public trust in government and state enterprises, deterring investment and delaying clean energy adoption [1]. In response, interest is growing in decentralised energy systems like peer-to-peer (P2P) energy markets, which reduce dependence on centralised generation, boost efficiency, and empower consumers to generate and trade energy directly [2].

The success of P2P energy markets hinges on building trust in a decentralised environment without central oversight, ensuring honest transactions, system security, and sustainable energy generation [2]. Participants face challenges in decision-making, such as choosing when to trade, assessing partner reliability, and verifying energy quality, making trust mechanisms essential [4, 6].

This study examines the role of blockchain, zero-trust architecture, and reputation systems in establishing trust in P2P energy markets. It reviews current research,

highlights gaps, and suggests future directions for enhancing trust and security in these markets by addressing these key questions:

- What are the trust requirements of P2P energy markets?
- What is the state of the art for trust mechanisms in P2P energy markets?
- What trust requirements of P2P energy markets are not sufficiently addressed?

The study is structured as follows: Section 2 provides background on P2P energy markets; Section 3 explores trust requirements; Section 4 reviews existing work and gaps; Section 5 concludes the study.

2 Background

The growing urgency to reduce the global carbon footprint has sparked interest in renewable energy resources and fostered the growth of P2P energy markets [3,4]. These markets empower passive consumers in traditional power systems to become active participants, known as 'prosumers', who generate, consume, and trade energy withing their communities. Unlike traditional centralised power systems, where large scale producers and industry consumers dominate, the P2P energy market enables small-scale consumers and producers to actively participate in the energy market [2].

P2P energy markets disrupt traditional power distribution models by enabling direct energy trading between individuals and communities. Figure 1 depicts a transactive energy market environment where peers, consumers, or prosumers, directly trade energy with one another. Prosumers can buy and sell energy to each other, as shown by the green bidirectional line between Prosumer 1 and Prosumer 2.

Consumers purchase energy from prosumers, as depicted by the red arrow between Prosumer 2 and Consumer B. Each transaction represents a mutual agreement between participants to exchange energy for monetary value, called a bilateral contract [7]. Red contracts in Figure 1 indicate a trade agreement between a prosumer and a consumer, while the agreement between two prosumers is illustrated by a green contract. An intermediary utility can supply energy to the local market in case of power disruptions or receive surplus energy when supply does not meet demand [15].

The integration of IoT devices enables P2P markets. Several IoT devices are depicted in Figure 1 alongside an IoT smart meter. IoT-enabled smart meters collect and process data from household sensors, forming the basis for trading decisions, demand forecasting in the grid and aiding in accurate billing information [8]. They are means by which prosumers and consumers can connect directly with one another and trade within the P2P energy market [2,8]. Cryptographic techniques and blockchain technologies are among several ways these devices are secured [17].

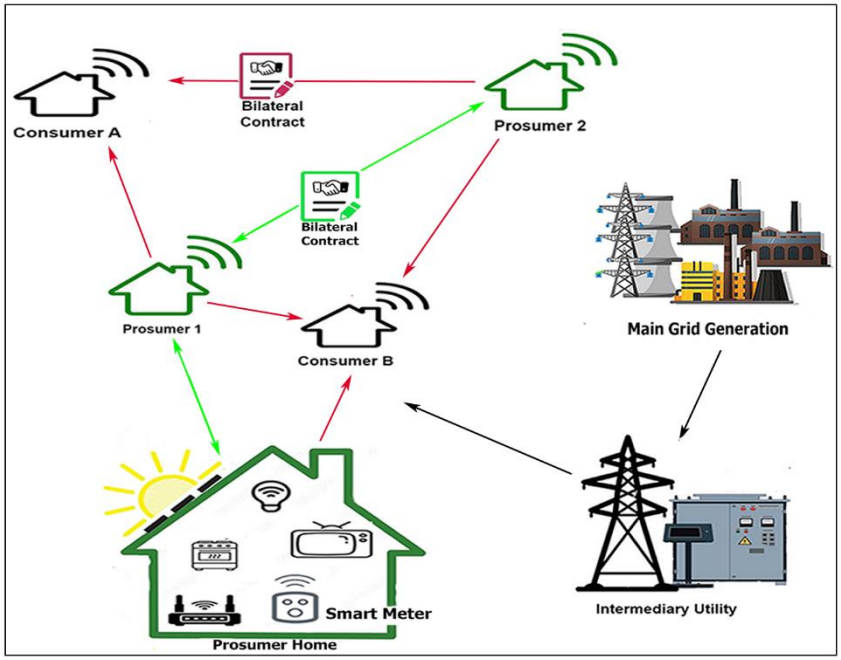

Fig. 1. A P2P energy market.

