Blockchain-enabled device authentication and authorisation for Internet of Things

Singh, Raman; Sturley, Sean; Sharma, Bhisham; Dhaou, Imed Ben

Published in:
2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC)

DOI:
10.1109/ICAISC56366.2023.10084957

Published: 03/04/2023

Document Version
Peer reviewed version

Singh, R., Sturley, S., Sharma, B., & Dhaou, I. B. (2023). Blockchain-enabled device authentication and authorisation for Internet of Things. In *2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC)* IEEE. https://doi.org/10.1109/ICAISC56366.2023.10084957

Blockchain-enabled Device Authentication and Authorisation for Internet of Things

Raman Singh
School of Computing, Engineering and Physical Sciences
University of the West of Scotland
United Kingdom
raman.singh@uws.ac.uk

Sean Sturley
School of Computing, Engineering and Physical Sciences
University of the West of Scotland
United Kingdom
sean.sturley@uws.ac.uk

Bhisham Sharma
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India
bhisham.pec@gmail.com

Imed Ben Dhaou
School of Engineering, Computing and Informatics
Dar Al-Hekma University
Saudi Arabia
bendhaou.imed@gmail.com

***Abstract*—The Internet of Things (IoT) is the network of multiple devices known as "things" which includes sensors, security cameras, smart lights, smart TV, traffic lights etc. in the smart home or industrial environment. In many applications, these IoT devices are installed in open areas for example traffic lights/ security cameras in a smart city. Strong authentication and authorisation for these devices need to be deployed to ensure trust among IoT networks. IoT devices produce and forward security-sensitive data and hence confidentiality, authentication and proper authorisation should be the primary priority of an IoT system. Implementing Certificate Authority-based digital certificate solutions is costly because of the number of devices involved in IoT networks. Blockchain is a decentralized ledger-based technology which can help to provide seamless yet cost-effective solutions for confidentiality, authentication, and authorisation for IoT environments. A blockchain-based system for device registration, authentication, authorisation, and data confidentiality is proposed. The paper shows the methodological and procedural details of the proposed security scheme.**

***Index Terms*—Blockchain Technology, Internet of Things, Authentication, Confidentiality, Digital Certificate, Industry 4.0, Smart City**

I. Introduction

The Internet of Things (IoT) is paving its way in the Industrial and smart city environment and helping in facilitating enormous applications. In an industrial setup, various sensors, devices, robotic units etc. are interconnected and communicate with each other to complete a given task. This kind of industrial setup is known as the Industrial Internet of Things (IIoT). More and more industries are adopting the Industry 4.0 framework to optimize and revolutionize their manufacturing, distribution, innovation and customer satisfaction. Along with Industry 4.0, the concept of a technologically advanced urban area known as a smart city is also becoming popular. In smart city environment devices like sensors, cameras, lights, meters, microbots, terminals etc. are interconnected to collect and analyze data for various use cases like smart traffic management, smart waste management, smart lighting systems, smart parking, environmental monitoring, and efficient city transportation. The use of IoT in smart cities helps us to achieve various goals like enhanced efficiency, reduced crime, better environment, better services, reduced traffic congestion etc.

The immense benefits of IoT in Industry 4.0 and Smart City environment makes us excited but the research community still working to get cost-effective and efficient cyber security solutions. In this paper, emphasis is given to authentication and authorization aspects of cyber security for IoT devices in Industry 4.0 and Smart City environment. It is important to authenticate the identities of IoT devices before these devices are allowed to enter an IoT network. The proposed framework will help network administrators to identify each IoT device and avoid the accidental inclusion of hackers' devices. The proposed framework will also help in making sure that only authorised IoT devices are allowed to communicate and collect data in Industry 4.0 or Smart City. The proposed framework will also mitigate grey market products' inclusion in an IoT network.

The rest of the paper is organised as follows. Section II discusses IoT security and various security-related issues, especially in applications like Industry 4.0 and Smart City. Section III describes the proposed security framework for the authentication and authorisation of IoT devices. This section explains various components, aspects and procedures of the proposed framework. Section IV discusses the deployment challenges and implications of the proposed security framework. This section also talks about future research directions in the area. Finally, section V concludes the study.

