Cleaner Engineering and Technology 8 (2022) 100481

Contents lists available at ScienceDirect

Cleaner Engineering and Technology

journal homepage: www.sciencedirect.com/journal/cleaner-engineering-and-technology

Blockchain-based trust management and authentication of devices in smart grid

Vasudev Dehalwar [a], Mohan Lal Kolhe [b,*], Shreya Deoli [a], Mahendra Kumar Jhariya [a]

[a] Maulana Azad National Institute of Technology, Bhopal, 462003, MP, India
[b] University of Agder, Faculty of Engineering and Science, PO Box 422, Kristiansand, NO, 4604, Norway

ARTICLE INFO

Keywords:
Smart grid
Blockchain
Self-soveregin idetification
Distributed ledger
Identification
Authentication

ABSTRACT

The digitalization of the power grid and advancement in intelligent technologies have enabled the service provider to convert the existing electrical grid into a smart grid. The transformation of the grid will help in integrating cleaner energy technologies with energy management to improve power network efficiency. Internet of things (IoT) and various network components need to be deployed to harness the full potential of the smart grid. Also, integrating intermittent renewable energy sources, energy storage, intelligent control of selected power-intensive loads, etc will improve energy efficiency. But deployment of this information and communication technologies will make the grid more vulnerable to cyber attacks from hackers. In this work, blockchain-based self-sovereign identification and authentication technique is presented to avert identity theft and masquerading. The proposed approach can minimize the chances of identity-based security breaches in the smart grid. This paper provides an overview of the model of identification and authentication of IoT devices in Smart Grid based on Blockchain technology. The Blockchain based implementation of identification and authentication of devices is proposed to validate the model in the distributed electrical energy network. The model is able to authenticate the device using Blockchain in a trusted model. The system works according to plan validating the authenticity of transaction in a node in log(n) time, which justifies presented result.

1. Introduction

The electrical energy systems are facing tremendous challenges for integrating sustainable energy technologies to contribute to net-zero energy targets (IEA, 2019). Advancements in information and communication technologies (ICT) can help in digitalizing the electrical energy network (i.e. smart grid) for intelligent operation with increased penetration of renewable energy sources (Kolhe, 2012). The smart grid operation can help in improving power system reliability and security. The power grid's digitalization has created an opportunity to manage operations more efficiently. Smart grid operation, especially within the distributed network will work for multi-directional energy and information flows via coordinated distributed clean energy technologies with the help of higher-capacity power generators located at medium and/or higher voltages levels (Refaat et al., 2021). A smart grid will facilitate the active participation of distributed energy sources and energy management of selected non-critical power- intensive loads using ICT networks and IoT devices. In order to optimize the utilization of electricity, a demand management system must be developed (Kolhe, 2015).

Smart Grid requires a large-scale deployment of network components for monitoring and control. Interoperability of the system requires integration of resources at multiple levels, such as networking, cloud database, operating system, etc. for smart and resilient system (McLaughlin et al., 2015). The existing TCP/IP-based grid network has many weaknesses that have been exposed over the past. The massive deployment of network components for digitizing the electrical energy network may render the grid vulnerable to cyber-attacks from hackers (Ulltveit-Moe, 2015). The critical infrastructure (i.e., electrical energy network) is under a persistent threat from evil-intention cyber-criminals/enemies. These criminals are weaponizing themselves by developing sophisticated surveillance tools to mount an attack on critical infrastructure. Therefore, protecting these critical assets from cyber-attacks is very important.

The smart grid security is tightly coupled with a communication network; so, Authentication, Authorization and Access Control (AAA) must be strictly enforced at the device level (Amrani et al., 2016). It is

* Corresponding author.
E-mail addresses: vasudevd@gmail.com (V. Dehalwar), mohan.l.kolhe@uia.no (M.L. Kolhe), shreyadeoli169@gmail.com (S. Deoli), mahendra_jhariya@rediffmail.com (M.K. Jhariya).

https://doi.org/10.1016/j.clet.2022.100481
Received 2 May 2021; Received in revised form 9 March 2022; Accepted 30 March 2022
Available online 5 April 2022

reported that nearly 90% of all power outages occur at the distribution network level (Budka et al., 2014). The machine-to-machine communication in the smart grid needs to be secure and authenticated (Dehalwar et al., 2016). The endpoints in the distribution network like the smart meter are the point of contact with the grid and they are the weakest link in the chain of security (Dehalwar et al., 2017a). Some malicious endpoints may create identity theft, Sybil attack, load-altering attack, false data injection attack, etc., which may give wrong feedback to the control center of the grid resulting in taking faulty decisions (Le et al., 2017). The wrong feedback may prompt control center to take erroneous decision which may have serious consequences such as blackout. The 2014 cyber-attack on Iranian uranium enrichment plants via Stuxnetorm is an example of a security breach that a cybercriminal could cause (Stoustrup et al., 2018). Even vibration generated by different devices/components can be profiled to identify a device installed at a given point in a network. Because of the damaging potential of the endpoint devices, it is imperative to have proper identification and authentication of devices in order to eliminate the possibility of attacks (Nuss et al., 2018).

Threat mitigation has three major steps: (i) prevention, (ii) detection, and (iii) elimination. In order to have a resilient Smart Grid, the security threats need to be addressed at different levels of power generation, transmission, and distribution. If the standard operating procedure and best practices of risk assessment are carried out, there are chances of minimising the security risk.

