International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

The Evaluation of Security and Privacy Components in the Context of Peer-To-Peer Power Trading Methodologies using Network Intelligence

[1]Dr. Cuddapah Anitha, [2]Dr. Niti Saxena, [3]Dr. Prakash Chandra Swain, [4]Dr. S. Pramila, [5]Dr. Deepali Rani Sahoo, [6]Mr. K. K. Bajaj, [7]Dr. Umesh Kumar

Submitted: 01/12/2023 **Revised**: 25/01/2024 **Accepted**: 31/01/2024

Abstract: The widespread implementation of renewable energy sources, along with a more proactive approach to managing electricity use, is causing a shift in the way power systems operate and electricity is traded in the market. The P2P economy in particular is benefiting from this change. To efficiently handle the fast changes in renewable power generation at the distribution network level, a local market mechanism that can adapt is required. The efficient and safe operation of the distribution network is also bound to be affected by the extensive adoption of P2P energy trading. This study presents a new paradigm for P2P power trading that accounts for constraints imposed by distribution network security. Specifically, the design makes use of the generalised quick dual ascent method. The article lays out the groundwork for an event-based local peer-to-peer market, which would facilitate rapid and efficient energy swaps inside a certain region. The next step in making sure the distribution system is secure is to evaluate the impact of peer-to-peer transactions on the network using the nodal voltage and network loss in relation to nodal power injections. This allows for an internal determination of how to distribute the costs of P2P energy trading and the incorporation of the external operating constraints. Distributed market-clearing is also applied efficiently by means of a universal quick dual ascent technique. The numerical results show that the proposed model can implement P2P energy trading securely into the distribution system. Furthermore, the method for solving the problem shows remarkable efficiency in achieving convergence.

Keywords: *Peer-to-peer (P2P), Security, Privacy, Network Intelligence, Power Trading Methodologies*

1. Introduction

Peer-to-peer (P2P) power trading methods utilising network intelligence entail the transfer of electricity between individual users or prosumers within a decentralised energy system (Piclo, 2019). It is essential to prioritise the security and privacy of members in order to establish confidence and promote general acceptance of the network.

Global efforts are presently promoting the widespread use of solar power for self-consumption. This is done to decrease the need for investment and minimise operating losses in the transmission as well as the distribution network. Peer-to-peer (P2P) energy trading, an extension of self-consumption, allows prosumers to exchange energy through local distribution systems, potentially reducing strain on the transmission grid. Currently, the decentralised peer-to-peer energy trading market, exemplified by projects like (E. Mengelkamp,et.al., 2018) is becoming a viable choice due to recent advancements in technology for communications and information (C. Feng, et.al., 2020) . The primary objective of P2P sharing is to disrupt the conventional centralised hierarchical control paradigm of power networks and facilitate direct communication and distribution of energy.

2. Related Studies

Blockchain technology guarantees a high level of transparency and prevents unauthorised alterations in peer-to-peer power trading, hence improving the reliability and trustworthiness of transactions. Smart contracts on blockchain have the ability to automate and ensure compliance with the parameters of power trading agreements. (Narayanan, V., et al., 2016). Kshetri, N. (2018) Strong authentication systems, such as digital signatures and multi-factor authentication, are essential for confirming the identity of participants. Authorization, facilitated by either smart contracts or conventional access control techniques, guarantees that only authorised entities are able to participate in transactions. Methods such as homomorphic encryption and zero-knowledge proofs are effective in safeguarding the confidentiality of

[1]*Associate Professor, Department of Computer Science and Engineering, School of Computing, Mohan Babu University, (Erstwhile Sree Vidyanikethan Engineering College, Tirupati, Andhra Pradesh. ORCID ID: 0000-0002-3502-266X*

[2]*Associate Professor, Department of Commerce, Jagannath International Management School, New Delhi*

[3]*Assistant Professor, Department of Commerce, School of Social, Financial & Human Sciences, Kalinga Institute of Industrial Technology (KIIT), Bhubaneswar, Odisha, India*

[4] *Associate Professor, School of Commerce Finance & Accountancy, Christ University, Delhi, NCR*

[5]*Assistant Professor, Symbiosis Law School, Noida, Symbiosis International (Deemed University), Pune, India, ORCID 0000-0001-6949-7439*