II. Security in Internet of Things: Related Work

Authenticating IoT devices and device-to-device communication security are two major issues in IoT networks. Researchers from all over the world contributed to proposing

various methodologies to make IoT networks more secure. Authors in [1] proposed a device-to-device authentication mechanism for the Internet of vehicles using digital certificates issued by a trusted third party. The proposed technique provides quick authentication for fast-moving vehicles and safeguards against key compromise impersonation attacks in an IoT environment. In one research, the authors presented a blockchain-based device authentication and registration mechanism for a smart city environment. This decentralized authentication mechanism removes the requirement of a centralized Registration Center Authority (RAC) which is a single point of failure. This mechanism improves device authentication and provides secure device-to-device communication but device identification and secure handover from manufacturer to industry are still unresolved [2]. Researchers in [3] proposed a trust-based monitoring scheme for user-level and communication-level security using agent-based middleware. The trust signals are capable to provide message authentication along with spoof detection. A new authentication technique is proposed for the identification and authentication of IoT devices [4].

Digital certificates are used to identify and authenticate IoT devices by researchers in one research [5]. The researchers in this study used X.509 certificates for authentication and achieved more than 84% of accuracy. Static random-access memory-based Physical Unclonable Function (SRAM PUF) is a promising way of authenticating IoT devices. In one research [6], SRAM PUF is used to produce a unique fingerprint for each device which is then used for unique IDs to authenticate devices in an IoT network. The proposed ID matching scheme yielded promising results to mitigate attacks like impersonating or spoofing IoT devices. Authors in [7] used hardware serialisation methods to mitigate attacks like man-in-the-middle, masquerading, device cloning and replay in an IoT network. An integration of various techniques like Radio Frequency Fingerprinting, Authentication by Hardware Variation, Wireless Key Generation, and Secure Communication by Channel Randomness is proposed for better authentication and key generation in IoT networks [8]. RSA and hashing are also used by researchers to provide a secure framework for Industrial IoT (IIoT). Authors [9] proposed resource efficient authentication protocol for IIoT. Lightweight Cryptography (LWC) along with hashing is used to authenticate IIoT devices and secure communication to mitigate man-in-the-middle & replay attacks.

Integration of PUF and Public Key Infrastructure is advised by researcher [10] to provide lightweight digital certificates based authentication mechanism for IoT network. An edge-assisted authentication scheme is proposed in [11] for an information-centric networking-based cyber-physical system. In this authentication mechanism, a two-way authentication scheme using a session connection and proxy signature is presented for IIoT devices. In one research [12], authors proposed a device authentication scheme for smart home networks against attacks for example replay attacks, server spoofing and man-in-the-middle attack. In this proposed scheme, users need to be registered in the system and generate their private-public key pair. The authentication device, the controller and the user deploy a public key cryptosystem to authenticate IoT devices. A blockchain-based identity management scheme is presented by [13] for protecting IoT against fake nodes and identity theft. In this scheme, distributed tamper-proof ledger is maintained for IoT devices and a lightweight consensus-based device authentication scheme is utilized. Blockchain technology is used for authentication and authorisation of IoT devices using a multi-level layer approach in [14]. Blockchain is also widely used to propose authentication mechanisms in IoT environments other research like [15], [16] and [17]. Researchers in various studies like [18] discussed the need, features, applications and challenges in the IoT field and emphasised the need for secure authentication.

The approaches presented in this section are promising for local authentication but have not addressed the problem of secure transfer of IoT devices from manufacturers to distributors and further industrial customers. Also, approaches based on certificate authorities issued digital certificates or PKI etc., have not discussed one major factor i.e. cost. Large industries and smart city environments may have hundreds or even thousands of IoT devices and getting digital certificates for each device are extravagant. Our proposed security framework aims to solve two issues: a cost-effective authentication mechanism and an end-to-end secure supply chain of IoT devices.

III. The Proposed Security Framework

The proposed security framework utilizes the beauty of the decentralization nature of Blockchain technology. In the proposed framework, a community but permissioned Blockchain is established where each participating entity like manufacturers, distributors and industrial customers configures at-least one blockchain node in their premises. For this research, the smart city is also considered an industrial customer because the smart city authorities are expected to purchase IoT devices in large numbers just like industrial customers and operate on a similar scale. The idea of community Blockchain is to provide the same ledger to all manufacturers, distributors and industrial customers to verify, and identify each IoT device. Figure 1 shows the overall architecture of the proposed security framework. The first entity which is the manufacturer will manufacture IoT devices and create one digital certificate known as blockCert_m for each device. These blockCerts are stored on the corresponding Blockchain. In the next phase of the supply chain, the IoT devices are taken over by distributors. The distributors after receiving IoT devices will verify the identity using blockCert_m from Blockchain. After verification, issue a new blockCert known as blockCert_d and store them on their Blockchain node.