The Blockchain is distributed open ledger technology that is primarily used for cryptocurrencies, but has the potential to be used for other applications also like electronic voting, health care, supply chain, device identification, transport network, etc. (Maesa et al., 2020). It provides easy and efficient verification of the transaction between the users based on Smart Contract (Wu et al., 2019). Blockchain works on the principles of distributed computing, maintaining a distributed ledger (Bouras et al., 2020). A digital ledger-based record keeping technology, records all the transaction performed between the users using digital signature and cryptographic hash function (Sockin et al., 2020). A block is an entity of record which can be appended to the core chain of Block after verification using the consensus algorithms such as Proof of Work, Proof of Stake, etc. Current Blockchain version 3.0 will be used for wide-ranging applications. Standardization activities by ISO and IEEE are also going on internationally in the area of IoT security. ISO/IEC 30141 has provided the reference architecture for IoT, which includes ISO/IEC 27400 — Cybersecurity — IoT security and privacy – guidelines (O'Reilly et al., 2021). These guidelines provide security and privacy requirements for IoT devices. When ISO guidelines are integrated with the blockchain technology for identification, authorization, and authentication, better security and transparency can be attained amongst all the stakeholders of Smart Grid.

Blockchain based technologies are going to revolutionise electricity energy operations and market mechanism (Iberdrola, 2022). It is going to be used for allocating net zero energy requirements at a specific node via establishing hierarchical priorities (e.g., prioritization of renewable energy, maximization of local energy resources, etc.). Blockchain technology solution can be implemented for ancillary services of the electrical energy network for making power system more reliable and secure (Powerledger, 2022).

In this work, blockchain-based self-sovereign identification/authentication technique has analysed to avert the identity theft and masquerading. This paper provides a model of identification/authentication of IoT devices based on Blockchain technology. Also, implementation of identification/authentication is presented to justify the results. The presented approach can minimize the chances of identity-based security breaches in the smart grid. The paper comprises six sections. Section 2 discuss the general models of identifications and authentication with a focus on digital identity. Section 3 provides challenges to identity management and potential attacks on Smart Grid. It also identifies challenges to blockchain based implementation in distributed environment. Section 4 discuss the proposed model of implementation. Section 5 gives implementation details and the final outcome. Conclusions are provided in Section 6.

2. Identification and authentication

Identity management systems are the foundation for co-operations between devices/entities (i.e., users, issuers, and authenticators). Authentication of the message, message generator, transmission medium, and the process itself are an important part of identification and authentication (Amrani et al., 2016). Identification and authentication are used together as a single two-step process to establish the identity of an entity (Denning, 1982). The system binds device/entity, issuer, authenticator, and application to prove an unambiguous identification of a device/entity (Kuperberg, 2019). It is also essential to establish accountability and rights to access the resources. An issuer/entity may own applications or services in the system, and other devices/entities can request access to these services, but these services are provided only after the identity of the devices/entity is authenticated and access permission is verified.

Identity can be authenticated through biometrics information, documents, or personal information. In a computer network, an IP address and MAC address identify a machine. In e-commerce, a digital certificate issued by Certification Authority (CA) identifies a transaction. This digital certificate is exchanged between the client and server using TSL/SSL security protocol over the Internet to authenticate each other (Dehalwar et al., 2016). Clients and servers maintain states through cookies to simplify the transaction over the Internet. Cookies may contain authentication information of the user and host.

The identity management models of user are classified as isolated, centralized, federated, user-centric, and Self Sovereign (Bartolomeu et al., 2019). The basic isolated user identity model known as SILO model, which is depicted in Fig. 1. The user has to register individually with each service provider (SP); and each SP has its own identity domain, and all identity-related operations are performed on a specified domain, which is not applicable for cross-domain verification. This process results in multiple identifiers and associated credentials on multiple domains/platforms that are cumbersome to maintain on various platforms. A centralized model provides a single point of entry for all service providers through a unique identity verifier, which is supplied by a single identity provider. It allows a Single Sign On (SSO) for all the resources. This unique identity has a weakness of a single point of failure, which means a hacker can target a single identity to expose the entire database of identity.

A federated model is a hybrid of isolated and centralized models. Federated identity consists of a group of service providers (SP) that have trust relationships with each other to exchange digital identity information (Amrani et al., 2016). It eliminates the replication of data in multiple service providers. It consists of an identity provider (IdP) and

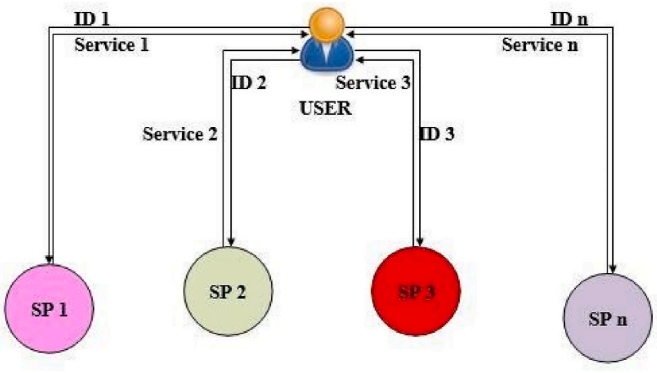

Fig. 1. An isolated user's identity model (Amrani et al., 2016).

one or more SPs. The attributes (IdP, SP and User) are used to authenticate the user. The shared domain between IdP and SP is a federated domain created when a contract-based trust rating is shared between IdP and their respective SP. Fig. 2 depicts the idea of Federated identity.