[6]*RNB Global University, Bikaner, Rajasthan*

[7]*Professor, Glocal University Pharmacy College, Glocal University, Saharanpur, U.P.*

sensitive data during peer-to-peer power transactions. These techniques enable computations to be performed on encrypted data without disclosing the real information (Zyskind, G., et al., 2015). Mendling et al. (2007) argue that the utilisation of decentralised identification solutions on blockchain and reputation systems plays a crucial role in fostering trust among participants in P2P power trading, by guaranteeing that only users with a good reputation are involved. (Rescorla, E., 2018) Deploying robust communication protocols such as TLS/SSL ensures the safeguarding of data during transmission, effectively thwarting interception and manipulation attempts by unauthorised individuals. (Roman, R., et.al., 2018) It is crucial to incorporate security measures at the edge devices, such as secure boot processes and regular security updates, in order to protect against local attacks in P2P power trading. Complying with regional and international norms and regulations is crucial in order to guarantee data protection and privacy in peer-to-peer power trading. This contributes to establishing trust in the system. (Whitman, M. E., 2018) The implementation of an incident response plan and the regular execution of user education programmes enhance the overall security stance, facilitating prompt reactions to security incidents and increasing users' awareness of potential hazards.

Detailing of Security and Privacy Components for Peer-to-Peer Power Trading Methodologies

Authentication: Implement secure authentication mechanisms to verify the identity of participants in the P2P trading network. This may involve the use of cryptographic techniques such as digital signatures or biometric authentication.

Authorization: Define and enforce access controls to ensure that only authorized participants can engage in power transactions. Role-based access control (RBAC) can be employed to manage permissions.

3. Data Encryption:

Communication Encryption: Utilize encryption protocols (e.g., TLS/SSL) to secure communication channels between participants. This prevents eavesdropping and man-in-the-middle attacks.

Data-at-Rest Encryption: Encrypt stored data to protect sensitive information, such as transaction records and user details, stored on servers or in the blockchain.