Once these IoT devices are purchased by industrial customers, identification, and authentication are carried out using blockCert_m & blockCert_d before their deployment to the IoT network. After successful authentication, the industrial customer has the option to create their own digital certificate known as blockCert_net and store them on the Blockchain

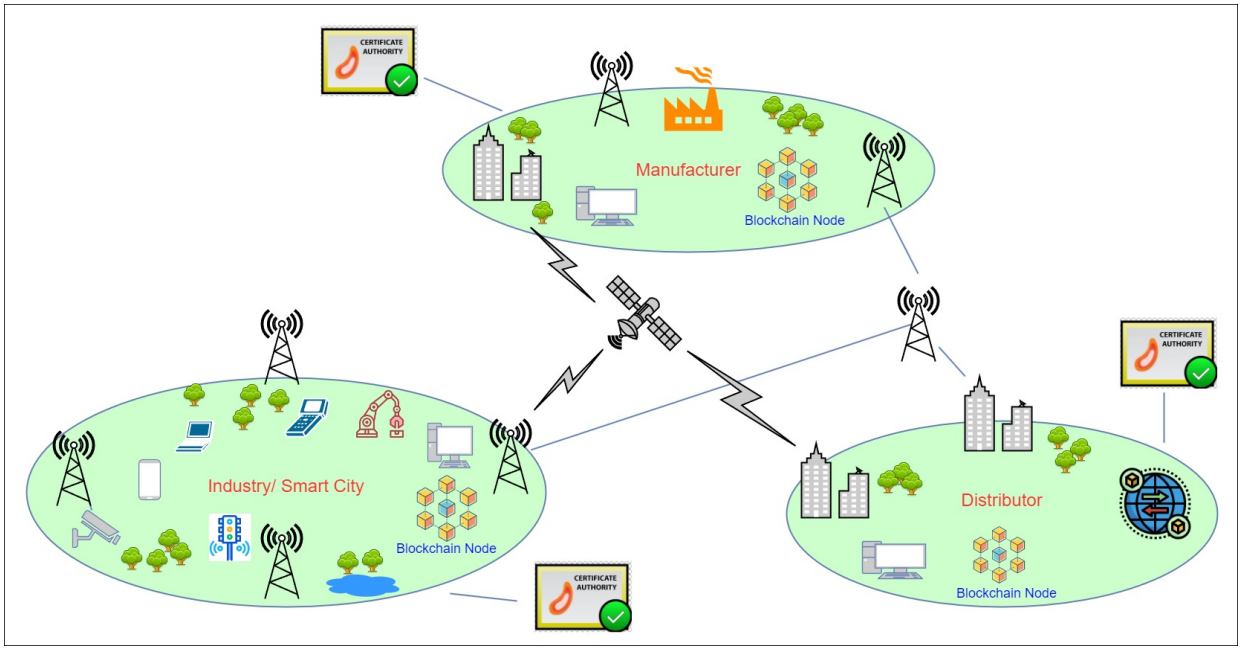

Fig. 1. The overall architecture of the proposed framework

node. Authorisation for each IoT device is carried out using this network block certificate i.e. blockCert_net. One Blockchain node is maintained by an industrial customer to carry out these identification, authentication and authorisation. To establish mutual trust between participating entities, each entity i.e. manufacturer, distributor and the industrial customer will have a digital certificate issued by a trusted third-party certificate authority (CA). The digital certificates issued by CAs are used to make sure that IoT devices are signed by manufacturers and distributors. The proposed framework limits third-party digital certificates to one for each entity and hence the annual cost of having CA-issued digital certificates for each IoT device is eliminated.

The first prerequisite for the proposed security framework is to have one digital certificate issued by a trusted third-party CA for each entity. Secondly, each participating entity will maintain one Blockchain node and will be part of the community Blockchain. The life cycle of an IoT device is as given in Figure 2. The life cycle is explained in four phases as given below.