3 Trust requirements for P2P energy markets

Computational trust models aim to replicate social trust in digital environments, capturing key properties like asymmetry, subjectivity, partial transitivity, and context sensitivity [9, 10]. Trust is asymmetrical when it is not equally reciprocated, subjective when shaped by personal experiences, partially transitive when trust in one peer does not extend to others, and context sensitive as it varies across situations. Trust is also dynamic, evolving with interactions and changing expectations [9, 10]. A hybrid approach that combines hard trust mechanisms, like security protocols and encryption that offer objective certainty, with soft trust mechanisms, like reputation and user experiences that capture the more dynamic and subjective aspects of trust, could secure the market environment while accommodating the dynamic nature of trust [11]. Trust is vital in P2P energy markets where participants lack prior relationships. Participants need confidence that the platform will fairly manage energy prices and transactions, securely manage payments and accurately record energy production and consumption. They must trust that peers will honour agreements and that the energy traded meets quality standards. In P2P energy trading, a successful transaction between a consumer and a prosumer relies on trust, i.e., both peers acting honestly and reliably. The prosumer must deliver the agreed-upon quality and amount of energy timeously, while the consumer must follow through with the payment [4]. Trust in these transactions depends on the reliability of the system, the honesty of the participants, and their

reputation from previous successful transactions. High levels of trust and positive reputation are crucial for facilitating participation and peer selection in the energy market.

Based on a review of the literature, the following trust requirements are identified [3, 4, 7, 8]:

- **Security:** Data must be protected, and financial transactions secured.
- **Privacy:** Participants' personal and transactional data need to be confidential to ensure compliance with data protection regulations like the POPIA Act.
- **Transparency:** Real-time data and pricing structures are transparent.
- **Fairness:** Equal market access and regulations to prevent unfair practices are crucial.
- **Consensus:** Before a transaction is recorded on the blockchain, market peers should agree that it is legitimate and meets market rules.
- **Accountability:** Peers conduct transactions in a reliable and trustworthy manner by meeting their contractual obligations.
- **Reputation:** Participant ratings and reviews to help maintain the reliability of peers in the market.

In the following section, current work addressing building trust in P2P energy markets is reviewed.

4 A review of trust for P2P energy markets

Numerous studies have leveraged hard and/or soft trust to enable a trusted environment in energy markets. While a variety of solutions exist, this study narrows the focus to studies considering the use of blockchain, zero-trust architectures, and reputation systems. These technologies were selected due to their potential to address the unique challenge of trust, reliability, and security in P2P energy trading. A comprehensive search was conducted using a combination and a variation of the following search string:

(‘Peer-to-peer energy market’ ***OR*** ‘Energy Market’ ***OR*** 'decentralised marketplace' ***OR*** 'energy trading') ***AND*** (blockchain) ***AND*** (‘trust’ OR 'decentralised trust' ***OR*** ‘reputation’)

Ten peer-reviewed studies were selected that were published within the last three years in reputable repositories like Science Direct, IEEE Xplore and MDPI, and primarily focused on decentralised trust and security in P2P energy markets. Seven of these papers discuss the trust requirements in P2P energy markets, while three of them look at the trust requirements in IoT environments where zero-trust architecture is leveraged, since there a few works implementing zero-trust architecture in P2P energy markets. The review process was guided by the Kitchenham et al. [12] protocol for conducting systematic literature reviews. Selected studies were analysed to identify common trust requirements, explore the implementation of trust-building mechanisms, and assess the effectiveness of these mechanisms. The following sections discuss blockchain, zero-trust architectures, and reputation as trust mechanisms.

