A Cyber Resilience Framework for NG-IoT Healthcare Using Machine Learning and Blockchain

1st Vasiliki Kelli  
Department of Electrical and Computer Engineering  
University of Western Macedonia  
Kozani, Greece  
vkelly@uowm.gr

2nd Panagiotis Sarigiannidis  
Department of Electrical and Computer Engineering  
University of Western Macedonia  
Kozani, Greece  
psarigiannidis@uowm.gr

3rd Vasileios Argyriou  
Computer Science Department  
Kingston University  
London, UK  
avasileios.argyriou@kingston.ac.uk

4th Thomas Lagkas  
Department of Computer Science  
International Hellenic University  
Thessaloniki, Greece  
tlagkas@cs.ihu.gr

5th Vasileios Vitsas  
Department of Information and Electronic Systems Engineering  
International Hellenic University  
Thessaloniki, Greece  
vitsas@ihu.gr

Abstract—Internet of Things (IoT) technology such as intelligent devices, sensors, actuators and wearables have been integrated in the healthcare industry, thus contributing in the creation of smart hospitals and remote assistance environments. Ensuring the eHealth network adopts the appropriate security measures in order to effectively protect sensitive patient data against malicious attempts is a tough challenge. Devices composing eHealth infrastructure are considered to be easily exploitable. To that end, a solution monitoring the intelligent healthcare environment is of essence. In addition, by digitalising all health records, appropriate measures need to be implemented in order for patient records to be accessible by authorized personnel only. Furthermore, creating interoperable systems, capable of being integrated by multiple organizations such as hospitals and insurance companies, while maintaining a General Data Protection Regulation-friendly posture, providing access to health data is a great importance for optimal patient assistance. To address both concerns, we present a framework featuring a multi-layer tool for providing a highly effective security solution specifically designed to address the eHealth requirements, and a blockchain access control component, based on smart contracts to provide access control for authorized users to patient records and health data in a distributed way.

Index Terms—eHealth, IoT, Security, Blockchain, Machine Learning, Access Control

I. INTRODUCTION

Nowadays, the expansion of IoT technology is notable in numerous areas, one of the most predominant being the Healthcare sector [1] - [6]. This exponential growth of IoT integration in this privacy-sensitive domain, has raised a lot of questions regarding the security aspect of smart applications [7], as vulnerabilities in smart equipment pose a significant threat against data privacy and patient safety. According to recent reports, over 93 percent of healthcare organizations have experienced a data breach in the last 3 years, with 57 percent of them reporting data breaches as a common incident with recurrence at least 5 times during the same timespan [8]. Furthermore, it is estimated that attacks targeting the healthcare infrastructure have increased by 125 percent in the last 5 years [9]. A research conducted by ENISA [10], provided a taxonomy indicating the most common threats smart hospitals may encounter, which are, namely, malware and ransomware, hijacking, tampering with medical devices, social engineering, device and data theft, and finally Denial of Service (DoS) attacks. At the same time, hospitals and remote healthcare are deemed unprepared to tackle cyberattacks, even to their simplest forms. Cyberattacks against critical infrastructures such as the eHealth sector can have very serious impacts [11], as compromising the availability of intelligent devices or controlling wearable medical devices can endanger patient lives [12] [13]. The recent incident of the September 10th 2020 cyberattack, targeting the Dusseldorf University Hospital, where hackers encrypted hospital systems thus resulting in the loss of human life is a tragic reminder that security in healthcare must be taken extremely seriously. As such, the integration of intelligent solutions aiming in timely detecting cyberattacks compromising medical assets is of essence in the healthcare domain.

In addition, resolving the issue of cross-border, cross-institution information sharing in a secure and private manner is of essence for transferring medical and health records of patients. Such data are characterized by their highly confidential nature, thus, access to such information should be granted to authorized staff only. However, cross-border incidents present challenges regarding the transferability of health
data, which are related to the lack of common access control mechanisms. Furthermore, integrity of data such as laboratory tests, medication, hospital admissions and radiology reports is crucial and any errors can affect patient health, insurance or employability [14]. Since data in smart hospitals are stored in a digital format, data protection and recovery is of great importance. For this reason, in this paper we suggest adopting blockchain technology to enable distributed access control and information sharing, in an immutable and private manner [15].

