CYBERSECURITY IN CENTRALISED VS DECENTRALISED ENERGY SYSTEMS

Dr Zoya Pourmirza
NEWCASTLE UNIVERSITY
FEBRUARY 2023

Supergen
Energy Networks

Cyber Security in Centralised vs Decentralised Energy Systems

I. Decentralised Energy Systems

A decentralized energy system is a network of energy generation and distribution systems which are controlled by multiple independent entities, (e.g., homes, organizations, and communities), rather than being controlled by a single authority such as grid control centre. Decentralized energy systems enable local generation and consumption of energy, which can reduce the greenhouse gas emissions while offering a more resilient, reliable, and sustainable energy supply.
This report investigates cyber security for decentralised and centralised energy systems and discuss pros and cons of each system by exploring three categories of Identity management, energy trading, and network topology.

II. Cyber security for consumer identity management in centralised vs decentralised energy system

Components such as generators, distribution lines, EV charging stations, and substations in the digital energy systems have their unique identity and require an identity management system to be able to interact with other components. A decentralised identity solution used in a decentralised eco systems will spread out data rather than managing and controlling them in a centralised manner. This can help components talk together without having a central authority, avoid single point of failure, and increase the resilience of the system. Additionally, if personal information of one component or prosumer is compromised, it will not affect the information of other components or users.
With the advance of technology such as blockchain, a decentralised prosumer identity managements have eased the privacy challenges for energy systems [1]. This is in contrary to the previous belief that centralised system proved to be more secure and provided enhanced privacy for the users.
Blockchain ensures private data remains immutable and secure, improves transparency, and enables users to own and control their data. Digital identities can be stored on a platform with a private key that grants access to the verified user only. This will mitigate the data breach risk and will prevent unauthorized access to the prosumers and components data within energy sector [2].

III. Cyber security for energy trading in centralised vs decentralised energy system

Traditionally energy trading is being managed by a centralised entity and the security of the system maintained by securing the central systems (e.g., grid control rooms). While centralised systems can provide secure energy trading, but the single point of failure, privacy concerns, and dependency on the centralised entity are some its main challenges. These issues within centralised energy trading supports the transition from centralised to decentralised energy trading [3].
P2P energy trading, which is a form of decentralised energy trading, is a new paradigm where buildings can produce and share energy locally. This paradigm addresses the flexible energy trade between energy prosumers, where excess energy from one building can be

traded between other neighbours within their community. While this decentralised system can reduce the cost for energy customers and CO2 emissions, but it creates new security challenges, as the system is now composed of many interconnected nodes that need to be secured individually. This decentralised energy trading needs to prevent unauthorized access to the system, ensure the authenticity and integrity of transactions, and secure the communication channels between nodes. Blockchain technology has the potential to improve the security of a decentralised energy trading by providing immutability which offers integrity and a high degree of accountability. It uses hash functions and public-key cryptography, an asymmetric cryptography protocol, to provide authentication (ensuring transaction is initiated by the source it claims to be from) and authorisation (ensuring actions are performed by eligible users) [4]. Additionally, blockchain can improve trust between parties by removing dependency on centralized control [3]. However, blockchain technology still has privacy and security concerns which needs to be considered, such as blockchain wallet theft, security threats because of quantum computing, security issues in blockchain integration with constrained devices, transaction linkability, non-erasable data in blockchains, Bitcoin address tracing through P2P network traffic analysis and compliance with regulations [5].
To summarise, table 1 compares the centralised energy trading and P2P energy trading.

	Centralised Energy Trading	P2P Energy Trading
Control	Centralised	Decentralised
Security	Risks of hacking is lower, as there is only one central node to attack, but the impact of such attacks are extremely high	Risks of hacking is higher, due to increased attack surface, but it has lower impact as it is difficult to compromise the whole system
Privacy	Less privacy, as data are stored and managed in a centralised location	Higher privacy, as data are on multiple locations
Transparency	Transparency is lower, as data is stored in a central location	Transparency is higher in P2P, as data is stored on multiple locations
Vulnerability	Less vulnerable to hacking and tampering of data, as data are being managed and secured at one central location	More vulnerable to hacking and tampering of data because it builds new networks and connections between prosumers and components, which introduce new points of vulnerability that can be exploited

