Security Risk Assessment for Blockchain-Based Identification and Authentication Method of Internet of Things Objects

Raimundas Savukynas*
Vilnius University, Vilnius, Lithuania
Institute of Computer Science, *email: raimundas.savukynas@mif.vu.lt

Abstract

The Internet of Things (IoT) takes promises the possibility of connecting billions of objects into networks providing a wide variety of information. The exponent growing number of connected heterogeneous objects brings security issues for identification and authentication method of IoT. The major security risks for the identification and authentication method of IoT objects are identity spoofing, network disruption, signal jamming, software modification, unauthorised access, and information disclosure. A security risk assessment is an essential part of the information security process that identifies critical assets, threats, vulnerabilities in the IoT and removes found hazards or minimizes the level of their risk by adding control measures and taking precautions with respect to security issues. Therefore, the ultimate goal of the security risk assessment is to measure the risk using a testing process of the identification and authentication method of IoT objects in order to obtain numerical values that could be used to compare the obtained security risk for each asset and process. Existing identification and authentication methods of IoT objects are based on a centralized model which has risk with a single point of failure. Meanwhile, a blockchain-based identification and authentication method of IoT objects is considered an alternative that eliminates a single point of failure and uses a cryptographic hash function as the core of security. A blockchain-based identification and authentication can prevent the loss of identities, effectively detect frauds and mitigate critical risk issues, provide transparent and secure authentication of different IoT objects. The aim of this work is to propose a structured methodological approach to identifying security threats and assessing related security risks for blockchain-based identification and authentication method of IoT objects. Resulting of this assessment, countermeasures are proposed to improve blockchain-based identification and authentication method of IoT objects.

Methodology

The methodology applied for security risk assessment blockchain-based identification and authentication method of IoT objects is shown in Figure 1.

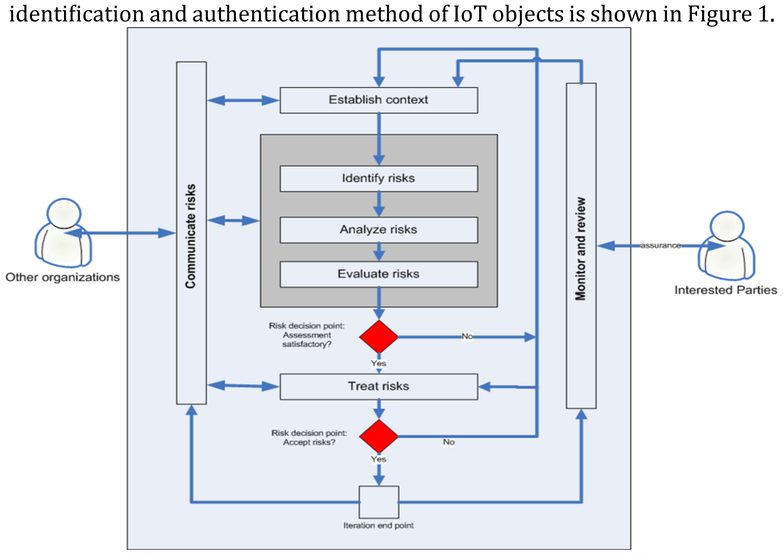


Figure 1: *Security risk assessment methodology [1]*

Method

The method and components of the extended functionality of checking the process of IoT objects before connection to the environment developed with detailed implementation of security processes are shown in Figure 2.

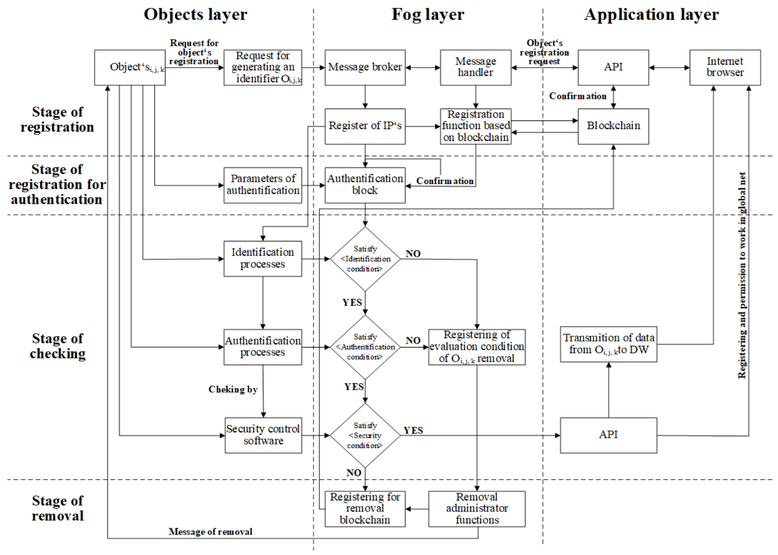


Figure 2: *Identification and authentication method of IoT objects [2]*

The identification and authentication start when the object $O_{i,j,k}$ initializes the data transmission process, which is transmitted from the objects layer. The process of registering and recognizing object $O_{i,j,k}$ is detailed analyzed, which must ensure decentralization and protection using cryptography. There are three important identifiers of object $O_{i,j,k}$, where i is an identifier of equipment, j is an authenticity index of the object, and k indicates the functional status of the object. On the registration stage, object $O_{i,j,k}$ sends a message with name and identifier to the message broker in the fog layer, which forwards a received message for further processing and inspection. An object $O_{i,j,k}$ identifier i consists of the last two variables $i=\{i_1, i_2\}$, where:

- i_1 – variable represents the unidirectional function of device hardware.
- i_2 – variable represents of usage of a physical unclonable function (PUF).

The Fog device receives a message from the object $O_{i,j,k}$ and applies it to the blockchain using an API with a request to verify identification parameters. The necessary checking procedures in the verification process are included for object $O_{i,j,k}$ security increase before starting work in the IoT environment:

- ISCS – responsible for checking object $O_{i,j,k}$ registration conditions.
- ACSS – responsible for checking object $O_{i,j,k}$ authentication conditions.
- SCSS – responsible for checking object $O_{i,j,k}$ security control conditions.

If such conditions types are not satisfied, the object $O_{i,j,k}$ is removed from the IoT environment, and some activities are performed to inform about the insecure conditions of $O_{i,j,k}$, which forwarded to the stage of removal of the object from the IoT environment. The object $O_{i,j,k}$ removal process is performed by the block of the system administrator in the fog layer server if this action is affected by consensus or other satisfaction checking activities. The fog server or system administrator block can refer to the blockchain by using a simple API request and remove the object $O_{i,j,k}$ from the blockchain.

Matrix

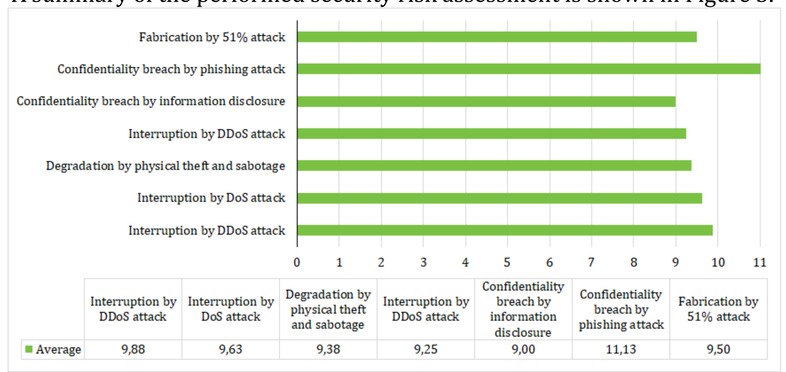
Table 1 shows the assessed impact and probability of each method threat. The scoring shown in this table is subjective and depends on the definition of the scales, best practices, intuition, and the security expert's knowledge.

Table 1: *Security risk assessment matrix [3]*

Probability \ Impact	No impact	Very low	Low	Average	High
Vanishingly low	1	2	3	4	5
Very low	2	4	6	8	10
Low	3	6	9	12	15
Average	4	8	12	16	20
High	5	10	15	20	25
Extremely high	6	12	18	24	30

Results

A summary of the performed security risk assessment is shown in Figure 3.



	Interruption by DDoS attack	Interruption by DoS attack	Degradation by physical theft and sabotage	Interruption by DDoS attack	Confidentiality breach by information disclosure	Confidentiality breach by phishing attack	Fabrication by 51% attack
Average	9,88	9,63	9,38	9,25	9,00	11,13	9,50

Figure 3: *Security risk assessment summary*

Conclusion

Performing security risk assessment in a structured way helps identify dangerous locations for blockchain-based identification and authentication method of IoT objects that are most easily vulnerable to break or attack. There is still a need for more research to highlight the problems of security, privacy, scalability, and describe technologies which yet to be implemented.

References

[1] Amarachi, A. A., Okolie, S. O., Ajaegbu, C. (2013). Information Security Management System: Emerging Issues and Prospect, IOSR Journal of Computer Engineering (IOSR-JCE), 12(3), 388 - 393. ISSN 2278-0661.

[2] Savukynas, R. (2020). Integration of Safety Means with Functions of Blockchain in Multi-layered Architecture of IoT for Safer Data Transmission Procedures, in Proc. of the 10th International Conference on Computer Science & Information Technology, 33 - 18. ISSN: 2231-5403.

[3] Andrade, R. O., Yoo, S. G., Ortiz-Garces, I., Barriga, J. (2022). Security Risk Analysis in IoT Systems through Factor Identification over IoT Devices, Applied Sciences, 12(6), 1 - 32. ISSN 2076-3417.