A. Phase 1: Registration

The first phase starts at the manufacturer's premises where the manufacturing of IoT devices is practised. The manufacturer will create a digital certificate for each manufactured IoT device and save it on Blockchain. A Physical Unclonable Function (PUF) is used to create a unique identifier (known as ID_{puf} for an IoT device. This unique identifier along with other information like manufacturer name, manufacturing date, type of device, and MAC address is also stored in a Blockchain-based digital certificate. All this information is signed by a manufacturer using the private key of the manufacturer and has a public key verifiable by a third-party CA. This process is known as the registration of IoT devices with the manufacturer and is summed as given in equation 1.

$$\begin{aligned} &blockCert\_m = E_{skm}(ID_{puf}, manufacturer\_name, \\ &manufacturing\_date, type\_of\_device, MAC\_address) \\ &||\ Hash_{sh256}(ID_{puf}, manufacturer\_name, \\ &manufacturing\_date, type\_of\_device, MAC\_address) \end{aligned} \tag{1}$$

In equation 1, *blockCert_m* is a Blockchain-based digital certificate for each IoT device, *E* is the encryption process, *skm* is the third-party CA-based private key of the manufacturer, ID_{puf} is the unique PUF based identifier of an IoT device, *manufacturer_name* is the name of the manufacturer, *manufacturing_date* is the date on which that IoT device manufactured (it may be only month or year based on manufacturer's policy), *type_of_device* is additional information about the IoT device, *MAC_address* is MAC address assigned to that IoT device and $Hash_{sh256}$ is SHA256 hashing function used to create message authentication code or message digest. The *blockCert_m* is signed by the private key of the manufacturer to ensure that all the information about an IoT device is provided by the manufacturer itself and has not been altered by any attacker. Distributors and industrial customers can verify the source of information and identify the manufacturer of an IoT device by decrypting the *blockCert_m* information using the public key of the manufacturer. This public key of the manufacturer can be verified by a trusted third-party CA.

B. Phase 2: Endorsement

In the next phase of the supply chain, IoT devices are received by distributors from manufacturers. In this phase,