This paper undertakes the presentation of a novel machine learning and blockchain technology-enabled framework, capable of detecting cyberattacks against healthcare applications and allowing international patient information and health data exchange. The contribution of this paper is two-fold:

- This paper presents a multi-layer Healthcare-centric Security Information and Event Management (H-SIEM) framework utilizing machine learning and big data analytics, reputation mechanisms and visual-aided IDPS, focusing on eHealth services for rapid attack detection and prevention.
- Permissioned blockchain technology is utilized to enable cross-border medical information sharing, allowing distributed access control of multiple medical users.

The paper is organized as follows: in Section 2, related work is presented. The main methodology, offering detailed explanation of the framework is displayed in Section 3. Finally, in Section 4, discussion and trends will be described.

II. RELATED WORK

A lot of research has been conducted in order to analyse current cybersecurity issues and possible countermeasures in intelligent systems. The authors in [16] offer a view of limitations found in SIEMs, present specific attacks targeting Critical Infrastructures (CIs) and offer solutions that, if integrated in the future within a SIEM, could potentially detect and mitigate such malicious actions. Specifically, the danger and impact of Sleep Deprivation attacks targeting Wireless Sensor Network (WSNs), Distributed Denial of Service (DDoS) and GPS spoofing attacks in CIs was explored. For each scenario, possible countermeasures SIEM systems could adopt for quick attack detection were displayed. The insufficiency of usual security technologies against Advanced Persistent Threats (APTs) and Botnets targeting the smart grid was highlighted in [17]. Therefore, the authors suggest that solutions offered in tackling threats should have increased situational awareness. For this purpose, a comparison of three open-source SIEM tools, namely AlienVault OSSIM [18], Cyberoam iView [19] and CS Prelude [20] was conducted, in order to locate the best solution for use in situational awareness platforms. The evaluation of the aforementioned tools which involved the usage of Sahay and Gupta [21] software selection model, indicated that OSSIM was the most efficient according to the model used. Similarly to [17], the authors in [22] also support the idea of extensive situational awareness platforms for attack detection and mitigation in the smart grid. They explain the wide impact cyberattacks may have if executed against Industrial Control Systems (ICSs). To this end, the authors designed and implemented a Situational Awareness Network (SAN) platform, aiming in timely detecting threats targeting the infrastructure and decreasing their impact. The proposed SAN is organized in a 3-layer architecture, using sensors such as Host Intrusion Detection System (HIDS) and Network Intrusion Detection Systems (NIDS) for traffic monitoring as the first layer. The second layer integrates the OSSIM SIEM for data collection from the sensors, data normalization and transfer to the upper layer, which in turn handles the visualization of data in a dashboard, in a user-friendly way. Tests conducted indicate that the SAN operates as intended.

Apart from implementing SIEM solutions to secure the infrastructure, in the healthcare sector, it is crucial to consider access control to the confidential patient data, as in classifying the levels of data access individuals and organizations may have to such sensitive records. Specific research targeting Electronic Health Records (EHRs) and access control was conducted. In [23], a review of the three traditional security models for access control, namely Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC) was presented. Then, the access control requirements for EHRs were identified, and a possible scenario was presented, which indicated that all security models were inadequate to provide the required access control for EHRs. To this end, a conjunctive model was proposed, by carefully combining all three aforementioned models. Specifically, two MAC labels are introduced to classify the sensitivity of the data, a DAC-style Access Control List (ACL) is set by the patient in order to select their trusted medical practitioner and set a clearance for them, and finally the medical authority manages RBAC restrictions. The RBAC model is extended further in [24] to enable trans-organizational access control through distributed points. For this purpose, blockchain technology and smart contracts are exploited using the Ethereum [25] blockchain, thus forming the RBAC-SC model. The proposed solution is an effective and secure mechanism for role assignment and verification.

As noted in the previous paragraph, blockchain technology constitutes an efficient solution for information sharing and verification in distributed environments. In addition, machine learning and specifically anomaly detection is considered one of the most effective solutions for the development of contemporary Intrusion Detection Systems (IDSs). Thus, the integration of anomaly-based IDS in SIEMs is a viable option for effective threat detection. In the following paragraph, works combining machine learning and blockchain for security enhancement purposes are presented.

