This project has received funding from the European's Union Horizon 2020 research innovation programme under Grant Agreement No. 957258

Architecture for Scalable, Self-*, human-centric, Intelligent, Secure, and Tactile next generation IoT

ASSIST-IoT Technical Report #14

Decentralising Access Control for IoT environment

Charalampos Savvaidis, Christos Patsonakis, Georgios Stavropoulos, Anastasia Kassiani Blitsi, Iordanis Papoutsoglou, Konstantinos Votis, Dimitrios Tzovaras

Submitted to the IEEE 8th World Forum on Internet of Things

Decentralising Access Control for IoT environment

Charalampos Savvaidis
Information Technologies Institute
CERTH
Thessaloniki, Greece
chsavvaidis@iti.gr

Christos Patsonakis
Information Technologies Institute
Centre of Research and Technology Hellas (CERTH)
Thessaloniki, Greece
cpatsonakis@iti.gr

Georgios Stavropoulos
Information Technologies Institute
CERTH
Thessaloniki, Greece
stavrop@iti.gr

Anastasia Kassiani Blitsi
Information Technologies Institute
CERTH
Thessaloniki, Greece
akblitsi@iti.gr

Iordanis Papoutsoglou
Information Technologies Institute
CERTH
Thessaloniki, Greece
ipapoutsoglou@iti.gr

Konstantinos Votis
Information Technologies Institute
CERTH
Thessaloniki, Greece
kvotis@iti.gr

Dimitrios Tzovaras
Information Technologies Institute
CERTH
Thessaloniki, Greece
dimitrios.tzovaras@iti.gr

***Abstract*—IoT has a profound impact on businesses and individuals as its adoption grows. Security and scalability are key subjects for enabling the technology's adoption. Cyber attacks increase each year, and the addition of emerging technologies such as Machine Learning can introduce vulnerabilities with additional complexity. Access control can mitigate security threats with proper rights management. XACML is an appropriate way to enforce complex policies in heterogeneous environments such as IoT since it is a flexible standard allowing scalability. Furthermore, the blockchain's advantages like data immutability and availability can aid in building a trustworthy access control system for IoT. Blockchain can support a decentralised architecture for policy evaluation and avoid single points of failure for the policy evaluation, which results in enhancing the security of the IoT network. Smart contracts accommodate the evaluation of access control policies for delivering a decentralised and tamper-proof system with consistent outcomes. For this reason, this paper proposes a decentralised access control approach following the XACML standard and enabling the access control decision evaluation using smart contracts. The implementation's impact on a complex real-world environment is described. The reference implementation is extensible to a great degree as it has flexibility in including services on top of the blockchain, such as an audit mechanism on the access decisions.**

***Index Terms*—IoT, XACML, blockchain, consortium blockchain, smart contract**

I. Introduction

Industry 4.0's aim is to rearrange daily routines in all aspects drastically. This new era brings novel technologies and synergies between these technologies. The Internet of Things (IoT) impacts a range of activities, and lately, blockchain has gained popularity in various fields like the utility sector with an abundance of devices. IoT devices cover a wide surface of enterprises and use communication channels. As IoT becomes integral for businesses, it is paramount to upkeep security at all levels. Access control is a fundamental concept in security. Access control is a technique to permit legitime users to their appointed actions or activities (Sandhu and Samarati, 1994). The delegation module expands access control capabilities, where delegation is a procedure for giving a user temporary permissions (Wang et al., 2008). A delegator, for instance, might act as someone transferring their permissions. The delegatee is the individual who is granted these permissions. A user delegates permissions in response to a query or an event. In event-based permission delegation, a specified user receives permissions in response to an event. The user asks permission on a resource from the owner via query-based permission delegation. Similarly, IoT devices issue a query when attempting to access a protected resource. In response to a query, the system/administrator grants the requester access to the resource. It is worth noting that under the systems described above, validating individuals' access rights is typically carried out by a centralised entity that intervenes in every request to enforce the authorisation decision. This ultimately leads to performance issues, namely single points of failure and absolute trust in this entity. Blockchain can aid in shifting from centralised approaches to decentralised ones. As the different blockchain generations indicate the ongoing improvements of the technology, the introduction of smart contracts has provided the opportunity for deploying decentralised applications. Smart contracts' ability to execute programs has piqued the academics' interest in combining blockchain with IoT. As a result, the aim of this paper is to use smart contract-enabled blockchain technology to create distributed and trustworthy access control for IoT. This paper aims to contribute by presenting an application with an extendable architecture for a decentralised access control system. The application of the architecture constructs a consortium blockchain network with smart contracts for handling access control based on attributes. Furthermore, the application is extendable as the blockchain can be considered as a layer for deploying applications such as audit mechanisms. The benefits of the application relate to the real-world scenario of a construction site. his paper is structured as follows: initially, an overview of the technological background is provided, focusing on the used technologies, such as blockchain and security policies. Afterwards, it displays the related work in the permission management scope and concentrates on blockchain approaches for access control. The final section describes the proposed solution's use cases, summarising the contributions and pointing out further developments.