A user-centric model is like a Federated model but without trust (Amrani et al., 2016). It does not have domain restriction and the SP can grant or deny user access to the requesting party. User-centric identity manages private and sensitive identity information of the user from their perspective (Nuss et al., 2018). Users can control their own digital identities without relying on a third party. They have complete control over their identity data. Users can decide which credential to share with the requesting party. Due to the lack of trust, this model is also known as the open trust model. Fig. 3 illustrates the user-centric model.

The self-sovereign model eliminates the dependence on a trustworthy central authority (Gruner et al., 2019). With the traditional identity management system, it is difficult for internet users to manage their own digital identities (Houtan et al., 2020). In a self-sovereign model, the service provider can access identification information, but only with the consent of the user (Bartolomeu et al., 2019). Sovrin, uPort, and OneName are examples of self-sovereign identity systems (Kassem et al., 2019). Flexibility and security are added in a self-sovereign identity, as users only reveal their personal information on a need-to-know basis. In case of more than one identity, the identifiers can present claims associated with relevant identifiers without revealing the complete identity. Identities are persistent, interoperable, and portable. User rights are protected in every condition. Fig. 4 illustrates the diagram of the self-sovereign model.

An attacker may hack the central server where the relying party is storing the users' credentials. The users' privacy and confidentiality are compromised through these illegal activities, leading to loss of identity. Developing a user-centric self-sovereign identity management system can overcome these drawbacks. It will empower the user to have absolute control of his credentials over the Internet. Our endeavour is to develop a unique self-sovereign digital identity management system for devices using Blockchain technology to prevent attackers originating from end-devices.

An electrical grid is a network of power generation, transmission, and distribution. Communication and coordination with the control center play an essential role in monitoring and control of the grid. There are multiple security risks to Smart Grid in terms of data tampering, impersonation, man-in-the-middle attack, denial of service, Phishing, Spoofing, Sybil attacks, etc. (Kolb et al., 2020). Device identification, authentication, and management will help the Smart Grid to eliminate identity theft, impersonation, and password breaches (Li et al., 2019). By binding the device's identity with the resources list, the Smart Grid will severely reduce the surface of the attack and harden the network security.

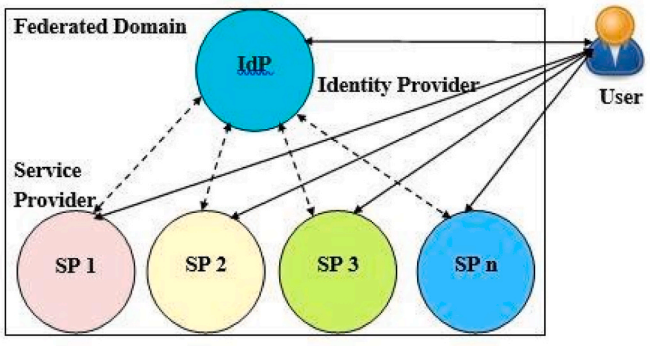

Fig. 2. Federated user identity model (Amrani et al., 2016).

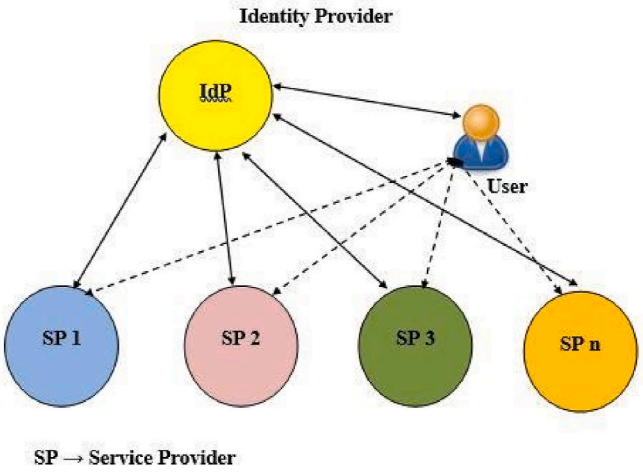

Fig. 3. User-centric identity model (Amrani et al., 2016).

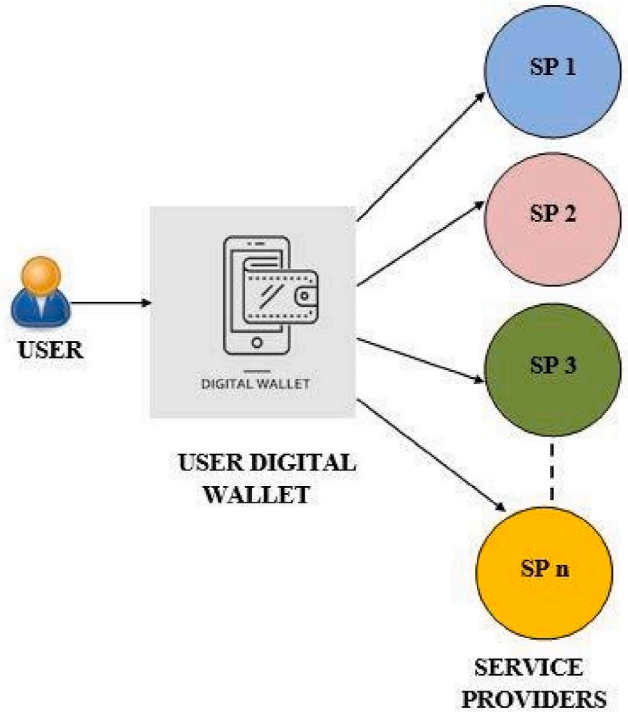

Fig. 4. Self-Sovereign user identity model (Mühle et al., 2018).