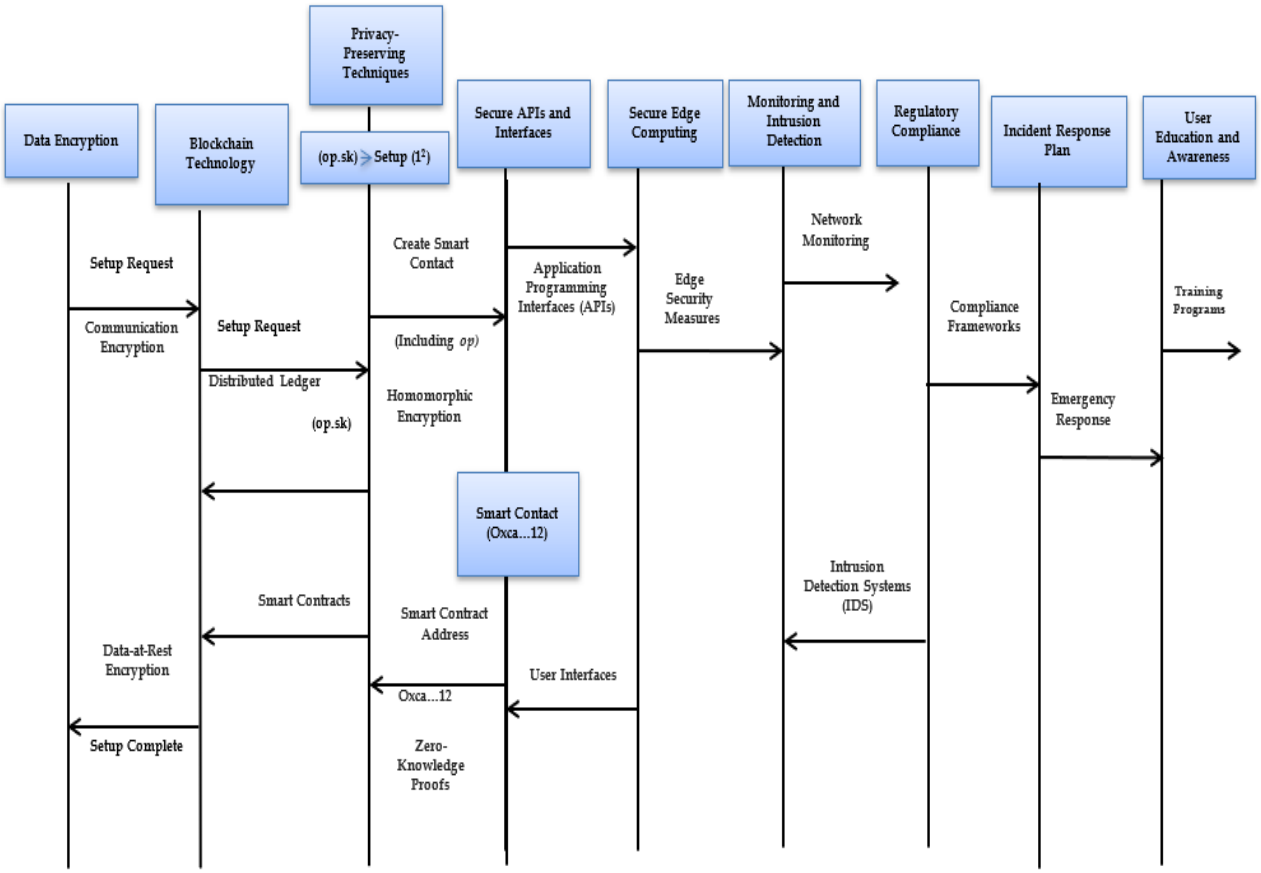


Fig 1: Implementation Diagram of Security and Privacy Components for Peer-to-Peer Power Trading Methodologies
Blockchain Technology:

Distributed Ledger: Implement a blockchain or distributed ledger technology to maintain a transparent and tamper-proof record of all transactions. This ensures the integrity of the power trading process and reduces the risk of fraud.

Smart Contracts: Use smart contracts to automate and

enforce the terms of power trading agreements. Smart contracts are self-executing and can help eliminate the need for intermediaries.

Privacy-Preserving Techniques:

Homomorphic Encryption: Explore the use of homomorphic encryption to perform computations on encrypted data. This allows calculations to be carried out without exposing the raw data, enhancing privacy.

Zero-Knowledge Proofs: Implement zero-knowledge proofs to validate the truth of a statement without revealing any information about the statement itself. This can be useful in verifying transactions without disclosing the specific details.

Secure APIs and Interfaces:

Application Programming Interfaces (APIs): Ensure that APIs used for communication between different components of the P2P power trading system are secure. Employ standards like OAuth for secure API authentication and authorization.

User Interfaces: Design user interfaces with security in mind, including features like multi-factor authentication and secure password policies.

Secure Edge Computing:

Edge Security Measures: If edge computing is employed, implement security measures at the edge devices to protect against local threats. This includes secure boot processes and regular security updates for edge devices.

Monitoring and Intrusion Detection:

Network Monitoring: Deploy robust network monitoring tools to detect and respond to any abnormal activities or potential security threats.

Intrusion Detection Systems (IDS): Implement IDS to identify and alert on any unauthorized access or malicious activities within the P2P power trading network.

Regulatory Compliance:

Compliance Frameworks: Adhere to relevant data protection and privacy regulations. Ensure that the P2P power trading system complies with regional and international standards to build trust among participants.

Incident Response Plan:

Emergency Response: Develop an incident response plan to efficiently address and mitigate security incidents. This includes procedures for notifying affected parties and authorities in the event of a data breach or security incident.

User Education and Awareness:

Training Programs: Conduct regular training programs to educate participants about security best practices and potential risks associated with P2P power trading. Informed users are better equipped to protect themselves and the overall network.

Utilizations of the Finite Volume Method in Solving P2P Trading Equations

Applying the Finite Volume Method (FVM) to simulate P2P trade requires formulating mathematical equations that represent the pertinent physical or economic processes. The precise equations will vary based on the individual attributes of the P2P trade system being modelled. Below are few versatile equations that can be customised for this specific objective:

Mass (or Energy) Conservation Equation: Within a peer-to-peer trading system, it is possible to establish a mass (or energy) conservation equation for every trading node. Q_i represents the quantity of the exchanged commodity, such as energy, at node i. The conservation equation can be expressed in the following manner:

$$\frac{dQi}{dt} = \sum j \in neighbors\ of\ i\ (Q_j\ -\ Q_i)$$

Price Propagation Equation: To simulate the spread of prices in the network, you can incorporate a price variable P_i at each trading node. The equation for price propagation can be stated as:

$$\frac{dPi}{dt} = \sum j \in neighbors\ of\ i\ (P_j\ -\ P_i)$$

K_{ij} denotes the coupling coefficient between nodes i and j.