Table 1 Centralised energy trading vs P2P energy trading

IV. Cyber security for network topology of centralised vs decentralised energy system

Centralised topologies are the ones where all the data and services are concentrated in a central node which makes it fairly easy to manage. Other advantages of the centralised topology are its simplicity and the fact that it offers information coherency, whereas the potential single point of failure is its main disadvantage, which makes it a prime target for attacks. The scalability (referring to the ability to add more nodes and machines to the system, such as having more smart meters) in centralised topology is questionable, and the extensibility (referring to the ability to add more resources and data, for example smart meters capturing data with higher frequency) in a centralised topology is hard to achieve because new resources can only be added to the central node [6]. Regarding the cyber security measures, it is easier to implement security measures and policies, and to monitor the system for any security incidents, but the cost of implementing such cyber security measures is high due to its complexity. For example, in energy systems it is easier to manage and secure a centralized control system that manages and monitors the energy supply network, as the security threats can be identified and monitored easier. However, this centralised control centre can be a prime target for cyber-attacks.

In decentralised topology, nodes can communicate with each other through other nodes in the network which act as a relay, and can be a service provider, or a consumer or both. This topology is extensible and scalable, and a single point of failure could be avoided [6]. Accordingly, decentralisation can help provide a more resilient network which can avoid highly vulnerable central control unit and prevent single point of failure and provide faster control actions when required [7]. Although offering information coherency, managing network, implementing security measures and policies, and monitoring the system for security incidents is difficult in decentralised energy network, but at the same time is more difficult for hackers to compromise the entire network. However, if cyber attacks occur simultaneously at multiple points, they can have greater impact. For example, it is more difficult to monitor and control smaller Distributed Energy Resources (DERs) [8] such as wind turbines and rooftop solar panels. Generally, DERs have more vulnerable points for cyber-attacks [9]. Additionally, decentralisation in energy systems can present unique cyber security challenges due to its distributed nature, increased attack surface, and reliance on communication and information technology. These security challenges in energy systems could be mitigated by implementing a number of security measures such as encryption, access control and authentication mechanism, network segmentation, regular monitoring and auditing, having incident response plan, and software and devices updates with the latest security patches.

To summarise, table 2 compares the centralised topology and decentralised topology.

	Centralised Topology	Decentralised Topology
Resilience	Less resilience due to single point of failure	Higher resilience
Manageability	Easy to manage	Difficult to manage
Vulnerability to cyber attack	Highly vulnerable on central control system, with great impact	Less vulnerabilities due distributed control and management, with less impact

Cost of cyber security	High cost of securing the complex central system	Lower cost of securing decentralised systems with less complexity
Response time	Slower because of higher latency and coordination of actions takes more time	Faster because of lower latency and distributed decision making
Scalability	Questionable	Higher scalability
Extensibility	Lower extensibility	Higher extensibility

Table 2 Centralised topology vs decentralised topology

References

[1] Alanzi, H. and Alkhatib, M., 2022. Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review. Applied Sciences, 12(23), p.12415.

[2] Zhang, S., Rong, J. and Wang, B., 2020. A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain. International Journal of Electrical Power & Energy Systems, 121, p.106140.

[3] Ali, F.S., Aloqaily, M., Alfandi, O. and Ozkasap, O., 2020. Cyberphysical blockchain-enabled peer-to-peer energy trading. Computer, 53(9), pp.56-65.

[4] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P. and Peacock, A., 2019. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and sustainable energy reviews, 100, pp.143-174.

[5] Thukral, M.K., 2021. Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: A review. Clean Energy, 5(1), pp.104-123.

[6] Minar, N., 2002, January. Distributed systems topologies: Part 2. In Emerging Technology Conference.

[7] Wang, Y., Yemula, P. and Bose, A., 2014. Decentralized communication and control systems for power system operation. IEEE Transactions on Smart Grid, 6(2), pp.885-893.

[8] De Carvalho, R.S. and Saleem, D., 2019. Recommended functionalities for improving cybersecurity of distributed energy resources (Vol. 1, pp. 226-231). IEEE.

[9] Qi, J., Hahn, A., Lu, X., Wang, J. and Liu, C.C., 2016. Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Physical Systems: Theory & Applications, 1(1), pp.28-39.