3. Challenges in identity management

Access to resources at the right time and right place require proper identification, authentication and access management. The cybersecurity and privacy challenges are evolving for IoT. Important considerations have to be made to understand the security aspects of device communication and identifications.

3.1. Security challenges

The smart meter in Advanced Metering Infrastructure (AMI) is Smart Grid's perimeter (Dehalwar et al., 2017c) in home area network. AMI is a part of the distribution power network that collect massive multi-source data in real-time. Many advanced technologies of such as Phasor Measurement Unit (PMU), IoT, and Machine to Machine (M2M) communication will also generate massive amounts of data called Big

Data in power network (Sousa et al., 2020). Dispatching this Big Data to the control center for efficient decision-making is a big task. The majority of last-mile communication will be wireless because of the wide geographic spread of the Smart Grid. The onset of a 5G wireless network with high-speed data communication will be the harbinger of next generation communication. Capacity management of wireless networks will be critical for power protection in a reliable Smart Grid. The attacker may inject false data on the fly to give wrong information to the control center. This may lead to abnormal situations in the grid, resulting in a blackout or power outage. Following are some of the common attacks in the Smart Grid network. Therefore, blockchain technology can be used to get selected nodes act like miners for energy efficient operations in distributed network.

3.1.1. Web-based attack

Most online transactions are done through web browsers, namely Google Chrome, Internet Explorer, Firefox, etc. The web-enabled transactions are done through computers, smart equipment, Mobile, Personal Digital Assistant (PDA), etc. Many scripting languages use a floating inline frame called iFrame of the browser to render the advertiser information on the screen. The information feed is sourced from a different server, which is innocuous, but if the source is malicious, it can act as a trojan or bot for the system (Mitchell et al., 2012). This trojan or bot may leak the system's critical information to the attacker without the user's knowledge creating a security risk.

Additionally, cookies are used for web session management on end devices. The attackers may gain cookie information and change it to hijack the ongoing session. Cross-site request forgery (CSRF) attacks are a type of web exploit where a website transmits unauthorized commands as a user that the web application trusts. In a CSRF attack, a user is tricked into submitting an unintended (often unrealized) web request to a website.

Though all the secure applications delivered over the web use security protocols of SSL/TSL, these SSL/TSL certificates can be stolen or leaked by attackers (Dehalwar et al., 2017b). The increased use of extensions in the browsers will also add risk to the system. These extensions, if not vetted by the security agencies, may increase the risk of attack (Dehalwar et al., 2017a). Open Web Application Security Project (OWASP) is an online community that monitors and advises users on web application security (OWASP, 2017). These threats can affect the stability of financial, medical, energy, and other infrastructure (Dehalwar et al., 2017b).

3.1.2. Extortion attacks

Hackers block some services and demand money to recover the service. WannaCry ransomware is one such type of extortion attack. The hacker demanded $300 from the user within 72 h to get back the system running.

3.1.3. Data manipulation attacks

Hackers send malicious code from the compromised system by manipulating the genuine message. The major web-based security attacks like SQL injections, Broken Authentication, Sensitive Data Exposure, Security Misconfiguration, Cross-Site Scripting (XSS), etc., are data manipulation attacks (Li et al., 2019). Load altering attack in Smart Grid is also a data manipulation attack.

3.1.4. Mobile/IoT device attacks

The vulnerability in mobile phones, appliances at the home, car, medical equipment, monitoring camera, etc., are exploited by attackers. They try to gain valuable privacy information from this type of device. Spyware named Pegasus from Israel company NSO Group is installed on mobile devices running iOS and Android. Security companies are bracing for more lethal attacks in the future.

3.1.5. Bot net attack

Viruses and worms have certain fixed behaviors. A bot, on the other hand, has a broader repertoire of behavior. A bot communicates, directly or indirectly, with a human administrator, commonly known as a botmaster or bot pastor.

Many of the sophisticated bots may engage with AI-based virtual personal assistants – such as Bixby, Alexa (Amazon), Siri (Apple), and Cortana (Microsoft) to send private information on the mobile (Mitchell et al., 2012) to hackers. These virtual agents can interact with website chatbots to find the perfect gift, airfare, loan, or any other number of valuable goods and services. If these virtual agents' security is compromised, they may leak valuable information voluntarily to the attackers.

The blockchain technology has noteworthy structures, using it appropriately for operation of distributed power network (i.e. smart grid) to overcome security challenges (Hasan et al., 2022). It is important to explore use of blockchain technology applications with cyber security sensitivity and energy data privacy and security within electrical energy network having IoT devices for cleaner energy technologies (Ammar et al., 2018).

3.2. Challenges in distributed environment

Distributed ledger technology for energy management will be the outcome of merging of IoT for intelligent management of components and cleaner energy technologies using cloud solutions. Distributed ledger, including blockchain and Directed Acyclic Graph are used in transforming the next generation innovation and information dissemination for sustainable electrical energy technologies. Though it is going to be one of the promising technologies, however it has following challenges: -

(i) As there are no approved standards in Device identification and authentication, there will be a problem of interoperability and scalability. All the development is now in the preliminary stage and some more time is needed for the technology to mature.
(ii) Due to heavy duty transaction of authentication, consensus and smart contract the high-end system with high energy need will be used. It may take a long time for a new block to be added to the core block. The storage capacity will also increase due to redundancy of distributed ledger and increased block generation.
(iii) In an open blockchain, there will be the issue of privacy. Everyone will be able to know the pseudo-identity of the user/devices, thus compromising the anonymity in the transparent environment.
(iv) Distributed blockchain may be subjected to DDoS. A botnet may overwhelm the blockchain ledger with irrelevant request, thereby delaying the process of authentication.