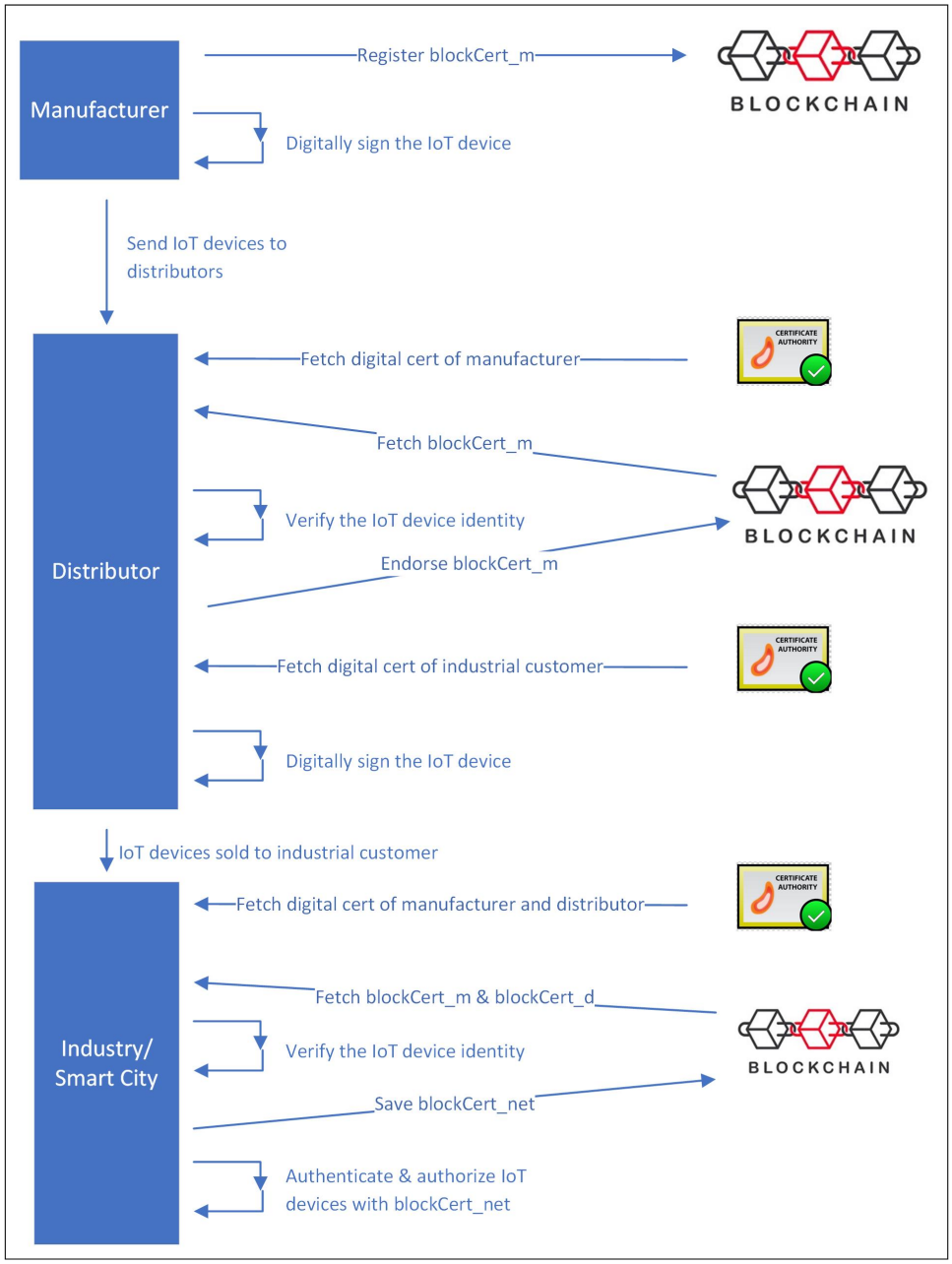

Fig. 2. The flow chart of the security life cycle for an IoT device

the authenticity of IoT devices is verified by distributors and the same is endorsed in the form of a Blockchain-based digital certificate known as *blockCert_d*. The distributor verifies the public key of the manufacturer with trusted third-party CA, fetches the *blockCert_m* from Blockchain and then decrypts it using the public key of the manufacturer. The information given on IoT devices and information yielded from decryption of *blockCert_m* is matched, if it is found same, the distributor can be sure that they receive original devices and not any counterfeited, spoofed or grey-market products. Once the source of origin of the IoT device is verified, the distributor uses information like ID_{puf}, MAC address, distributor ID, distributor name, endorsement date, customer name, and customer ID to generate a digital certificate *blockCert_d*. This certificate is signed with CA based private key of the distributor and encrypted using CA based public key of the customer. Once *blockCert_d* is generated, it is saved on Blockchain. The endorsement process is carried out by the distributor once the industrial customer makes a purchase order. The endorsement process is given in equation 2.

$$
\begin{aligned}
&blockCert\_d = E_{pkc}(E_{skd}(ID_{puf}, MAC\_address,\\
&distributor\_ID, distributor\_name, endorsement\_date,\\
&customer\_name, customer\_ID)\\
&||\ Hash_{sh256}(ID_{puf}, MAC\_address,\\
&distributor\_ID, distributor\_name, endorsement\_date,\\
&customer\_name, customer\_ID))
\end{aligned} \tag{2}
$$

In equation 2, *blockCert_d* is a Blockchain-based digital certificate for each IoT device endorsed by the distributor, *E* is the encryption process, *pkc* is CA-based public key of the customer, *skd* is CA-based private key of distributor, *distributor_ID* is a unique identification of distributor, *distributor_name* is the name of the distributor, *endorsement_date* is the date on which endorsement is made, *customer_name* is the name of a customer to which that IoT device is intended to sell, *customer_ID* is the unique identity of the customer. The Hash code of the endorsement information is also included in the *blockCert_d* certificate. Since the information is encrypted using the secret key of the distributor, it will help the customer to be sure that *blockCert_d* is issued by a genuine distributor. The information in the *blockCert_d* is encrypted using the public key of the industrial customer, which ensures that information given in this *blockCert_d* is accessed by the customer only. This process of endorsement is also shown in figure 2. Once the endorsement process is completed and *blockCert_d* is locked on Blockchain, the IoT device is ready to be shipped to the customer.

C. Phase 3: Identification, Authentication and Authorisation

Phase 3 starts when IoT devices are received by the industrial customer and they want them to deploy in an IoT network in an industrial or smart city environment. As shown in 2, *blockCert_m* and *blockCert_d* are fetched from Blockchain. CA-based public keys of manufacturers and distributors are fetched from corresponding trusted third-party CAs. These certificates are used to verify, identify and authenticate the originality of IoT devices. IoT device information is retrieved and this information is matched with the information decrypted from *blockCert_m* and *blockCert_d*. The process of retrieving information from the blockchain certificate is given in equation 3. In this way, industrial customers can verify the distributor and manufacturer of an IoT device and simply save themselves from counterfeited or spoofed devices. Blockchain-based identification and authentication of IoT devices will also help in promoting a robust & genuine supply chain cycle.

$$
Information_d = D_{pkd}(D_{skc}((blockCert\_d)) \tag{3}
$$

In equation 3, $Information_d$ is information retrieved from *blockCert_d* certificate, *D* is the decryption process, *skc* is the CA-based private key of the customer, and *pkd* is CA-based public key of the distributor. A similar process can be followed to retrieve information from *blockCert_m* using the public key of the manufacturer.