4.1 Blockchain

Blockchain technology offers a robust foundation for trust in P2P energy trading, where participants often lack prior relationships. Blockchain boasts transparent and immutable ledgers distributed across the network, thus ensuring secure storage of information in the P2P energy markets. These also encourage accountability and ensure non-repudiation [7]. Additionally, blockchains use consensus algorithms to ensure that market operations follow market rules, ensuring that all peers agree on a single source of truth. This is especially crucial in the P2P energy market with no central authority as it helps maintain consistency and the system's reliability [7]. Smart contracts facilitate the automatic and secure execution of energy transactions [7, 15].

Several studies explore blockchain-based P2P energy markets [7, 15]. Tkachuk et al. aimed to address issues related to following regulations, security, privacy and trust concerns by leveraging blockchain technology [7]. The authors incorporated a regulator for oversight and used private data collections to protect privacy. Tkachuk et al. [7] aim to address privacy and trust concerns by leveraging the private data collections within the Hyperledger blockchain, which allows for privacy preservation while maintaining the integrity and auditability of transactions.

While the characteristics of blockchain addressed security and trust Kumari et al. [15] addressed single points of failure, scalability, trust and security issues. They combined blockchain with the interplanetary file system (IPFS), a decentralised file system for efficient and secure data storage and mitigating single points of failure. The authors proposed a P2P energy trading scheme that is transparent and decentralised in addition to a dynamic pricing mechanism, which both aim to manage energy generation in smart grids and increase profit for peers in the market, respectively. Similarly to the work done by Tkachuk, security and trust are addressed by blockchain, although this is not explicitly addressed.

4.2 Zero-trust architectures

Traditional security models, relying on network perimeters, are inadequate for decentralised P2P energy markets. The dynamic and open nature of these markets makes it challenging to maintain secure boundaries [16]. Zero-trust architecture offers a more robust approach. By continuously verifying users, devices, and connections regardless of location, risks posed by cyberattacks and fraudulent activities can be mitigated.

Based on the pre-defined search criteria, few works were found implementing zero-trust architectures in P2P energy markets to enhance security and trust. Thus, a significant gap exists at the intersection of P2P energy markets and zero-trust architecture.

In the field of P2P energy markets, Rasool et al. [17] was the only work found that attempted to implement zero-trust architecture in a proposed framework that distributes trust in green energy certificate issuance from central registries to prosumers using a hybrid distributed ledger and blockchain solution along with Self-Sovereign Identity (SSI). The use of blockchain ensures the immutability and verifiability of certificates, preventing fraud and promoting trust in the green energy market. The SSI allows prosumers to control their digital identities and verify the authenticity of green energy

certificates. By distributing trust from centralised registries to individual prosumers, the framework enhances security and transparency in the certification process, thus propelling the work towards a zero-trust architecture.

Various studies have demonstrated the effectiveness of zero-trust architecture in safeguarding decentralised IoT environments and power grids. For instance, the framework by Ameer et al. [16] emphasised continuous authentication and authorisation, treating every IoT device and environment as potentially compromised. Therefore, trust was decoupled from network location.

Similarly, Awan et al. [18] integrate zero-trust architecture with Attribute-Based Access Control and blockchain technology to ensure that only authorised IoT devices can access the network while dynamically adjusting access policies based on real-time environmental data. This framework uses zones with policy enforcement points and decision points to regulate device access. In contrast to the other studies leveraging zero-trust architectures in IoT networks, Pang et al. [19] proposed a zero-trust access control mechanism based on service reputation assessment for power grids, using real-time and historical reputation values to assess the trustworthiness of services, ensuring that only trusted services are granted access to the network.

4.3 Reputation

Reputation plays a significant role in P2P energy trading, measuring trustworthiness based on past interactions and community feedback [10]. Reputation systems aggregate this feedback to provide transparent assessments, reducing uncertainty and aiding participants in deciding whom to trust in transactions [9, 10]. Decentralised reputation systems are particularly effective in these markets, as they distribute the responsibility of evaluating and storing scores across the network, eliminating the need for a central authority. These systems encourage honest behaviour by incentivising good behaviour, thus deterring malicious and fraudulent behaviour, while promoting trust, security, and broader market adoption [5, 9].