A cyber secure energy management within distributed electrical energy network can be achieved through blockchain technology (Kim et al., 2019). In blockchain technology, data handling is distributed through participants. Blockchain technology application within distributed energy network may overcome above mentioned security challenges for cyber-secure management of energy information. It is going to contribute in intelligent operation of distributed energy network for integrating cleaner energy technologies and energy efficiency.

4. Blockchain-based identification

The activities related to smart grid energy data are to search, retrieve, store, capture, transfer, and analyze for energy efficient operation. The energy data in smart grid (collected through SCADA) is time-serialized and gathered through streaming from various sources (e.g., substation automation, AMI, load controllers, clean energy sources,

etc.). Data manipulation and password breaches are common in the system, which can be minimized by using proper authentication techniques. Many organizations like Google, Microsoft, etc., have encouraged the user to avail of two-factor authentications for verification. Two-factor authentications improve the authentication processes. More improvement can be achieved by integrating biometrics information for authentication. But biometrics has one drawback; if biometrics information is compromised, it cannot be replaced. So, biometrics are only used for second-factor authentication.

In smart distributed electrical energy network, authentication of nodes can be improved through digital certificates and the Certification Authority (CA) has a log of all certificates. HTTP public-key pinning contains an HTTP header that lets a site declare CAs that can sign its certificates associated with an energy node. This is called trust on first use. On subsequent HTTPS requests, browsers will accept only the earlier verified certificates and reject certificates issued by other CAs. Again, the problem is that many certificates are issued, so searching for the right certificate is time-consuming. Certificate exchange is also an issue that needs careful analysis especially in energy information distributed network.

In distributed electrical energy network, vulnerabilities can be eliminated by developing a trust management system using self-sovereign identity using Blockchain technology. A blockchain block consists of block id, timestamp, previous block hash, digital signature, etc., which uniquely distinguish it from the other blocks in a Blockchain (Liu et al., 2020). The Blockchain structure depends on the requirements of the system and the type of ownership of the Blockchain (Zhang et al., 2019). Miners mined the block based on the consensus algorithms, such as proof of work and proof of stake. Miner mined the block, which can be added to the Blockchain once it gets verified by the members. Once the block is added into the Blockchain no alteration, deletion or updation is allowed. The distributed nature of the Blockchain makes it more transparent, as the records are visible online on the distributed platform in the network and frequent updation of the Blockchain.

There are two types of Blockchain, private and public. Private blockchain is further classified as permissioned and permissionless (Dai et al., 2020). Public permissionless Blockchain allows anyone to join the Blockchain without the authorization of the third party. The owner of the private permissioned Blockchain restricts the access of the Blockchain to the authorized user.

4.1. Identification model

The identification of the devices differs from the human being. Human being is having multiple identity such as passport, social security number, driving license, etc., but the device is having only one identity which is given by the manufacturer. We proposed permissioned blockchain for the self-sovereign device identification and management based on distributed ledger. Initially, there will be three categories of block, namely whitelist, blacklist, or grey list based on the past performance and trust index. The trustworthy miners will be from the whitelist as they will have the maximum trust index and highest access permission. When more than 60% of the whitelisted blocks reach the consensus, the block will be added into the core blockchain. A sample block structure is shown in Fig. 5.

The device id must be standardized and unique like IP addresses and with IMEI number that identifies the device distinctively in the network. Most of the time, the identifiers of devices use printed numbers, bar codes, QR codes, or Radio Frequency Identification (RFID). There are activities going on to develop the standards for identifiers in IoT by European body of Alliance for Internet of Things Innovation and IEEE (AIOTI, 2018). Our presumptions are that the device identifier must be designed in such a way that it includes the manufacturer-id, country of origin, batch number, validity, etc. in the similar pattern of VIN number of vehicle. The block also contains the geolocation information, which is essential to prevent tampering of the device or misplacing the device for

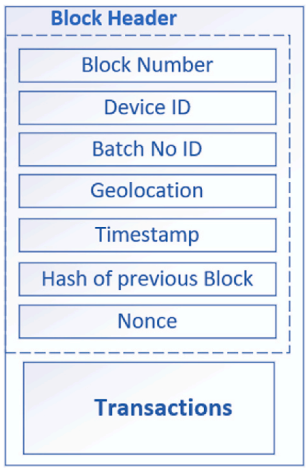

Fig. 5. Single block of the Blockchain.

espionage. Once this information is securely fed in the block, the block is ready for appending in the core of the blockchain if the miners authenticate the block.

4.2. Registration of a new block

As the core blockchain is a permissioned blockchain, which implies there is central authority for a blockchain. The central authority will delegate power to administer the new block in a distributed manner using distributed ledger technology. Registration and retrieval of information from the blockchain is depicted in Fig. 6. The new device identifier will request the registration authority to register the new block by supplying its credentials. On satisfactory verification of the credentials, a new block is generated in the blockchain, and the approval is communicated to the new block. The device identifier such as smart meter will start sending the required data to the block and all the transactions are recorded in the assigned block. The service provider desiring information from the device will first check the authenticity of the device from the registration authority and on satisfactory confirmation of identity, the retrieval of information is initiated. The service provider can check the authenticity of the transaction by checking the hash key.