II. Background

This section introduces three important technologies, including blockchain, smart contracts and XACML, to pave the way for the proposed architecture.

A. Blockchain

Blockchain is commonly parallelised with a distributed database accessible to everyone and runs on millions of devices, allowing anything of value to be moved, stored, and managed securely and secretly with cryptography implementation. It provides a decentralised public digital transaction record that securely tracks ownership in a trustless setting. The information stored on the blockchain is guaranteed to be correct since it is almost impossible to alter due to the replication of the ledger to the peer nodes, which upkeeps the blockchain's state with the execution of consensus algorithms. As blockchain does not rely on a single point of storage, data is made even more secure, diminishing the risk of being lost or destroyed. Blockchain is a technology for building trustless environments, as unlimited access to the data is not bestowed on a single authority, and the possibility of misuse is minimised. Therefore, the decentralised nature of blockchain technology also returns ownership of private and personal data to the individual user. The idea of blockchain originated from the whitepaper by Satoshi Nakamoto in 2008 [7], after which the technology has matured with projects creating cryptocurrencies and deploying smart contracts. The blockchain is built on asymmetric cryptography, peer-to-peer network, and blockchain protocols, and it has the following characteristics:

- Distributed computing, the consensus protocol's deployment abolishes central authorities for confirming the addition of new transactions.
- A shared ledger records every transaction. Each node keeps a copy of the ledger, while replication keeps copies of other peers updated.
- Transparency, as all transactions are accessible to all peers.
- Transactions are processed simultaneously by all blockchain peers. Even if certain peers cease to function, the network may still execute transactions.
- The blocks included in the blockchain cannot be copied, deleted or updated.

The blockchain consists of a chain of blocks with the first called genesis block. Every block beside the genesis has a hash of the preceding block. The chain grows by adding new blocks and acts as a ledger of transactions. Cryptography is used to add and link blocks to the chain. The addition of extra blocks is done with network authorization, and the new blocks, along with the encryption, contain a timestamp. The chain's integrity is therefore guaranteed from the first to the last block. The network uses a consensus algorithm to add blocks to the chain, as distributed systems run the risk of Byzantine fault where the information transmission may be imperfect. The consensus algorithm is described as the method through which the majority of network nodes agree on the state of the ledger. In general, there is a plethora of consensus algorithms with different features, like Proof of Work (PoW) and Proof of Stake (PoS). Blockchain projects have to decide on the specifications of their peers' network and select one of the three types of blockchain for regulating access; public, private, and consortium blockchain [14]. The most renowned blockchain applications are networks where participants can join or leave the network without approval. This type of blockchain is named public blockchain. On the opposite spectrum, there are private blockchains where participation is managed and regulated by a single entity. In between public and private blockchain lies the consortium blockchain, where a group of entities manages the network's participation. The access restriction is decided by the consortium governing the protocol. Blockchain is a disruptive technology that matures with ongoing research. There are three generations [15] impacted by developments like the development of smart contracts. The first generation of blockchain refers to the inclusion of transactional data in a distributed ledger, with Bitcoin being the most prominent example. The inclusion of smart contracts has shifted blockchain to the second generation, where they are mainly used for establishing the digital economy. Finally, the proliferation of smart contracts has broadened the applied industries to healthcare, energy, and more, as researchers and developers encode business logic to solve problems in their respective fields.

