Traditional and Blockchain-based access control models in IoT: A review

Milan Stojkov, Miloš Simić, Goran Sladić, Branko Milosavljević
Faculty of Technical Sciences, University of Novi Sad, Serbia
{stojkovm, milos.simic, sladicg, mbranko}@uns.ac.rs

Abstract — **Internet of Things gained popularity in recent years and the number of devices that are being interconnected is increased every day. These devices can exchange all kinds of information which is beneficial but also this introduces some concerns in terms of security and privacy. Conventional security approaches have shown as modestly applicable for IoT primarily due to the decentralized and lightweight nature of the devices. Access control is one of the concerns that have to be addressed. Traditional models are widespread in IoT systems as a starting point solution, but their shortcomings can be overcome with emerging technologies such as Blockchain that is a base for various cryptocurrencies that have recently gained popularity to provide security and privacy in peer-to-peer networks with similar topologies to IoT. In this paper, an analysis and comparison of different traditional and Blockchain-based solutions are conducted to see if and how IoT specific challenges can be tackled with these new technologies.**

Keywords: IoT, Internet of Things, security, access control, authorization, Blockchain, smart contracts

I. INTRODUCTION

Internet of Things (IoT) popularization in recent years introduced the period of a constant increase of smart devices that are connected to the Internet. With systems of interconnected smart devices and cheap sensors, the collection of information from the environment can be achieved more smoothly and in a greater amount. This information can then be formed into a knowledge that can improve efficiencies of services in a wide range of application domains such as healthcare, industrial automation, transportation, the energy sector. On the other hand, this rapid collection, processing, and dissemination of data raise serious security and privacy concerns [1]. Security issues such as authentication, access control, privacy, system configuration, information storage, and management are among the top challenges in IoT environments today [2]. Access control (AC) is one of the priority issues that IoT systems have to face. In [3] AC is defined as a method for controlling who (subject) can perform which access rights (actions) on which resource (object).

Traditional AC models can be incorporated in IoT systems but cannot address new challenges in an efficient way that these systems require. That is why new approaches that involve relatively new technologies such as Blockchain should be taken into consideration as a possible solution for shortcomings of the traditional models. Bitcoin [12] is the first decentralized digital currency that was launched in 2008. It uses the idea of a peer-to-peer computer network that is made of its users' machines. The main technology behind Bitcoin is precisely Blockchain, which is an immutable public record of data secured by a network of peer-to-peer participants that has a similar topology to IoT systems. Nowadays, Blockchain is used for many different applications such as smart contracts, distributed cloud storage, and digital assets. The idea is to have blocks chained together as a ledger. These blocks have to be mined by miners - entities that solve a resource-intensive cryptographic puzzle called *Proof of Work* and appended as new blocks to Blockchain. Any node in the peer-to-peer network can be a miner. Every time a new transaction occurs, it is broadcast to the entire network. Every miner who receives the transaction has to verify it by validating the signatures contained within the transaction and appends that transaction to its pending block of transactions that are waiting to be mined. Two things make this system theoretically tamperproof - a cryptographic fingerprint unique to each block called a hash, and a *consensus protocol*, the process by which the nodes in the network agree on a shared history. If anyone wants to change an entry in the ledger retroactively, it has to calculate a new hash not only for the block it is in but also for every subsequent block. And this has to be done faster than the other nodes can add new blocks to the chain. However, this robustness comes at a price since miners consume their resources for mining the same transaction, which in turn also increases the delay.

The goal of this paper is to present the analysis of different traditional AC models and new Blockchain-based ones and to identify the shortcomings of different approaches in terms of introduced challenges by IoT systems.

The rest of this paper is organized as follows: Section II presents related work in the area of access control models in IoT. Section III describes challenges in IoT that have to be taken into consideration when modeling access control. In Section IV, Blockchain-based general access control flow is presented. Section V describes selected existing access control models, traditional and Blockchain-based, and how they fit into the IoT environment. The conclusion of the paper is presented in Section VI.

II. RELATED WORK

In literature, there has been a lot of work done that involves access control. However, in constrained environments such as IoT, solutions for AC are not mature enough. Access control models such as Role-Based Access Control (RBAC) [4] with extensions such as GEO-RBAC [5] and GSTRBAC [6] and Attribute-Based Access Control (ABAC) [6] are widely used in traditional IT systems. IoT systems come with new challenges that these models

cannot efficiently solve such as scalability, heterogeneity, a large number of distributed and lightweight devices, etc. With that in mind, authors in [18] proposed a hybrid access control model based on RBAC and ABAC in order to improve some performance of the two for IoT. New environments require new approaches when it comes to AC and authors in [19][21] recognize Blockchain as a technology that may propose solutions that can make progress or even solve these new challenges that arise.