5. Implementation in smart grid

In this work, a Merkle tree architecture is suggested for Blockchain implementation in distributed electrical energy network (i.e. smart grid), which is depicted in Fig. 7 (Narayanan et al., 2016). The root node connects to Wide Area Measurement System (WAMS) and Control center like hash functions of left and right subtree. WAMS and the control center node are further connected to substations 1 and 2. This iterates until it reaches the leaf node, which is a Smart Meter of AMI in the Home Area Network (HAN). The data aggregation can also follow the same path as depicted in Fig. 7.

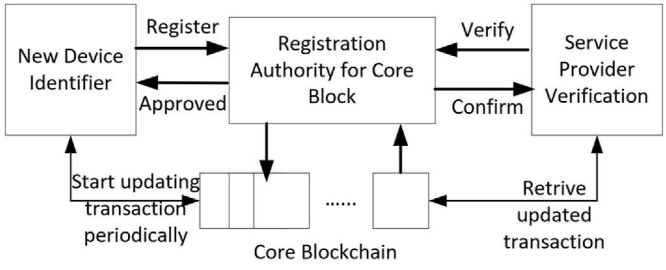

Fig. 6. Adding, updating and retrieval of information.

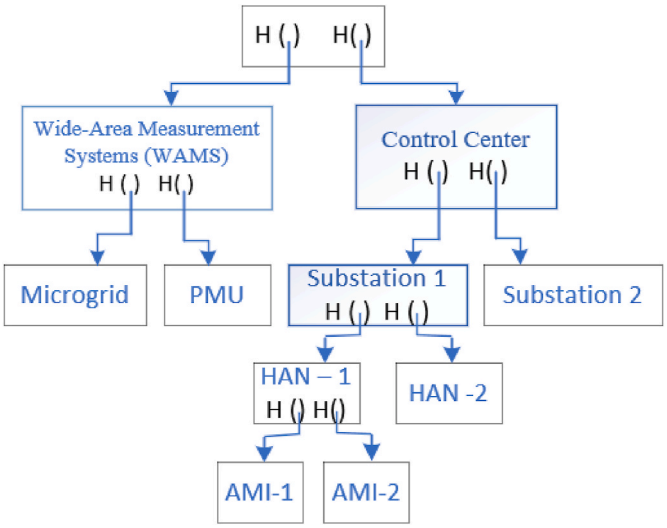

Fig. 7. Merkle tree architecture of blockchain (Narayanan et al., 2016).

The validity of energy at nodes and transactions can be easily verified by traversing the path of a Merkel tree. The tree traversal can take log(n) time to verify the transaction and the node and SHA 256 can be used for hashing. In this work, it is proposed to have an append-only mode for adding a new device using smart contract and consensus. The new device verification and authentication is done by the miners. These miners are rewarded for their efforts through incentives. When the block is authenticated by miners who are more than 60%, then it is successfully added to the core Blockchain (Nakamoto, 2009). When the new block is added, its notification is sent to all the members to update and synchronize the copy of the ledger. Thus, all members will have the latest copy of the node in distributed ledger. Once the device is added to the Blockchain, it can start communicating with the control center. The service provider can check the integrity of the data and the credentials of the block any time by verifying the hash key. Thus, integrity and authenticity of devices and data are ensured. The blockchain-based device-centric approach will significantly enhance the smart grid cyber secure operations. Hyperledger from Linux Foundation is used to create private blockchain architecture. Hyperledger Composer contains many APIs to support building Blockchain (Baset et al., 2019). The class diagram is depicted in Fig. 8 illustrates the fields used for developing the Blockchain.

The Blockchain system is developed in three stages. (i) In the first stage, a user interface is developed to add a new device; (ii) in the second stage, Hyperledger based Blockchain is developed; and (iii) in the third stage, the new device is added, and the authenticity is tested using a voting mechanism. Blockchain follows Byzantine fault tolerance characteristics for a distributed system (Kolb et al., 2020). Synthetic data and a pseudo-random nonce are used to test the model with complexity from 0 to 10. The model performed as per the specifications and requirements. The mining and updating in the Blockchain is also tested and authenticated using consensus protocol. The model work fine in a networked environment synchronized the transaction with other nodes with some communication delay. The model also rewarded a certain tangible amount for mining activity. The model was able to authenticate the device using Blockchain in a trusted model. The system work according to plan when some nodes are down but with reduced performance of mining. Validation of the node is performed in log(n) time that justifies our result.

6. Conclusion

Blockchain based technologies are going to revolutionise electricity energy operations and market mechanism. It is going be used for allocating net energy requirements at a specific node via establishing hierarchical priorities (e.g. prioritization of renewable energy, maximization of local energy resources, etc.). In this work, blockchain-based self-sovereign identification and authentication technique has been presented to prevent the identity theft and masquerading in distributed electrical energy network. This paper discusses a model of identification and authentication of IoT devices based on Blockchain technology using a Merkle tree architecture. Also, implementation of identification and authentication is discussed with a focus on identity based security.