As highlighted in [26], the relationship between machine learning and blockchain has not been well-addressed in the past. The focus is on the integration of blockchain and machine learning for communications and networking systems, while open issues and challenges are discussed. Finally, the authors dive deeper into explaining how blockchain and machine learning can benefit from each other. Specifically, blockchain can benefit machine learning for data and model sharing, in a decentralized, secure and private way. On the other hand, machine learning can benefit blockchain for energy and resource efficiency, scalability, security and privacy and
intelligent smart contracts. In [27], the authors focus on resolving the security, privacy and technicality issues that rise with training a model on big data, on a central server. They propose training in a decentralized manner, using machine learning and blockchain. The participants form a peer-to-peer system and decide on the initial training parameters like the learning rate or the batch size. Then, data holders create random pseudo-identifications to protect their privacy and then proceed with creating their own model, using their own training data, with the last model update found on the blockchain. Their local gradient is encapsulated on a message, with their pseudo-identity, and broadcasted to computing users (miners), in order to compute the new global model. The new global model is finally added to the chain. The authors in [28] propose a novel anomaly detection solution for IoT that takes advantage of blockchain technology for the creation of an Extensible Markov Model (EMM) in a distributed environment. In essence, blockchain is used for the update of the anomaly detection model, in consensus with other similar Internet of Things (IoT) agents. All local trained models will be merged into a final global model. The challenges of training an anomaly detection model for IoT based on normal traffic are addressed, as it is difficult to simulate all possible scenarios in a testbed. Finally, a secure and fair method for model exchange in federated learning was introduced in [29]. Federated learning security is enhanced by integrating blockchain for model sharing, as blockchain can avoid the single point of failure problem. Fairness is enhanced by taking the contributions of participants into account. Specifically, the more a participant shares his local gradients, the greater his contribution; and the greater his contribution, the more gradients he can download, with each transaction recorded on the blockchain. Eventually, participants with the biggest contribution will get the most generalized model.

As noted, a lot of great research has been conducted for finding optimal solutions for enhancing data security and enabling distributed information sharing. As such, we aim to further contribute in the aforementioned research areas, specifically catering to eHealth requirements, by introducing a framework which enhances current security measures adopted by the healthcare sector by extending the capabilities of SIEMs, and allowing distributed access control and information sharing via blockchain technology.

III. METHODOLOGY

In contrast with traditional IT networks, where data confidentiality is considered the top security priority, in healthcare, availability and confidentiality are all considered equally important, therefore, the same weight should be given to all security aspects. However, the lack of sufficient security standards in the current eHealth systems, pose a significant threat for exploitation [30]. Specifically, the security tools used can be wrongly configured, underutilized due to the lack of training by medical personnel, or simply outdated [31]. The results of cyberattacks against eHealth infrastructures can be catastrophic, as not only highly personal and sensitive data could be exposed, but additionally, interruptions to service provision in smart hospitals threaten human lives. Furthermore, current SIEM solutions are unable to handle the enormous amount of data collected and exchanged by medical devices. Machine learning and specifically, anomaly detection solutions are needed in order to timely and accurately detect threats, a function that current SIEMs lack of.

To this end, we propose a Security Enhancing and Distributed Access Control (SEDAC) solution, a framework which is designed to elevate security levels to a higher standard, taking into account the copious requirements for eHealth applications. Specifically, we aim in enhancing the security of SIEMs, with the addition of big data analytics, reputation algorithms and visual-aided Intrusion Detection and Prevention System (IDPS), in order to detect any incidents that the SIEM failed to catch. SEDAC utilizes anomaly detection for all devices in the healthcare intranet and reputation assessment, thus devices, including legacy, will be continuously monitored and managed accordingly. Another crucial aspect for consideration, is the interoperability of healthcare services and information exchange between different hospitals, in different areas or countries. This is important as medical and health records and patient profiles should be exchangeable and presented in a common format for safer and better patient assistance, no matter their location. For this reason, we adopt permissioned blockchain technology in order to ensure private, secure, distributed and immutable information sharing, in the form of smart contracts. Since transactions will be registered on the distributed ledger, the single-point-of-failure issue is overcome. In addition, the integrity of the data is guaranteed due to the strong cryptographic nature of blockchain. By exploiting the benefits of this technology, cross-border information sharing between hospitals and other organizations is enabled. Figure 1 illustrates the added value of SEDAC integration.