III. Challenges in IoT

A comprehensive literature review was conducted by examining the electronic database Google Scholar using secondary research approach. By using the snowball and cross-referencing methodologies the most mentioned models in papers are considered for analysis. The only papers considered were those written in English and that contained an abstract and were published between 2010 and 2019. Authors conducted this review using search terms "access control", OR "access control model", OR "blockchain", OR "smart contract" combined with "IoT" (or "Internet of Things").

Several challenges that apply to IoT that access control models have to tackle are recognized and extracted from the filtered papers. These challenges are:

- Scalability – Increased number of devices that are interconnected in a typical IoT system directly affect cumulative management workload to access control systems. The system must be able to handle large numbers of users, applications, and policy evaluation and enforcement points. Scalability is considered at the architectural level, i.e., whether the system can be implemented, deployed, and used in a manner where management, maintenance, and operational costs do not increase as the number of system components increases [13].
- Granularity – Many different users and devices with varied roles and responsibilities are projected to access data collected by IoT devices and thus fine-grained access control that would support that is necessary.
- Fault tolerance – Robustness has an important role in the reliability and creditability of an application. The system's readiness to face failure on devices is better supported in distributed architectures than in the centralized architectures.
- Latency to get authorization – This challenge evaluates the latency to get an authorization. The centralized architectures have dedicated nodes responsible for access control that means almost real-time authorization. Distributed architectures have to introduce some overhead of communication or computation.
- Distributed environment – A distributed approach for access control in IoT has many advantages. The end-devices are no longer passive entities that only send information to a central entity but can manage them on their own. Also, these devices are able to send information just when necessary, since in this case there is no central entity responsible for gathering the data from the devices in order to make decisions about access control. Further, the removal of intermediate entities enables devices to carry out end-to-end security for access requests [14].
- Ease of management and upgrade – IoT context is ever-changing and this in return demands that access control policies and rules have to be easily managed with great potential for upgradeability. With an enormous number of devices, this might be very hard to achieve.
- Possibility to adapt – Access control should be flexible to be adapted to different contexts. Also, it should be able to support predefined patterns as well as spontaneous and short-lived interactions. This may be the biggest challenge that has to involve sophisticated techniques such as novel machine learning approaches.

Access control models that were analyzed against these challenges in mind are:

- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- FairAccess [9]
- BlendCAC [10]
- Smart Contact-based AC (SC AC) [11].

IV. Blockchain AC Model Concept

Blockchain has several advantages that make it an attractive technology for addressing security and privacy challenges in IoT [8]:

- Decentralization – All nodes with their resources can be involved in communication and thus improve the scalability and robustness of the whole solution. In that way, the overall delay can be decreased, and a single point of failure can be prevented.
- Security – Blockchain represents a secure network using nodes that can be considered untrusted which is desirable in IoT with a great number of heterogeneous devices.
- Anonymity – The inherent anonymity is well-suited for most IoT use cases where the identity of the users must be kept private.

On the other hand, integration of Blockchain in IoT is not straightforward and at least the following critical challenges have to be taken into consideration:

- Mining of blocks is time-consuming while in most IoT applications low latency is desirable. Also, mining is a computationally intensive operation, while the majority of IoT devices are resource-constrained.
- Blockchain scales poorly as the number of nodes in the network increases. IoT networks are expected to contain a large number of nodes.
- The underlying Blockchain protocols create significant overhead traffic, which may be