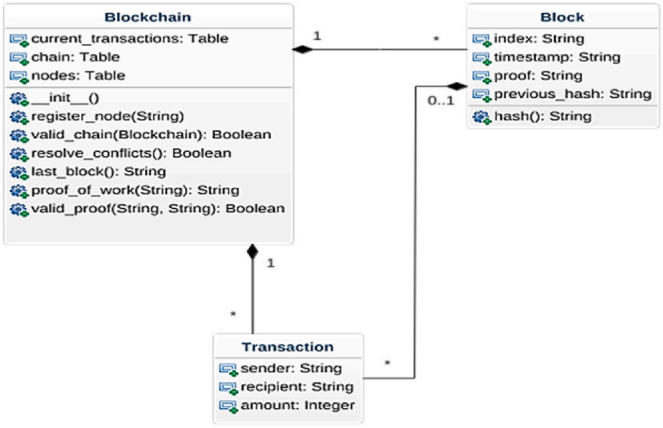

Fig. 8. Class diagram of blockchain.

The blockchain technology has noteworthy structures for using it appropriately in operation of distributed intelligent power network considering cyber security challenges. It is important to explore use of blockchain technology applications with cyber security sensitivity, and for energy efficient operation of electrical energy network integrated with IoT devices for cleaner energy technologies management.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

AIOTI, 2018. Alliance for internet of things innovation. Identifiers in Internet of Things (IoT). https://euagenda.eu/upload/publications/identifiers-in-internet-of-things-iot.pdf (assessed on 06 March 2022).

Ammar, M., Russello, G., Crispo, B., 2018. Internet of Things: a survey on the security of IoT frameworks. J. Inf. Secur. Appl. 38, 8–27. https://doi.org/10.1016/j.jisa.2017.11.002.

Amrani, H.L., Berroukech, B.E., Idrissi, Y.E.B.E., Ajhoun, R., 2016. Identity management systems: Laws of identity for models evaluation. In: 4th IEEE International Colloquium on Information Science and Technology. https://doi.org/10.1109/CIST.2016.7804984.

Bartolomeu, P.C., Vieira, E., Hosseini, S.M., Ferreira, J., 2019. Self-sovereign identity: use-cases, technologies, and challenges for industrial IoT. In: 24th IEEE International Conference on Emerging Technologies and Factory Automation. https://doi.org/10.1109/ETFA.2019.8869262.

Baset, S.A., Desrosiers, L., Gaur, N., Novotny, P., O'Dowd, A., Ramakrishna, V., Sun, W., Wu, X., 2019. Blockchain Development with Hyperledger: Build Decentralized Applications with Hyperledger Fabric and Composer. Packt Publishing, Limited, ISBN 978-1838649982.

Bouras, M.A., Lu, Q., Zhang, F., Wan, Y., Zhang, T., Ning, H., 2020. Distributed ledger technology for ehealth identity privacy: state of the art and future perspective. Sensors 20, 1–20. https://doi.org/10.3390/s20020483, 483.

Budka, K.C., Deshpande, J.G., Thottan, M., 2014. Communication Networks for Smart Grids, ISBN 978-1-4471-7213-0. https://doi.org/10.1007/978-1-4471-6302-2.

Dai, Q., Xu, K., Dai, L., Guo, S., 2020. Dizar: an Architecture of Distributed Public Key Infrastructure Based on Permissoned Blockchain. Blockchain Technology and Application. https://doi.org/10.1007/978-981-15-3278-8_11.

Dehalwar, V., Kalam, A., Kolhe, M.L., Zayegh, A., 2016. Review of machine to machine communication in smart grid. In: International Conference on Power and Renewable Energy. https://doi.org/10.1109/ICSGCE.2016.7876040.

Dehalwar, V., Kalam, A., Kolhe, M.L., Zayegh, A., 2017a. Review of detection, assessment and mitigation of security risk in smart grid. In: International Conference on Power and Renewable Energy.. https://doi.org/10.1109/ICPRE.2017.8390698.

Dehalwar, V., Kalam, A., Kolhe, M.L., Zayegh, A., 2017b. Review of web-based information security threats in smart grid. In: 7th International Conference on Power Systems. https://doi.org/10.1109/ICPES.2017.8387407.

Dehalwar, V., Kalam, A., Kolhe, M.L., Zayegh, A., 2017c. Electricity demand management by optimising the use of HVAC and HWS through AMI. Australasian Universities Power Engineering Conference. https://doi.org/10.1109/AUPEC.2017.8282383.

Denning, D.E.R., 1982. Cryptography and Data Security. Addison-Wesley, ISBN 978-0-201-10150-8.

Gruner, A., Muhle, A., Meinel, C., 2019. An integration architecture to enable service providers for self-sovereign identity. IEEE 18th Int. Symp. Netw. Comput. Appl. 1–5. https://doi.org/10.1109/NCA.2019.8935015.

Hasan, M.K., Alkhalifah, A., Islam, S., Babiker, N.B.M., Habib, A.K.M.A., Aman, A.H.M., Hossain, M.A., 2022. Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations. Wireless Commun. Mobile Comput. 2022, 1–26. https://doi.org/10.1155/2022/9065768, 9065768.

Houtan, B., Hafid, A.S., Makrakis, D., 2020. A survey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access 8, 90478–90494. https://doi.org/10.1109/ACCESS.2020.2994090.

Iberdrola, 2022. How can blockchain be used to certify the source of green energy? https://www.iberdrola.com/innovation/blockchain-energy.

IEA Agency, 2019. Energy efficiency 2019. https://www.iea.org/reports/energy-efficiency-2019.

Kassem, J.A., Sayeed, S., Marco-Gisbert, H., Pervez, Z., Dahal, K., 2019. DNS-IdM: a blockchain identity management system to secure personal data sharing in a network. Appl. Sci. 9 (15), 1–19. https://doi.org/10.3390/app9152953, 2953.