Transaction Dynamics: To simulate the interactions between nodes, one can employ equations that regulate the movement of goods. For example, the rate at which transactions occur from node i to node j, denoted as T_{ij}, can be directly proportional to the difference in prices and may be subject to certain limitations:

$$\overline{Tij = Kij\ (P_i - P_j)}$$

Utility or Profit Maximization Equations: Participants in peer-to-peer trade strive to optimise their utility or financial gain. One can establish utility or profit functions for each player and create optimisation problems. As an illustration:

Maximize $U_I \bigcup_{.} i(Q_1 p_i)$ subject to constraints

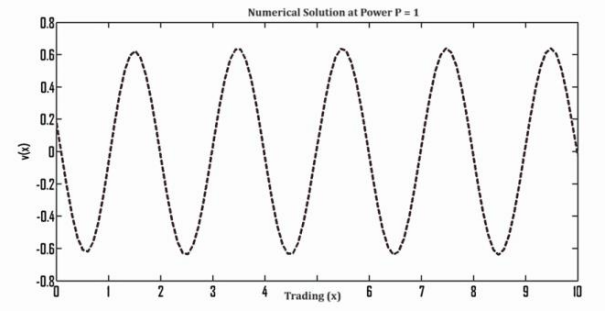
Capacity Constraints: If there are limitations on the capacity of the trading nodes, you can include these limitations in the equations. For instance, the quantity Q_i transacted at node i must adhere to the following condition:

$\overline{Qi \leq Q_{\max i}}$

Regulatory Compliance Equations: Peer-to-peer trading systems frequently must comply with regulatory mandates. Derive mathematical equations that guarantee adherence to pertinent requirements. For example, make sure that transactions comply with environmental standards or regulatory quotas.

Dynamic Pricing Equations: To simulate dynamic pricing techniques, one can use equations that depict how participants modify their prices in response to market conditions, historical data, or external influences.

Fig 2: Numerical Solution Finite Volume Method in Solving P2P Trading Equations



It is imperative to modify these universal equations to suit the particular circumstances and goals of your peer-to-peer trading platform. In addition, it is necessary to take into account the discretization of both space and time, establish boundary conditions, and use suitable numerical techniques to solve the resulting system of equations using the Finite Volume Method.

Authentication and Authorization of P2P Power Trading

Authentication and permission are essential elements of security in peer-to-peer power trading systems. They have a vital function in guaranteeing that only valid and authorized individuals can participate in transactions within the network.

Table 1: P2P Power Trading Approaches for Authentication and Authorization Using Security & Privacy Components

S.No.	Parameters	Authentication Consideration:	Authorization Consideration:	Secure Communication Consideration:	Decentralized Trust Mechanisms Analysis:	Continuous Authentication Analysis:	Secure Key Management Analysis:
1	(UIV)	✓	✓	⊙	👁‍🗨	⊙	✓
2	(DSC)	✓	✓	✓	✓	✓	👁‍🗨
3	(DID)	✓	⊙	✓	✓	👁‍🗨	⊙
4	(RBAC)	✓	✓	✓	✓	✓	✓
5	(SC)	✓	✓	👁‍🗨	⊙	✓	✓
6	(GAC)	👁‍🗨	👁‍🗨	✓	✓	👁‍🗨	✓
7	(TLS)	⊙	✓	✓	✓	✓	⊙
8	(SAPIs)	✓	✓	✓	👁‍🗨	✓	✓

9	(CAthms)	✓	✓	✓	✓	✓	👁‍🗨
10	(PRS)	✓	◎	👁‍🗨	◎	✓	✓
11	(BLsis)	◎	👁‍🗨	✓	✓	👁‍🗨	◎
12	(BCA)	👁‍🗨	◎	✓	✓	◎	✓
13	(KR)	◎	👁‍🗨	✓	✓	✓	👁‍🗨
14	(HSMs)	◎	◎	👁‍🗨	◎	👁‍🗨	◎

✓ Full Consideration, 👁‍🗨 Not at all Considered, ◎ Partially Consideration || (UIV) - User Identity Verification, (DSC) - Digital Signatures, (DID)- Decentralized Identity, Role-Based Access Control (RBAC), (SC)- Smart Contracts, (GAC)- Granular Access Controls, (TLS)- Transport Layer Security,