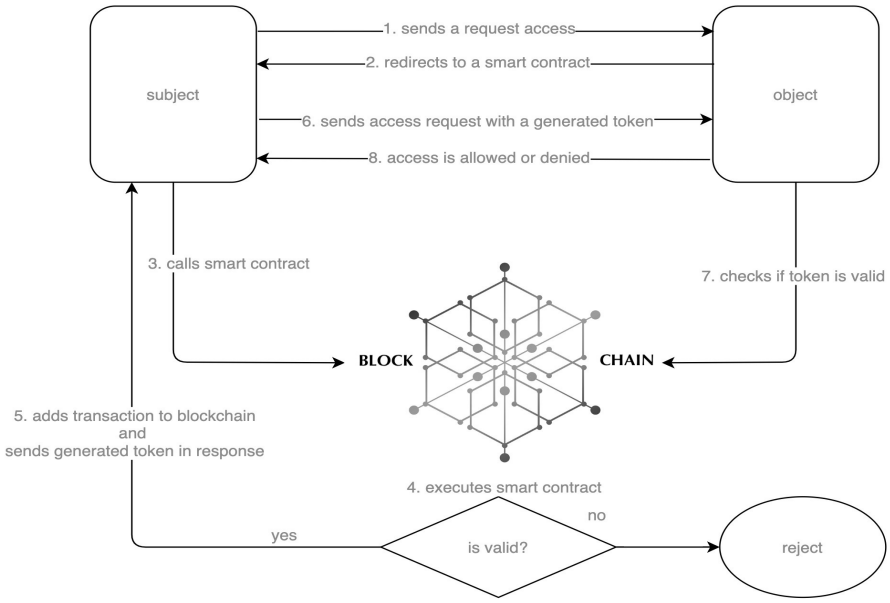

Figure 1. Access control models flow based on Blockchain; request for authorization

undesirable for certain bandwidth-limited IoT devices.

When it comes to access control models that are based on Blockchain, the main concept flow for the initial request for authorization is presented in Figure 1 where smart contracts [15] can be substituted with a more primitive function that would handle policy evaluation.

V. Access Control Models Evaluation

The analysis showed that traditional AC models have to be modified and combined to gain better performance in IoT systems. On the other hand, Blockchain-based solutions proposed new decentralized approaches that fit IoT needs in a good number of requirements. Concretely, the main findings in this analysis are:

- RBAC – Still widely adopted AC model in terms of usage and implementation; IoT systems are considered as systems with a lot of nodes (users) which can imply the existence of a lot of roles and RBAC can be considered unfit because of limited granularity and scalability; Consequence is that it is not easy to manage and upgrade; It is centralized model, so the authorization process involves no particular overhead.
- ABAC – Tries to solve problems with RBAC by using user's, resource's or environment's properties to specify access policies; It can be applied to scenarios where users are dynamically changing; Can be very complex and attributes have to be consistent within ever-changing domains in IoT; Has scalability issues in terms of managing trust among different attribute and service providers; Not easy to manage and upgrade with an increasing number of attributes; Does not provide flexible delegation of rights.
- FairAccess – This decentralized AC enables the Resource Owner (RO) to control the data; The model utilizes a scripting language used in Bitcoin for evaluation of the policy to make a decision which allows transcoding only two types of AC policies and that restricts the ease of upgradeability and granularity; It takes lightweight nature of the devices in mind but the transaction fees can be higher than the actual worth of the resource accessed which is not ideal in case of resource-constrained IoT devices; RO will issue a token when receiving an authorized request, which is similar to a centralized component; Token is issued with a smart contract which is published on the Blockchain and difficult to be modified.
- BlendCAC – Uses an identity-based capability token management strategy, which utilizes smart contract for registration, propagation and revocation of the access authorization; This AC model introduces slightly increased overhead in terms of computation as well as storage compared to RBAC and ABAC; It is only tested on a Raspberry Pi device which owns sufficient resources and cannot represent most IoT devices, thus lightweight nature of the devices is not taken into consideration; RO will also issue a token when receiving an authorized request, which is similar to a centralized component; Token is also issued with a smart contract which is published on the Blockchain and difficult to be modified.
- Smart Contract-based AC – The whole framework is based on Ethereum [16] smart contracts that consist of multiple access control contracts, one judge contract, and one register contract to achieve distributed and trustworthy AC for IoT with focus on access control lists that will achieve access control; Every resource (subject or object) in IoT system has to write a rule and this leads to decrease of management and upgrade potential; Device heterogeneity was not taken into consideration to make full use of the computing and storage capabilities of IoT devices to maintain the security of Blockchain; Number of smart

TABLE I.
COMPARISON OF DIFFERENT ACCESS CONTROL MODELS

Challenge / Model	Scalable	Fault-tolerant	Granular	Decentralized	"Fast" authorization	Easy to manage and upgrade	Possibility to adapt
RBAC	No	No	Yes (limited)	No	Yes	No	No
ABAC	No	No	Yes	No	Yes	No	No
FairAccess	Yes	Yes and No	Yes	Yes	No	No	No
BlendCAC	Yes	Yes and No	Yes	Yes	No	No	No
SC AC	Yes and No	Yes and No	Yes	Yes	No	No	No

contracts is big, thus great overhead is introduced in the evaluation process.