![Fig. 1. Benefits of integrating SEDAC in healthcare.](image-url)

The interaction of the SEDAC’s components, is displayed in Figure 2, below. Specifically, the security solution proposed, named H-SIEM, monitors all system events, such as network traffic and system log information. Access control occurs via the usage of the Blockchain Access Framework, and specifically via the Ethereum Smart Contracts. In order to achieve user authentication and authorization, the RBAC model used in conjunction with Smart Contracts (RBAC-SC)
was found to be the best solution for distributed access control. This means that each role is authorized to access data until a certain level [32] [33], and blockchain is used to verify the roles. In addition, SEDAC access control will allow for cross-border and cross-institution information exchange, implying that hospitals, insurance companies etc., will be able to obtain medical information. Detailed explanation of the individual components’ function follows below.

A. H-SIEM

SIEMs are tools responsible for monitoring distributed systems and locating possible threats. They deal with a large amount of possibly heterogeneous log messages, collected from a plethora of devices, which are normalized, and correlated in order to provide a general view of the security status [34] [35]. Depending on the results of SIEM analysis, an operator can make informed decisions about the issued alerts.

This paper suggests the adoption of a 4-layer Healthcare-centric SIEM framework (H-SIEM), capable of detecting and preventing threats, anomalies and attacks against the healthcare system in a timely manner. The H-SIEM suggested, gathers information from multiple levels, and by analysing and correlating incidents, will provide appropriate countermeasures. For presenting this framework, an open-source log collector such as AlienVault’s OSSIM SIEM is suggested as the base layer. This will aggregate logs and network traces from the whole ecosystem, normalize them and produce alerts, if any. The big data analytics layer is used as a second security level, which will apply machine learning to the collected data such as logs, packets and system traces in order to timely locate any possible anomalies. Specifically, anomaly detection methods such as One Class-SVM, Isolation Forest, Angle-Based Outlier Detection and One Class Deep Neural Networks (Autoencoders and GAN architectures) will be utilized for this layer. A reputation system, which is used as the third layer, aids in the location of internal threats, by using reputation algorithms that provide statistical analytics, measuring the threat level and assessing the activity of each one of the entities composing the eHealth ecosystem by including voting among neighboring users. Such mechanisms allow locating threats originating from within the infrastructure. At last, a visual-based IDPS is added to the H-SIEM, which combines the results of the machine learning analytics layer and the reputation system layer and represents the current security status of the eHealth environment in a visual manner in order to detect any malicious acts. If any threats are located, the IDPS will attempt to mitigate the attack by suggesting various countermeasures to the operator such as node isolation. Figure 3 below depicts the function of the H-SIEM component presented in this section.

B. Blockchain Access Control

Distributed access to medical information is a requirement in order to provide optimal services to patients. However, transparency regarding the way data is handled is needed. This means that patients should have control of their information, by giving consents that regulate how their data should be handled by the healthcare providers. This ensures the solution suggested is in compliance with the GDPR regulations [36]. By using permissioned blockchain to enable access control to distributed databases via smart contracts, only verified participants will have access to data found on the aforementioned databases, as seen in Figure 2. Participants can have access to the chain by using their identity to confirm membership and access privileges. The blockchain acts as a distributed
database, where medical data collected and exchanged will be private and immutable, and only authorized users will have access to them. Moreover, by registering medical transactions on the distributed ledger, the single-point-of-failure problem central processing faces is dismissed.

IV. DISCUSSION AND TRENDS

As presented in Section 2, a lot of research has been conducted in order to secure the healthcare sector from malicious attempts against the network. The establishment of robust security systems for protecting eHealth is of significance, as data exchanged should remain confidential, and should be made available strictly to authorized users. The role of SIEMs has been investigated as a security solution, however, current SIEM systems present significant limitations. Specifically, they have a limited capacity of dealing with network heterogeneity [16], and they do not include real-time mitigation and prevention techniques to reduce the impact of the detected attacks [37].