B. Smart Contracts

Smart contracts are programs run when specific criteria are satisfied and are recorded on a blockchain. The cryptographer, Nick Szabo [8], introduced the term smart contracts and parallelised it with the simple and humble example of vending machines. Essentially, they are often used to automate the implementation of an agreement so that all participants may instantly be confident of the conclusion without the participation of an intermediary or time lost. They can also automate a workflow by automatically activating the next activity when certain circumstances are satisfied. Each smart contract contains a contract address, private storage, and predefined functions. The process of smart contracts has four stages:

1) Creation. Several parties first discuss contract responsibilities, rights, and prohibitions. Parties draft a first contractual agreement with the assistance of lawyers and counselors.

Essentially, software engineers convert the agreement stated in natural language into an encoded logic executed with smart contracts written in a range of computer languages. Similarly to software development, the smart contract conversion technique consists of design, implementation, and validation. Smart contract development is an iterative process that includes numerous rounds of talks and iterations. Meanwhile, it also includes a variety of partners, including stakeholders, attorneys, and software developers.

2) Deployment. The verified smart contracts can subsequently be deployed on blockchain systems. Amendments to smart contracts stored on blockchains are impossible due to the blockchain's immutability, and any alterations need the formation of a new contract. Once smart contracts are placed on blockchains, all parties will be able to access them.

3) Execution. A review of the contractual conditions follows the deployment of smart contracts. The contractual operations are automatically carried out once the contractual requirements are met. Essentially, the automatic execution of the statement results in a transaction submitted to the network's peers for validation. After the execution, the committed transactions and modified states are recorded on the blockchain.

4) Completion. After a smart contract has been executed, the new states of all involved parties are updated. Accordingly, the transactions during the execution of the smart contracts and the updated states are stored in blockchains. Meanwhile, the digital assets have been transferred from one party to another (e.g., money transfer from buyer to supplier). Consequently, the digital assets of involved parties have been unlocked. The smart contract then has completed the whole life cycle. It is worth mentioning that during deployment, execution and completion of a smart contract, a sequence of transactions have been executed (each corresponding to a statement in the smart contract) and stored in the blockchain. Therefore, all these three phases need to write data to the blockchain.

All relevant parties' states are updated after the smart contract's execution. As a result, the updates are available on the blockchain as it records the executed transactions and the updated states. Meanwhile, digital assets have been unlocked and moved from one party to another. The smart contract has now completed its whole life cycle. The proliferation of smart contracts implementation is due to the advantages that they bring to organisations. As smart contracts are self-executed with no human intervention and less error-prone [9], they present benefits [10] by reducing risks, diminishing administration and service costs, and boosting the business processes' efficiency. These benefits can translate to different use cases for decentralising and increasing trust and security in the procedures.

C. XACML

XACML is the abbreviation for eXtensible Access Control Markup Language used for establishing a general-purpose policy system. A committee, OASIS [13], defines the standards for XACML and has published the third version of the standard. The definition of standards is essential for enhancing interoperability as vendors can align their development to the standards rather than creating their in-house solutions. In detail, the standard is flexible and allows entities to apply fine-grained attribute-based access control (ABAC) in dynamic and heterogeneous environments. The standard defines three fundamental components for basing the policy system: the rule, policy, and policy set. The three components follow a hierarchical order of magnitude for deploying policies. The most elementary component used by policies is the rules where the target, effect, condition, obligation, and advice are defined to compose the rules to enforce. A policy can consist of multiple rules and is the basic unit for the decision. Consequently, the policy set is a bundle of underlying policies for establishing access control. The standard suggests the inclusion of different components for the access control system. The division into separate components leads to separating actions like enforcement and decision making, which are allocated to different components. The four fundamental components are named points: Policy Administration Point (PAP), Policy Decision Point (PDP), Policy Enforcement Point (PEP), and Policy Information Point (PIP). Their respective functionalities are managing policies, evaluating requests, enforcing the decision, and curating the attribute values for evaluation. Thus, the XACML architecture decouples the enforcement point, the decision making and the management of policies while providing modular configuration and multiple ways of the corresponding components deployment. XACML defines the following phases conducted by every access decision:

- The PDP receives the full security policy from the PAP.
- The PEP receives each access request, translates it to an XACML request and sends it to the PDP.
- In order to retrieve the attributes, in case it is missing from the XACML request, pertaining to subjects, objects, actions, and context, it accesses the services of the PIP.
- The PDP assesses the request in accordance with the PAP's rules and the PIP's attributes.
- The PDP sends the AC decision to the PEP, which is either a permission or a denial and may come with necessary obligations.
- In compliance with the PDP judgment, the PEP enforces these commitments and grants or denies access.