Once the originality of an IoT device is verified, industrial customers need to create a Blockchain-based network certificate which will be used in the authorisation of IoT devices on a network and secure communication with other devices. Information like ID_{puf}, MAC address, network id, company name, location id etc. can be used to create a certificate. A pair of a private key and a public key is also created for each IoT device. The private key of the IoT device is securely stored whereas the public key of the IoT device known as pk_{dev} is stored as part of the network certificate. The network certificate known as *blockCert_net* can be created as shown in equation 4.

$$
\begin{aligned}
&blockCert\_net = E_{skc}(pk_{dev}, ID_{puf}, MAC\_address,\\
&network\_id, company\_name, location\_id\\
&||\ Hash_{sh256}(ID_{puf}, MAC\_address,\\
&network\_id, company\_name, location\_id)
\end{aligned} \tag{4}
$$

In equation 4, *network_id* is the identity of a network in which a particular IoT device will be deployed, *company_name* is the name of the company where the IoT device will be deployed, and *location_id* is the location identity where particular IoT device will be geographically located in a network. Once *blockCert_net* is generated, this certificate will be stored on Blockchain. Now, this *blockCert_net* is used to authorise the role, privilege, function etc. of that particular IoT device in a given IoT network. Various parts/components of an IoT network have access to Blockchain nodes and can anytime verify any IoT device. The public key given in *blockCert_net* and the private key of IoT devices can be used in device-to-device secure communication.

As every IoT device will have its own network certificate, handling authentication and authorisation will be a lot easier for an industry or smart city. Also, all the network certificates are locked in Blockchain, So, annual renewal cost from third-party CA is not required. The overall cost of the framework will be in maintaining one Blockchain node only.

D. Phase 4: Replacement and Revocation

The Blockchain enabled *blockCert_dev* supports replacement and revocation procedures for IoT devices. At any level, if network administration of an industry/smart city requires to replace private-public key pair for an IoT device, it can be easily done by re-authenticating the device and a new *blockCert_dev* is issued to that device. Since a newer version of *blockCert_dev* with the same ID_{puf} is stored on Blockchain, and in Blockchain, searches are done in the latest-to-older fashion, the network system will always find the latest *blockCert_dev* and hence will always fetch up-to-date information. The proposed framework allows virtually unlimited times of network certificate replacement without putting the extra burden of cost.

There is no requirement of maintaining a Certificate Revocation List (CRL) in the proposed framework. Adding a replacement network certificate for an IoT device will automatically invalidate the older certificate. If the network

administrator wants to discard an IoT device or a device is retired, a new network certificate with invalid information is added to Blockchain. Whenever any device fetches that network certificate, it will not be able to communicate with discarded/retired devices because it will fetch a certificate with invalid information and will not get the true public key of the device.

IV. Deployment, Implications and Future Directions

The deployment of the proposed framework will require understanding between manufacturers, distributors and industrial customers. Every entity will require to maintain one Blockchain node and the Blockchain will act as a decentralized ledger of IoT devices. In the proposed framework, the manufacturer registers IoT devices using their private keys, so that any distributor can receive those devices, and endorse them individually with their private key and customers' public key. But if the manufacturer and distributor decide to keep the device information secure, the manufacturer can register the device with their private key and the distributor's public key to ensure that only a particular distributor read that information. The endorsement of an IoT device by a distributor is always securely done and will only be verified by the intended industrial customer.

The Blockchain-based proposed framework is expected to make a positive impact on the security of IoT networks. The only implication we need to address is the scalability of the system because of the increasing chain size of the Blockchain. Once, the Blockchain is deployed and huge numbers of network certificates are added, it will be interesting to see how much retrieval time is tolerated in real-time communication. More research is required to solve the scalability issue of the proposed framework and innovative solutions can be presented to address the problem.