VI. CONCLUSION

The summary of the analysis is presented in Table 1. Traditional access control models are still being used in the IoT ecosystem, but there is a tendency to make a transition to more sophisticated ones for a specific domain. Analyzed Blockchain-based solutions have their flaws but also solve some of the identified challenges.

Looking at Table 1, we can conclude that between traditional models' centralized nature and Blockchain-based models' decentralized nature, it is necessary to make a tradeoff since IoT devices usually do not have the capacity for processing or storage to deal with a full distributed AC process. Another problem with all of these models is that the management of devices and policies in IoT context with a great number of devices is very hard. This forces AC models to define static policies where all the rules have to be written in advance. This is challenging since the rules by design have to be well-defined, optimal, conflict-free, and not to introduce further security problems when the system is in production. As a result, upgradeability potential is dropped to a minimum. Consequently, the possibility to adapt policies to the newly created context is very hard. A possible solution would be to employ specifically designed machine learning algorithms to generate new and update existing policies in runtime without the interference of the IoT system administrator. In the context of access control, Blockchain's main disadvantage is the mining process. Every model analyzed in the paper involved experiments with a small number of devices which is not the picture of the real environment and the mining problem was not stressed enough. Thus, these solutions are primarily for private Blockchain environment [20] purposes where overhead that mining introduces might be irrelevant. An alternative approach for tackling the access control model might be to switch to Tangle, i.e. direct acyclic graph or DAG that is used in IOTA [17] that has no miners, thus no miner fees and no incentives to slow the network down.

REFERENCES

[1] Das M. L. Privacy and Security Challenges in Internet of Things. Distributed Computing and Internet Technology. pp. 33-48, 2015.

[2] Fadele A., Othman M., Hashem I., Alotaibi F. Internet of things Security: A Survey. Journal of Network and Computer Applications. 2017.

[3] Gusmeroli S., Piccione S., Rotondi D. A capability-based security approach to manage access control in the internet of things. Mathematical and Computer Modelling. 2013.

[4] Sandhu R. S.Role-based Access Control. Adv. Comput. 1998.

[5] Bertino E., Catania B., Damiani M.L., Perlasca P. GEO-RBAC: A spatially aware RBAC. ACM Transactions on Information and System Security. 2007.

[6] Abdunabi R., Al-Lail M., Ray I., France R.B. Specification, Validation, and Enforcement of a Generalized Spatio-Temporal Role-Based Access Control Model. IEEE Systems Journal. 2013.

[7] Hu V. C., Ferraiolo D., Kuhn R. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication. 2014.

[8] Atlam H., Alenezi A., Alassafi M., Wills G. Blockchain with Internet of Things: Benefits, Challenges and Future Directions. International Journal of Intelligent Systems and Applications. 2018.

[9] Ouaddah A., Elkalam A.A., Ouahman A.A. FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks. 2017.

[10] Xu R., Chen Y., Blasch E., Chen G. BlendCAC: A BLockchain-Enabled Decentralized Capability-Based Access Control for IoTs. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). 2018.

[11] Zhang Y., Kasahara S., Shen Y., Jiang X., Wan J. Smart Contract-Based Access Control for the Internet of Things. IEEE Internet of Things Journal. 2019.

[12] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008.

[13] Keromytis A., Smith J. Requirements for Scalable Access Control and Security Management Architectures. ACM Transactions on Internet Technology. 2002. 7. 10.1145/1239971.1239972.

[14] Hernández-Ramos J., Antonio J., Marín L., Skarmeta A. Distributed Capability-Based Access Control for the Internet of Things. 2013.

[15] Alharby M., van Moorsel A. Blockchain-based Smart Contracts: A Systematic Mapping Study. Fourth International Conference on Computer Science and Information Technology (CSIT-2017). 2017.

[16] Ethereum Homestead Documentation. https://ethdocs.org/en/latest/index.html, accessed April 2020

[17] Meet the Tangle. https://iota.org/research/meet-the-tangle, accessed April 2020

[18] S. Kaiwen, Y. Lihua. Attribute-role-based hybrid access control in the internet of things. Asia-Pacific Web Conference. Springer International Publishing, 2014.

[19] Conoscenti M., Vetrò A., De Martin J.C. Blockchain for the Internet of Things: A systematic literature review. IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, 2016, pp. 1-6, doi: 10.1109/AICCSA.2016.7945805. 2016

[20] Buterin V. On Public and Private Blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ accessed April 2020

[21] Pilkington M. Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016. Available at SSRN: https://ssrn.com/abstract=2662660