The standard presents advantages for establishing an access control system. The crucial advantage is the separation between authorisation and decision enforcement, allowing modifications on policies depending on business needs. Moreover, the standardization can lead to a fine-grained authorisation as policies can relate to each other with policy sets. Finally, policy management can be easier and alleviate the hurdles in maintaining the system.

III. Related Work

The flexibility of the XACML and its capability for tuning a fine-grained access control system has inspired research in the field of IoT. Moreover, XACML permits the execution of access control in a decentralised manner to cover the requirements set by the growing number of devices. Researchers

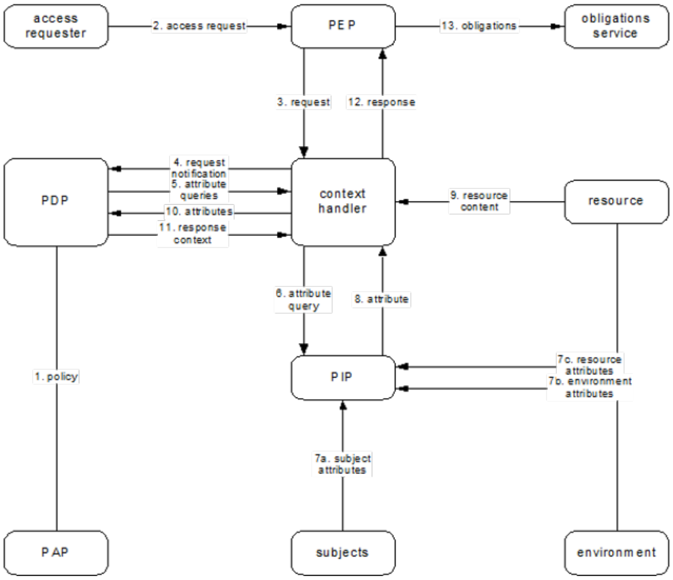

Fig. 1. XACML architecture.

suggest the implementation of XACML on blockchain for IoT devices. PolicyChain [11] executes the access control policies based on attributes and deploys PAP and PDP on the blockchain for a transaction-oriented policy expression. Additionally, the application manages the policy lifecycle by tracing three stages: creation, renovation, and revocation of policies. Similarly, Maesa et al. [12] deploy an auditable access control system that executes XACML components on the blockchain. In particular, the logical operations executed by PEP and PAP are encoded on smart contracts for their decentralised execution. Another application with a defining purpose to apply ABAC on IoT devices is suggested by Zhang et al. [3] introducing an attribute-based access control scheme combining the ABAC model and blockchain technology to enable IoT device authorisation that is decentralised, customisable, and fine-grained. Blockchain technology is used to give authentic and trustworthy credentials. More crucially, a verified cooperation method is intended to suit the demands of controlled access authorisation in emergencies. Authority nodes are built to do large computations and communicate with the blockchain. A proof-of-concept prototype has been developed to demonstrate that the system is scalable, efficient, and well-suited to IoT devices. The access control scheme can assure authorised access by blocking various attacks and supplying a revocation and supervision function. A subject of discussion for blockchain and IoT devices is the execution of actions, as devices can have limited capabilities. The definition of the layer to host blockchain nodes is part of research to connect edge, fog, and cloud layers involved in the IoT field. Alnefaie et al. [1] presented a distributed fog-based access control system for healthcare. The access control functions are spread in this architecture to bring policy decisions and policy information processes to the network's edges, close to the end nodes. This model has three levels. Sensor nodes are examples of IoT-enabled devices in the first level. A node in healthcare can be a sensor that monitors a patient's health state or a smart device. The fog computing layer is represented by the second level, which includes network equipment such as switches, routers, access points (APs), and gateways. The fog nodes can cooperate in providing computing and storage solutions. The third level is the cloud which comprehends servers and data centres. This method improves availability while decreasing latency.