V. Conclusion

Identification, authentication and authorisation of a device in an Internet of Things (IoT) network are crucial for its overall security. Industry 4.0 and Smart Cities are now becoming huge customers of IoT devices and hence need efficient yet cost-effective security mechanisms. The present security mechanism like third-party Certificate Authority (CA) issued certificates for each device is not sustainable because of the huge annual cost associated with digital certificates. A Blockchain-based framework is proposed for securing the complete supply chain life cycle of IoT devices which can ensure the security of identification, authentication and authorisation procedures of IoT devices. In the proposed framework, a distributor can easily identify and authenticate the source/ manufacturer of an IoT device and then can endorse the authentication for their customers. An industrial customer can also authenticate the manufacturer and distributor of an IoT device and can also issue a network certificate to authorise the IoT device to become part of their IoT network. In future, we will simulate the proposed framework to understand the deployment implications in detail and will also research to address the scalability issue of the proposed framework.

References

[1] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al-Barakati, and T. Shon, "An anonymous device to device authentication protocol using ecc and self certified public keys usable in internet of things based autonomous devices," *Electronics*, vol. 9, no. 3, p. 520, 2020.

[2] M. Vivekanandan *et al.*, "Bidapsca5g: Blockchain based internet of things (iot) device to device authentication protocol for smart city applications using 5g technology," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 403–419, 2021.

[3] F. Alqahtani, Z. Al-Makhadmeh, A. Tolba, and O. Said, "Tbm: A trust-based monitoring security scheme to improve the service authentication in the internet of things communications," *Computer Communications*, vol. 150, pp. 216–225, 2020.

[4] M. Azrour, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, "New enhanced authentication protocol for internet of things," *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 1–9, 2021.

[5] S. Karthikeyan, R. Patan, and B. Balamurugan, "Enhancement of security in the internet of things (iot) by using x. 509 authentication mechanism," in *Recent Trends in Communication, Computing, and Electronics*, pp. 217–225, Springer, 2019.

[6] U. Guin, A. Singh, M. Alam, J. Canedo, and A. Skjellum, "A secure low-cost edge device authentication scheme for the internet of things," in *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*, pp. 85–90, IEEE, 2018.

[7] A. Hasan and K. Qureshi, "Internet of things device authentication scheme using hardware serialization," in *2018 International conference on applied and engineering mathematics (ICAEM)*, pp. 109–114, IEEE, 2018.

[8] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the internet of things: Authentication and key generation," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 92–98, 2019.

[9] M. Tanveer, A. Alkhayyat, N. Kumar, A. G. Alharbi, *et al.*, "Reap-iiot: Resource-efficient authentication protocol for the industrial internet of things," *IEEE Internet of Things Journal*, 2022.

[10] Z. Siddiqui, J. Gao, and M. K. Khan, "An improved lightweight puf-pki digital certificate authentication scheme for the internet of things," *IEEE Internet of Things Journal*, 2022.

[11] Y. Lu, D. Wang, M. S. Obaidat, and P. Vijayakumar, "Edge-assisted intelligent device authentication in cyber-physical systems," *IEEE Internet of Things Journal*, 2022.

[12] V. Kumar, N. Malik, J. Singla, N. Jhanjhi, F. Amsaad, and A. Razaque, "Light weight authentication scheme for smart home iot devices," *Cryptography*, vol. 6, no. 3, p. 37, 2022.

[13] M. Mukhandi, F. Damião, J. Granjal, and J. P. Vilela, "Blockchain-based device identity management with consensus authentication for iot devices," in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 433–436, IEEE, 2022.

[14] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for internet of things," *Sensors*, vol. 21, no. 3, p. 772, 2021.

[15] X. Yang, X. Yang, X. Yi, I. Khalil, X. Zhou, D. He, X. Huang, and S. Nepal, "Blockchain-based secure and lightweight authentication for internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3321–3332, 2021.

[16] M. Rani, K. Guleria, and S. N. Panda, "Blockchain technology novel prospective for cloud security," in *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, pp. 1–6, IEEE, 2022.

[17] E. S. Babu, A. K. Dadi, K. K. Singh, S. R. Nayak, A. K. Bhoi, and A. Singh, "A distributed identity-based authentication scheme for internet of things devices using permissioned blockchain system," *Expert Systems*, p. e12941, 2022.

[18] I. Seth, S. N. Panda, and K. Guleria, "The essence of smart computing: Internet of things, architecture, protocols, and challenges," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, pp. 1–6, IEEE, 2021.