To address security vulnerabilities and malicious behaviour about peers not fulfilling transactions, Zhang et al. [4] proposed a reputation-aware secure transactive energy market (STEM) based on the Packetized Energy Management and Trading Co-Simulation (PEMT-CoSim) platform. Using smart contracts and blockchain to track historical behaviour, STEM calculates reputation scores based on objective behaviour information, influencing participant behaviour in energy auctions and transactions. The authors propose incentives in which peers with a good reputation are given higher preference during bidding. A multi-round table algorithm was proposed to mitigate malicious behaviour. This penalised malicious actors by increasing the ‘benefits’ for peers with a good reputation in the presence of malicious peers.

Wang et al. [6] follow a similar approach for incentives in their distributed reputation system, RBT, that leverages blockchain’s immutability and transparency to ensure the reliability of scores. The authors employed a reputation-based k-double auction mechanism for trading in the P2P energy market, where higher reputation scores lead to more favourable trade prices to incentivise good behaviour. The distributed

reputation system leveraged smart contracts to manage reputation automatically while also implementing the auction matchmaking scheme.

In [13], Olariu et al. focus on reducing uncertainty in buyer feedback through a trust and reputation service. Smart contracts provide automatic feedback, replacing unreliable buyer input with objective assessments stored on immutable ledgers. The trust measure is based on Laplace's Law of Succession, representing the probability that a seller will fulfil their obligations in the next transaction.

Decentralised trust can also be enforced through public key infrastructure. In [14] Bolgouras et al. propose a 'distributed security platform' they named 'RETINA', a distributed and secure trust management framework using public key infrastructure and a web of trust to address security challenges. Blockchain stores certificates and trust relationships in immutable and transparent ledgers, enabling decentralised trust and secure communication. Certificates are used to identify smart meters and are used to verify trust between the devices.

In the next section, these studies are analysed based on the trust requirements they addressed, and the trust mechanisms used to address them.

4.4 Analysis of trust requirements and trust mechanisms

Next, an analysis is presented based on the previously discussed trust-enabling technologies and the trust requirements they address. In Table 1, the first two columns indicate the use of either blockchain or zero-trust architectures in P2P energy markets and IoT environments. The rest of the columns indicate the trust requirements that each solution has addressed. Each column is now discussed in more detail.

Zero-trust architectures are not commonly used in P2P energy markets, as indicated in Table 1. Rasool et al. [17] is the only study identified by this research that employs this technology and implements just a few features in the P2P energy market environment. Self-sovereign identities, blockchain, and the constant and dynamic verification of trust through green energy certificates support decentralised trust and security. The last three papers in Table 1 are related works implementing zero-trust architecture in IoT environments. Features such as continuous authentication and monitoring, network segmentation, decoupling trust from a network location and least privilege [16, 17, 18, 19] are implemented. Since these are applied in decentralised IoT networks, they may be very useful to the P2P energy market. The work by Pang et al. [19] shows the potential for zero-trust architecture principles to be integrated with decentralised reputation models to ensure secure decentralised reputation models, indicating a research gap for P2P energy markets.

Blockchain technology is comprehensively used in P2P energy markets because of its secure, decentralised nature. It distributes responsibilities across the network, reducing reliance on central authorities and minimising the risk of single points of failure. However, some studies [7] introduce centralisation by adding a regulatory actor to oversee market operations.

Security is ensured by cryptographic hashes of blockchain technology and immutable ledgers [4, 6, 7, 13]. In other studies, it is supported by primary key infrastructure, SSI, access control policies and zero-trust architecture [14, 17, 18, 19].

Table 1. Evaluation of trust requirement in P2P energy markets

	Trust enabling Technologies		Trust requirements in literature						
Paper	Zero-trust architecture	Blockchain	Security	Privacy	Transparency	Consensus	Fairness	Accountability	Reputation
Peer-to-Peer energy market environments									
[7]		X	X	X	X	X		X	
[15]		X	X		X	X	X	X	
[4]		X	X		X	X	X	X	X
[6]		X	X		X	X	X	X	X
[13]		X	X		X	X		X	X
[14]		X	X	X	X	X	X	X	
[17]	X	X	X	X	X	X		X	
IoT environments									
[16]	X		X						
[18]	X	X	X		X	X		X	
[19]	X		X						X

Privacy in P2P energy markets is addressed explicitly by a few studies using Hyperledger Fabric, a permissioned blockchain platform limiting network access to authorised peers. The study [7] explicitly uses these features, while [14] implies privacy through a permissioned ledger without explicit details. In contrast to these studies, Rasool et al. [17] address privacy by allowing users to share selected data using methodologies like zero-knowledge proofs or selective disclosure of information.