As smart contracts are encoded logic executed on the blockchain, they are pivotal for decentralising the access control system. Andersen et al. [2] proposed a completely decentralised authorisation system, titled WAVE, that works on a global scale and supplies fine-grained permissions, noninteractive delegation, and proofs of permission that can be reliably validated while permitting revocation. It allows substantial and complicated rules to be defined using smart contracts on a public blockchain and is immune to DoS attacks without relying on any central trusted parties. In advance, there is a unique approach for safeguarding the confidentiality of resources on the public blockchain that does not rely on out-of-band communications or contact between granters, provers, or verifiers. WAVE is capable of reinforcing city-scale federation with millions of participants and permission regulations. Additionally, Zhang et al. [4] described a smart contract-based framework, which contains multiple access control contracts (ACCs), one judge contract (JC) and one register contract (RC), to accomplish decentralised and reliable access control for IoT systems. Each ACC offers one access control method for a subject-object pair and supports static access right validation based on established rules as well as dynamic access right validation by observing the subject's behaviour. By receiving misbehaviour reports from the ACCs, evaluating the misconduct, and delivering the associated penalty, the JC implements a misbehaviour-judgment mechanism to support dynamic validation of the ACCs. The RC stores the information about the access control and misbehaviour-judging methods, as well as their smart contracts, and offers functions to manage these methods. Finally, access control implementations use renowned public blockchains to benefit from the availability of resources in the public network. Essentially, the nodes execute the procedures alleviating the maintenance cost for operating a peer node in a network. Nakamura et al. [6] proposed a decentralised and trustworthy Capability-Based Access Control (CapBAC) scheme using the Ethereum smart contract technology. A smart contract is constructed for each item in this scheme to store and maintain the capability tokens allocated to the linked subjects, as well as to validate the ownership and authenticity of the tokens for access control. The proposed scheme handles tokens in access rights or actions, i.e., one token per action. To show the practicality of the suggested CapBAC system, it was deployed on a locally built Ethereum blockchain network. Furthermore, we calculated the monetary cost of our system in terms of gas usage to compare it to other researchers' current Blockchain-Enabled Decentralised

Capability-Based Access Control (BlendCAC) approach. The experimental findings suggest that the proposed system outperforms the BlendCAC approach regarding consistency of capability delegation, adaptability and granularity at almost the same monetary cost. The research on access management on IoT devices is ongoing, and there are different applications apart from applying XACML.For instance, BACI [5] is an architecture for permission delegation and access control in IoT. The owner of the IoT device generates a smart contract on the BC for his resource. To access a resource, the IoT device or user submits a request to the BC's resource smart contract. BC validates the delegatee platform's integrity and delegation rules prior to authorisation activation. BACI is a hybrid that handles both event-based and query-based permission delegation. The Confidentiality, Integrity, and Availability model is used to assess the security of the architecture. This approach was evaluated in the Simple PROMELA INterpreter (SPIN) model checker using PROMELA (Process Meta Language). The "Platform Verification", "Delegation", and "Mutual Exclusion" properties written in Linear Temporal Logic (LTL) were also validated against the PROMELA model.

IV. Decentralised XACML for IoT devices

This section presents the architectural approach of the implementation for deploying a decentralised evaluation of XACML policies. The application aims to benefit the real-world scenario of a construction site where devices and people constantly join and leave the network.

A. *Implementing decentralised decision*

As the number of devices grows in the network, the attack surface grows, and central approaches may affect the network's scalability. Moreover, new technologies are introduced in IoT systems, increasing the potential vulnerabilities. It is vital to establish secure access control as inspired by ENISA's best practices, including access control for IoT security. For this reason, this paper suggests the implementation of an XACML access control based on a consortium blockchain. Initially, the shift from a centralised architecture for access management to a decentralised one presents some benefits. Data immutability is a core feature of blockchain and enhances an access control system. The various components of the blockchain and its underlying cryptography, such as hash functions, Merkle tree, and consensus mechanisms ensure that data on the ledger is immutable. Every participant in the system is certain that once the data is stored in the blockchain, it is authentic and cannot be changed. In addition, every malicious change or attempt can be detected easily. This leads to a secure system that is resilient to cyber threats and can prevent human errors. Essentially, the attributes and policies are tamper-proof, resulting in a transparent decision. Participants can check the transactions and their validity. Therefore, they can verify the results of each authorisation decision and every stored policy used to evaluate the given requests. Thus, any participant whose access has been fraudulently denied can prove that the access should have been granted through the use of the stored data. Moreover, the network of IoT devices can benefit from a single source of truth set by the blockchain. In detail, the consensus algorithm maintains a stable state for the blockchain across the network, meaning that all the IoT devices can access the same information. Hence, a central authority that mediates every access request and manages all the data becomes unnecessary. With all due respect to policies, every access request can be evaluated through secure snippets of code distributed among participants. Each peer in the blockchain is able to execute these secure snippets of code that perform access control according to the policies that protect the resources. Therefore, the appropriate authorisation decision is made. This provides an effective way to prevent false authorisation decisions. The performance and the stability are increasing since the computational power of access control is distributed among the peers. Finally, centralised approaches may be proved as single points of failure, as the congestion from the devices' requests can result in service failures. The decentralised execution of procedures with smart contracts can mitigate this risk and boost the scalability of IoT networks, as it provides a fully stable system when software and hardware faults occur. Thus, an access control system that uses blockchain is always available for the participants.