(SAPIs)- Secure APIs, (CAthms)- Consensus Algorithms, (PRS)- Peer Reputation Systems, (BLsis) - Behavioral Analysis, (BCA)- Biometric Continuous Authentication, (KR) - Key Rotation, (HSMs)- Hardware Security Modules

4. Validation: P2P Power Trading Approaches

By including strong authentication and authorization procedures into the P2P power trading system, stakeholders can guarantee the reliability, privacy, and legitimacy of transactions, promoting confidence among participants and reducing the likelihood of unauthorised access and bad behaviour.

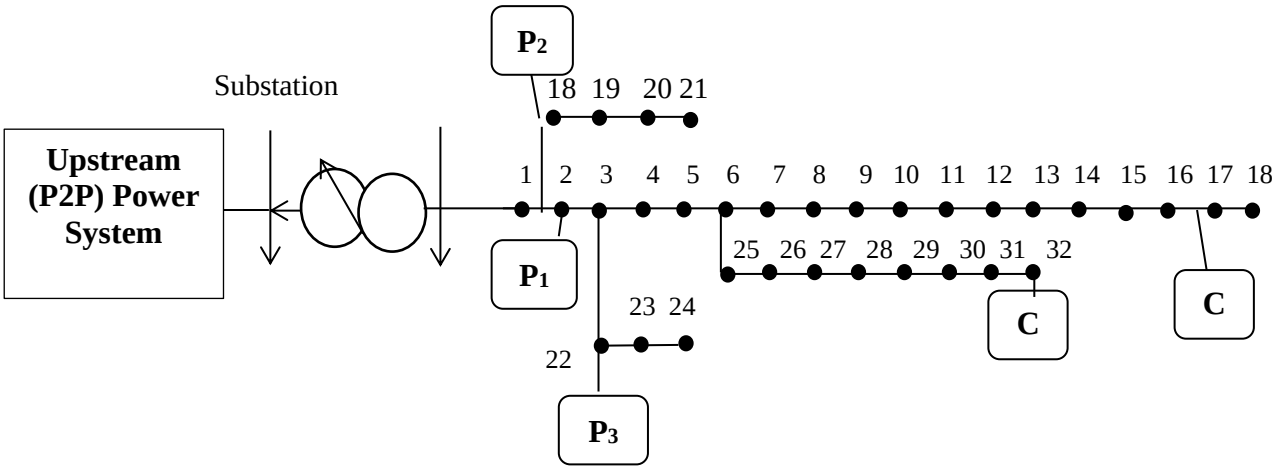


Fig 3: Frequency Validating Model for Upstream P2P Power System

Uniquely identifying participants is necessary in the P2P power trading network to establish their identity. Conventional techniques such as using username-password combinations, biometric authentication, or multi-factor authentication (MFA) can be utilised. Employ digital signatures to authenticate messages or transactions. Every participant is assigned a unique private key for message signing, while the public key is utilised for verification purposes.Leverage decentralized identity solutions to allow participants to manage their identities without relying on a central authority. Blockchain-based identity systems can provide a secure and tamper-resistant way to verify identities.

Integrate Role-Based Access Control (RBAC) to establish and oversee the authorization levels of various

participants involved in the peer-to-peer power trading system. Individuals in various roles, such as consumers, prosumers, and administrators, might be granted distinct access privileges that align with their respective tasks. Employ smart contracts on a blockchain to automate the process of granting authorization. A power trade agreement can have its terms and conditions encoded in a smart contract, which guarantees that the contract will automatically execute and cannot be tampered with. Establish granular access controls to limit access to particular functionality or data. For instance, a participant may possess the privilege to access the transaction history but lacks the authority to alter it.

Employ TLS or alternative secure communication protocols to cypher data during transmission among participants. This measure ensures the protection of sensitive data, such as authentication credentials and transaction details, from unauthorised interception and manipulation. For the P2P power trading system, it is important to secure the communication APIs by implementing appropriate authentication techniques such as API keys or OAuth. This will effectively prohibit unauthorised access.