Transparency is addressed by the presence of blockchain technology [4, 6, 7, 13, 14, 15, 17, 18], with immutable ledgers available to all peers on the network. These transparent ledgers store transaction and reputation information securely. This allows for verifying transaction information to ensure contractual obligations are met [4]. Additionally, this feature ensures that reputation information is available to all peers in the market and is less susceptible to manipulation by malicious users [4, 13].

Consensus is similarly addressed by blockchain technology to ensure that transactions are legitimate and all peers in the market agree with them before they are recorded on the chain [7,6,14,15]. This ensures that peers abide by market rules. Smart contracts contribute to consensus, as some studies explicitly mention that market rules are in smart contracts. These contracts facilitate and automatically execute transactions in the P2P energy market [4,13]. Consensus in the blockchain mitigates illegitimate transactions and collusion attacks [15].

Fairness, particularly in pricing, is addressed by only a few studies. Fair pricing ensures that all participants can access the same market prices or that pricing is based on objective and transparent criteria. For example, Kumari et al. [15] propose a dynamic pricing model based on supply and demand, ensuring non-discriminatory prices. Zhang et al. [4] and Wang et al. [6] link prices to a participant's reputation, where higher reputations yield better prices or bidding priority, promoting fairness and deterring malicious behaviour.

Accountability is achieved whenever blockchain technology is leveraged. Its transparent and immutable ledgers allow smart contracts to check that the energy traded during a transaction is reflected on the smart meters of the peers involved. This ensures that peers fulfil their contractual obligations. Peers can be held accountable should they not fulfil their contractual obligations.

Reputation systems are effective in fostering trust in P2P energy markets. However, they are vulnerable to manipulation, collusion, and trust saturation, requiring secure implementation. Blockchain technology ensures reputation information is transparent and immutable while reducing information asymmetry. Smart contracts are used in this environment to implement reputation models [13]. Zhang et al. [4] and Olariu et al. [13] collect objective feedback from smart meters and smart contracts to verify transactions on whether peers have successfully fulfilled their obligations. Reputation systems incentivise honest behaviour and penalise malicious actions, influencing pricing fairness [4, 6].

From Table 1, it is evident that there is limited focus on implementing zero-trust architecture within P2P energy markets, despite its potential to enhance security and trust. Moreover, reputation systems are rarely combined with zero-trust architectures in these markets, though their integration could improve peers' decision-making and strengthen the reputation system's security. Furthermore, privacy concerns are not fully addressed in these studies, highlighting another gap where zero-trust approaches could provide an additional layer of security to ensure security of data.

5 Conclusion

This study investigates trust requirements in decentralised P2P energy trading, emphasising the potential of blockchain technology, zero-trust architecture, and reputation systems for fostering trust. A short review identified several gaps and limitations in the current research, including a lack of consensus on implementing some trust requirements and the scope in which they are applied. The study also highlights the need to explore further dynamic trust using zero-trust architecture in P2P energy markets.

Future research focuses on developing a comprehensive trust and reputation framework that addresses these gaps by leveraging zero-trust architecture principles and trust-based reputation systems. This framework should prioritise the trust needs of decentralised P2P energy markets to build confidence among participants and create a more trustworthy trading environment.

By tackling these challenges, the study suggests that the full potential of P2P energy trading, particularly in the South African context, can be realised. Participants can be more comfortable engaging in the market, contributing to a more sustainable and resilient energy future.

Acknowledgement. This work was supported in part by the Council of Scientific and Industrial Research, South Africa and the Department of Science and Innovation, South Africa within the ambit of the Foundational Digital Capabilities Research (FDCR) programme [Project KR5ETRT] and the Unit for Data Science at North-West University, South Africa.