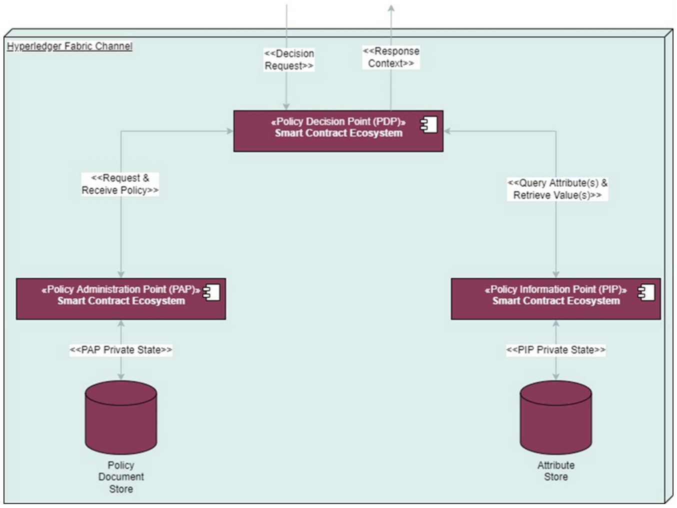
Hyperledger Fabric Channel
<<Decision Request>>
<<Response Context>>
«Policy Decision Point (PDP)» Smart Contract Ecosystem
<<Request & Receive Policy>>
<<Query Attribute(s) & Retrieve Value(s)>>
«Policy Administration Point (PAP)» Smart Contract Ecosystem
«Policy Information Point (PIP)» Smart Contract Ecosystem
<<PAP Private State>>
<<PIP Private State>>
Policy Document Store
Attribute Store

Fig. 2. XACML component architecture.

The implementation is based on a consortium blockchain created with the open-source framework Hyperledger Fabric [16]. The access control system uses blockchain to store in a private manner critical data for evaluation of policies. In detail, the data stored on blockchain are the policy documents and the attributes. Furthermore, smart contracts are tasked with executing the logic for decisions in a decentralised manner. Essentially, the points deployed on the blockchain are PAP, PDP, and PIP. As the three aforementioned points are deployed within smart contracts, the evaluation of a policy is fully decentralised as the data and evaluation are on the blockchain. The functionalities for each component are deployed on separate smart contracts. The implementation can be expanded as the architecture is flexible enough to leave room for developing applications on a layer above the blockchain. As the requests and decisions are stored on the blockchain's ledger as transactions, it is possible to deploy applications to analyse and visualise the underlying data. An application with added value to security is the creation of audit mechanisms for the decisions and their audit trail. As the distributed ledger stores access data in an immutable manner, it allows for the creation of an audit trail that is effective and tamper-proof. There are other sectors such as vehicle emission [17] benefitting from traceability and even publishing certificates based on standards.

B. IoT Scenario: Construction Site

The implementation of a decentralised access control system is to be tested in the challenging environment of a construction site. Initially, the environment is complex as people and machinery constitute a busy environment. Additionally, construction equipment includes various IoT devices, including but not limited to wearable devices, which are not explicit to specified people but rather allocated among construction workers based on characteristics and training. In such a fluid environment, the suggested access control system can alleviate the burden placed on the security team by enforcing Attribute-Based Access Control (ABAC). The IoT devices and people characteristics can be encoded to policies to evaluate access and be included as attributes to the rules. The proposed approach is independent of the resources and the actions which can be executed, as long as the appropriate policy for each resource is defined. The construction site is an excellent scenario for applying decentralised access control to avoid security attacks or unauthorised devices' access. As the evaluation of the policies is executed on the blockchain with the smart contracts, there is no central point for malicious users to attack, e.g. honeypots. Essentially, the availability of the system is enhanced and allows scaling by incorporating more and more devices. Finally, the immutability of data extending to smart contracts can enhance data security for users of the system. Wearables devices can capture data critical for the health condition of workers and augment reality with information to assist in completing tasks. The wearables proliferation demands maintaining data security as they are sensitive information. The ledger holds the access requests and decisions in the approved transactions making it possible to audit the access.