Consensus algorithms in blockchain-based P2P power trading systems are responsible for fostering confidence among participants. By achieving consensus on the legitimacy of transactions, the requirement for a central authority is eliminated, and trust is evenly spread throughout the network. Introduce reputation systems that allow players to establish trust gradually by demonstrating their conduct within the network. This reputation has the potential to impact their degree of authorization within the system.

Deploy persistent authentication mechanisms, such as behavioural analysis, to continuously monitor and assess user behaviour across an extended period. Any departure from the typical behaviour patterns may prompt supplementary authentication verifications or notifications. To confirm the authenticity of the participant who began key transactions, it is advisable to use continuous biometric authentication.

Periodically change cryptographic keys to minimise the consequences of a compromised key. This is especially crucial in systems that employ cryptographic keys for authentication and authorization. Utilise Hardware Security Modules (HSMs) to securely store and oversee cryptographic keys, hence enhancing security measures against unauthorised access to sensitive keys.

5. Conclusion

Implementing a comprehensive security and privacy framework in the context of P2P power trading methodologies using network intelligence is essential to create a resilient and trustworthy energy trading ecosystem. Regular updates, security audits, and collaboration with cybersecurity experts can further enhance the robustness of the system against emerging threats. By integrating robust authentication and authorization mechanisms into the P2P power trading system, stakeholders can ensure the integrity, confidentiality, and authenticity of transactions, fostering trust among participants and mitigating the risk of unauthorized access and malicious activities. It is of the utmost importance to modify these generic equations in accordance with the particular circumstances and goals of your peer-to-peer trading model. Additionally, in order to solve the resulting system of equations using the Finite Volume Method, you might need to take into consideration the discretization of space and time, set boundary conditions, and choose appropriate numerical methods.

References

[1] Adhikari, J. P., & Das, D. R. (2015). Assessing The Best Path In Routing For Network Security. Kaav International Journal of Science, Engineering & Technology, 2(1), 95-105. https://www.kaavpublications.org/abstracts/assessing-the-best-path-in-routing-for-network-security

[2] C. Feng, F. Wen, S. You, Z. Li, “Coalitional game-based transactive energy management in local energy communities,” IEEE Trans. Power Syst., vol. 35, no. 3, pp. 1729-1740, May 2020.

[3] D., A. M. (2023). Deep Neural Network for Classification of Inside Scene. Kaav International Journal of Science, Engineering & Technology, 10(2), 1-6. https://doi.org/10.52458/23485477.2023.v10.iss2.kp.a1

[4] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, “Designing microgrid energy markets: A case study: The Brooklyn microgrid,” Appl. Energy, vol. 210, pp. 870–880, Jan. 2018.

[5] European Union Agency for Cybersecurity (ENISA). (2018). "Smart Grid Information Security: Overview of the current state of the art, key challenges, and recommendations."

[6] Kshetri, N. (2018). "Blockchain's roles in strengthening cybersecurity and protecting privacy."

[7] Mendling, J., Weber, I., & van der Aalst, W. M. P. (2007). "Analysis of Web Services Composition Languages: The Case of BPEL4WS."

[8] Mishra, R. P., & Kapse, S. (2017). Cybercrime: A Hazard to Network Surveillance (1st ed., pp. 447-

451). Kaav Publications. https://www.kaavpublications.org/spiabstracts/cybercrime-a-hazard-to-network-surveillance

[9] Narayanan, V., et al. (2016). "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction."

[10] Rescorla, E. (2018). "The Transport Layer Security (TLS) Protocol Version 1.3."

[11] Roman, R., Lopez, J., & Mambo, M. (2018). "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges."

[12] Piclo, “Building software for a smarter energy future”, 2019, [Online]. Available: https://piclo.energy.

[13] P. (2017). Formal Verification of Energy Saving Techniques In Wireless Sensor Networks (WSN). Kaav International Journal of Science, Engineering & Technology, 4(3), 132-139. https://www.kaavpublications.org/abstracts/formal-verification-of-energy-saving-techniques-in-wireless-sensor-networks-wsn

[14] Upadhyay, A. (2015). History, Importance And Future Of Network Security. Kaav International Journal of Science, Engineering & Technology, 2(1), 9-14. https://www.kaavpublications.org/abstracts/history-importance-and-future-of-network-security

[15] Whitman, M. E., & Mattord, H. J. (2018). "Management of Information Security."

[16] Zyskind, G., et al. (2015). "Enigma: Decentralized Computation Platform with Guaranteed Privacy."