Kim, S.M., Lee, T., Kim, S., Park, L.W., Park, S., 2019. Security issues on smart grid and blockchain-based secure smart energy management system. In: 7th International Conference on Power Science and Engineering. https://doi.org/10.1051/matecconf/201926001001.

Kolb, J., Abdelbaky, M., Katz, R.H., Culler, D.E., 2020. Core concepts, challenges, and future directions in blockchain: a centralized tutorial. ACM Comput. Surv. 53 (1), 1–39. https://doi.org/10.1145/3366370, 9.

Kolhe, M., 2012. Smart grid: charting a new energy future: research, development and demonstration. Electr. J. 25 (2), 88–93. https://doi.org/10.1016/j.tej.2012.01.018.

Kolhe, M., 2015. Algorithms for Demand Response and Load Control, D5.1, Scalable Energy Management Infrastructure for Aggregation of Households, European Commission FP7 Program (Project - FP7-ICT-2013-11-619560).

Kuperberg, M., 2019. Blockchain-based identity management: a survey from the enterprise and ecosystem perspective. IEEE Trans. Eng. Manag. 67 (4), 1008–1027. https://doi.org/10.1109/TEM.2019.2926471.

Le, T.N., Chin, W.L., Chen, H.H., 2017. Standardization and Security for Smart Grid Communications Based on Cognitive Radio Technologies - A Comprehensive Survey. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2016.2613892.

Li, K.C., Chen, X., Susilo, W., 2019. Advances in cyber security: principles, techniques, and applications. https://doi.org/10.1007/978-981-13-1483-4, 978-981-13-1483-4.

Liu, H., Zhang, P., Pu, G., Yang, T., Maharjan, S., Zhang, Y., 2020. Blockchain empowered cooperative authentication with data traceability in vehicular edge computing. IEEE Trans. Veh. Technol. 69 (4), 4221–4232. https://doi.org/10.1109/TVT.2020.2969722.

Maesa, D.D.F., Mori, P., 2020. Blockchain 3.0 applications survey. J. Parallel Distr. Comput. 138, 99–114. https://doi.org/10.1016/j.jpdc.2019.12.019.

McLaughlin, K., Friedberg, I., Kang, B.J., Maynard, P., Sezer, S., McWilliams, G., 2015. Chapter 5 - Secure Communications in Smart Grid: Networking and Protocols, Smart Grid Security - Innovative Solutions for a Modernized Grid. Elsevier, pp. 113–148. https://doi.org/10.1016/B978-0-12-802122-4.00005-5.

Mitchell, J.C., Sharma, R., Stefan, D., Zimmerman, J., 2012. Information-flow control for programming on encrypted data. 25th Comput. Security Found. Symp. 45–60. https://doi.org/10.1109/CSF.2012.30.

Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C., 2018. A survey on essential components of a self-sovereign identity. Computer Science Review 30, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002.

Nakamoto, S., 2009. Bitcoin: a peer-to-peer electronic cash system. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S., 2016. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, ISBN 9780691171692.

Nuss, M., Puchta, A., Kunz, M., 2018. Towards blockchain-based identity and access management for internet of things in enterprises. Lect. Notes Comput. Sci. 11033, 167–181. https://doi.org/10.1007/978-3-319-98385-1_12.

OWASP - The Open Web Application Security Project, 2017. OWASP Top 10 2017: the Ten Most Critical Web Application Security Risks. https://www.owasp.org/images/b/b0/OWASP_Top_10_2017_RC2_Final.pdf.

O'Reilly, P., Rigopoulos, K., Feldman, L., Witte, G., 2021. Cybersecurity and Privacy Annual Report. https://doi.org/10.6028/NIST.SP.800-214.

Powerledger, 2022. Manage grid stability and flexibility services. https://www.powerledger.io/solutions/need/grid-stability.

Refaat, S.S., Ellabban, O., Bayhan, S., Abu-Rub, H., Blaabjerg, F., Begovic, M.M., 2021. Smart Grid and Enabling Technologies. Wiley-IEEE Press, ISBN 978-1-119-42231-0.

Sockin, M., Xiong, W., 2020. A Model of Cryptocurrencies. National Bureau of Economic Research. https://doi.org/10.3386/w26816. Working Paper Series No. 26816.

Sousa, P.R., Resende, J.S., Martins, R., Antunes, L., 2020. The case for blockchain in IoT identity management. J. Enterprise Inf. Manag. https://doi.org/10.1108/JEIM-07-2018-0148.

Stoustrup, J., Annaswamy, A.M., Chakrabortty, A., Qu, Z., 2018. Smart grid control: overview and research opportunities. Springer. Power electronics and power systems. https://doi.org/10.1007/978-3-319-98310-3.

Ulltveit-Moe N. (2015). Specification of security and privacy handling, D8.1, Scalable Energy Management Infrastrucutre for Aggrgation of Households, European Commission FP7 Program (Project - FP7-ICT-2013-11-619560).

Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., Rong, C., 2019. A comprehensive survey of blockchain: from theory to IoT applications and beyond. IEEE Internet Things J. 6 (5), 8114–8154. https://doi.org/10.1109/JIOT.2019.2922538.

Zhang, P., Liu, H., Zhang, Y., 2019. Blockchain enabled cooperative authentication with data traceability in vehicular edge computing. Comput. Commun. IoT Appl. 299–304. https://doi.org/10.1109/ComComAp46287.2019.9018754.