V. Conclusion

The growing use of IoT devices sets challenges to scalability and security. Access control is a way of upkeeping the system's overall operation by applying policies. As the XACML standard offers a fine-grained application of policies, it seems appropriate to apply it to IoT systems. Especially, coupling the standard with blockchain can ensure the security and decentralisation of the system. This paper suggested the deployment of vital points for the policy evaluation to be completely decentralised. The fully decentralised evaluation is based on a consortium blockchain on Hyperledger Fabric with smart contracts executing the business logic for the points. The architecture is flexible for building a future application on top of the blockchain layer. The implementation of the architecture is to be part of the real-world scenario of a construction site. The scenario is excellent for testing the implementation as it has interconnected individuals and devices.

Acknowledgment

This work was framed in the context of the project ASSIST-IoT, which receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement 957258.

References

[1] S. Alnefaie, A. Cherif and S. Alshehri, "Towards a Distributed Access Control Model for IoT in Healthcare," 2019 2nd International Conference on Computer Applications and Information Security (ICCAIS), 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769462.

[2] Kolb, J., Chen, K., Fierro, G., Culler, D.E., and Popa, R.A. (2017). "WAVE : A Decentralized Authorization System for IoT via Blockchain Smart Contracts".

[3] Zhang, Yan and Li, Bing and Liu, Ben and Wu, Jiaxin and Wang, Yazhou and Yang, Xia. (2020). An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices. Electronics. 9. 285. 10.3390/electronics9020285.

[4] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594-1605, April 2019, doi: 10.1109/JIOT.2018.2847705.

[5] Zhu, Yong and Wu, Xiao and Hu, Zhihui. (2022). Fine Grained Access Control Based on Smart Contract for Edge Computing. Electronics. 11. 167. 10.3390/electronics11010167.

[6] Nakamura, Y.; Zhang, Y.; Sasabe, M.; Kasahara, S. Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things. Sensors 2020, 20, 1793. https://doi.org/10.3390/s20061793

[7] Nakamoto S, 2008. Bitcoin: a peer-to-peer electronic cash system, Available: http://bitcoin.org/bitcoin.pdf.

[8] Szabo, Nick. "The idea of smart contracts." Nick Szabo's papers and concise tutorials 6.1 (1997): 199.

[9] Xu, Yongshun, Heap-Yih Chong, and Ming Chi. "A review of smart contracts applications in various industries: a procurement perspective." Advances in Civil Engineering 2021 (2021).

[10] Zheng, Zibin, et al. "An overview on smart contracts: Challenges, advances and platforms." Future Generation Computer Systems 105 (2020): 475-491.

[11] Chen, E., Zhu, Y., Zhou, Z., Lee, S. Y., Wong, W. E., Chu, W. C. C. (2021). Policychain: A Decentralized Authorization Service With Script-Driven Policy on Blockchain for Internet of Things. IEEE Internet of Things Journal, 9(7), 5391-5409.

[12] Maesa, D. D. F., Mori, P., Ricci, L. (2019). A blockchain based approach for the definition of auditable access control systems. Computers and Security, 84, 93-119.

[13] OASIS. "eXtensible Access Control Markup Language (XACML) Version 3.0 Plus Errata 01". https://docs.oasis-open.org/xacml/3.0/errata01/os/xacml-3.0-core-spec-errata01-os-complete.html (accessed: Juy 7, 2022).

[14] Fernandez-Carames, Tiago M., and Paula Fraga-Lamas. "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories." Ieee Access 7 (2019): 45201-45218.

[15] Akram, Shaik V., et al. "Adoption of blockchain technology in various realms: Opportunities and challenges." Security and Privacy 3.5 (2020): e109.

[16] Hyperledger Foundation. Hyperledger Fabric. https://www.hyperledger.org/use/fabric (accessed: July 11, 2022).

[17] S. Terzi, C. Savvaidis, K. Votis, D. Tzovaras and I. Stamelos, "Securing Emission Data of Smart Vehicles with Blockchain and Self-Sovereign Identities," 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 462-469, doi: 10.1109/Blockchain50366.2020.00067.