References

1. CORRUPTION WATCH. 2024. The influence of corruption on the transition to renewable energy in SA. https://www.corruptionwatch.org.za/the-influence-of-corruption-on-thetransition-to-renewable-energy-in-sa/. Accessed: 29 July 2024

2. Baig, M.J.A., Iqbal, M.T., Jamil, M. & Khan, J.: P2P Energy Trading in a Microgrid Using Internet of Things and Blockchain. Electron.J, 25:39-49 (2021).
3. Moniruzzaman, M., Yassine, A. & Benlamri, R. Blockchain and cooperative game theory for P2P energy trading in smart grids. International Journal of Electrical Power & Energy Systems, 151:109111. (2023).
4. Zhang, P., Wu, P., Liu, Y., Chen, Y., Li, Y., Yan, J. & Ghafouri, M.: Toward a BlockchainBased, Reputation-Aware Secure Transactive Energy Market. Blockchains, 2(1):61-78. (2024).
5. Nwebonyi, F.N., Martins, R. & Correia, M.E.: Reputation based approach for improved fairness and robustness in protocols. P2P Networking and Applications 12, 951-968. (2019)
6. Wang, T., Guo, J., Ai, S. & Cao, J.: RBT: A distributed reputation system for blockchain-based P2P energy trading with fairness consideration. Applied Energy, 295:117056 (2021).
7. Tkachuk, R., Ilie, D., Robert, R., Kebande, V. & Tutschku, K.: Towards efficient privacy and trust in decentralised blockchain-based P2P renewable energy marketplace. Sustainable Energy, Grids and Networks 35, 101146 (2023).
8. Condon, F., Franco, P., Martínez, J.M., Eltamaly, A.M., Kim, Y. & AHMED, M.A.: EnergyAuction: IoT-Blockchain Architecture for Local P2P Energy Trading in a Microgrid. Sustainability 15, 1713203 (2023).
9. Ahmed, A.I.A., AB Hamid, S.H., Gani, A., Khan, S. & Khan, K.: Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open Research Challenges. Journal of Network and Computer Applications 145, 102409 (2019).
10. Braga, D., Niemann, M., Hellingrath, B. & Neto, F.: Survey on computational trust and reputation models. ACM Computing Surveys (CSUR) 51, 51-40 (2018).
11. Varadharajan, V.: A Note on Trust-Enhanced Security. IEEE Security & Privacy 7, 357-59 (2009).
12. Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J. & Linkman, S.: Systematic literature reviews in software engineering – A systematic literature review. Information and Software Technology 51, 17-15 (2009).
13. Olariu, S., Mukkamala, R. & Aljohani, M.: Towards Trust and Reputation as a Service in a Blockchain-based Decentralised Marketplace. arXiv preprint (2024).
14. Bolgouras, V., Ioannidis, T., Politis, I., Zarras, A. & Xenakis, C.: RETINA: Distributed and secure trust management for smart grid applications and energy trading. Sustainable Energy, Grids and Networks 38, 101274 (2024).
15. Kumari, A., Chintukumar Sukharamwala, U., Tanwar, S., Raboaca, M.S., Alqahtani, F., Tolba, A., Sharma, R., Aschilean, I. & Mihaltan, T.C.: Blockchain-Based P2P Transactive Energy Management Scheme for Smart Grid System. Sensors 22, (2022).
16. Ameer, S., Gupta, M., Bhatt, S. & Sandhu, R.: Bluesky: Towards convergence of zero trust principles and score-based authorisation for iot enabled smart systems In Proceedings of the 27th ACM on symposium on access control models and technologies (2022).
17. Rasool, S., Saleem, A., Ikram Ul Haq, M. & Jacobsen, R. H.: Towards Zero Trust Security for Prosumer-Driven Verifiable Green Energy Certificates In 2024 7th International Conference on Energy Conservation and Efficiency (ICECE) (2024).
18. Awan, S.M., Azad, M.A., Arshad, J., Waheed, U. & Sharif, T. A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT. Information, 14(2) (2023).
19. Pang, L., Jin, Q., Qi, L., Yong, Y., Jiajia, H. & Qinyuan, L. 2023. Service reputation assessment for power grid zero-trust security. In.: SPIE. pp. 653-658. (2023).