Current eHealth systems usually employ the RBAC model for access control to restricted patient information [38]. With the implication of IoT technology in healthcare, RBAC is not as efficient as IoT devices can change roles continually, thus the allocation of access control privileges is complicated. In addition, the RBAC model does not take into account the patient’s right to their own data, therefore, is not a GDPR-friendly solution.

To tackle the limitations of the security aspect, the H-SIEM framework was presented, featuring a multi-layer approach to current SIEM solutions, focused specifically in the needs of the healthcare domain. The function of open-source SIEMs can be enhanced by appending more detecting layers above it. Anomaly detection is a machine learning technique frequently adopted for the creation of robust IDS, thus the addition of an anomaly detection layer with deep-packet inspection capabilities will detect threats in real time for this sector where time criticality is of essence. Furthermore, the integration of a reputation system which assesses the activity and threat level of each device in the ecosystem aims in timely recognizing any deliberate or accidental attacks, therefore, optimizing the detection process. Analysis results displayed visually, will help the operator come to a conclusion about the current security status. Mitigation techniques are of great importance when considering the creation of effective security tools, catering to critical ecosystems’ needs. To that end, we highlight the vitality of implementing a response mechanism through this layer, which will address the threats detected with various mechanisms, such as malicious node isolation.

Cross-border information sharing, especially of medical and health data, is a concept that can be life saving for patients. Blockchain technology can be used as a distributed database for EHRs, however, access to such sensitive data should be restricted to authorized personnel only. By coupling blockchain technology and RBAC model, access control in a distributed manner can be realized. Specifically, by using smart contracts as displayed in [24], and assigning specific roles to users, distributed access control and information sharing can be achieved as access to data found on the chain will be granted to users with specified roles. By using permissioned blockchain, non-repudiation is achieved in the healthcare domain, and the immutability and confidentiality of health data logged in the distributed ledger is ensured. In addition, GDPR rules establish that the data subject should have full control of their data; to this end, we follow a transparent methodology regarding the handling of patient data, to achieve GDPR-compliance.

An important consideration that needs to be taken into account when designing an effective security platform is the evaluation methodology. Specifically, we present actions that can be performed in order to validate the effectiveness of the implemented framework. In order to assess the efficiency of the H-SIEM, we suggest deploying various attacks against the protected infrastructure. Malicious actions should include common cyberattacks launched against intelligent hospitals, such as DoS, zero-day attacks and malware. All traffic produced can be forwarded to the H-SIEM component, where its reaction against these attacks will be monitored and evaluated. Experience gained from each cyberattack will allow the enhancement of the defences, by updating firewall rules, for instance. Man-In-The-Middle attacks and false data injections targeting wearable technology can be executed as well, aiming in the assessment of the H-SIEM’s anomaly detection layer.

In order to validate the distributed access control framework proposed, we suggest following the scenario described below: Suppose information sharing between institutions is required. The patient is located in hospital A in a different country, while hospital B, holds the patient’s health information. Said patient is required to get laboratory tests for further diagnosis. The patient certifies that the involved medical personnel of institution A such as doctors and nurses are authorized to access the records. Then, the patient certifies the laboratory equipment, such as the blood analyser which will handle their clinical data. At last, the patient authorizes medical personnel and laboratory equipment to share data between them and his/her healthcare providers. As such, the patient’s health profile is encrypted and shared from hospital B to hospital A, where the certified medical personnel can access the health data and create a list of transactions, such as blood tests. The patient then authorizes personnel for the transactions, which concludes the distributed access control process. In case hospital B wants to update the medical profile of the patient, a new transaction would have to be performed, so the patient would have to authorize the personnel of hospital B to access their health data from hospital A.

V. CONCLUSIONS

The purpose of this paper was to introduce a security-enhancing framework with respect to eHealth applications’ requirements. To that end, we design a multi-layer H-SIEM framework, featuring 4 security levels, including a SIEM, anomaly detection techniques, reputation algorithms and visual analytics in order to timely recognise if an attack is under execution against the system thus proposing the appropriate countermeasures. Furthermore, information sharing between different countries and institutions is a focal point of this paper, thus the design of a blockchain-enabled framework utilizing Smart Contracts and RBAC for healthcare applications was
realized. The framework resulting from the combination of the aforementioned components can be a viable and efficient solution for strengthening security in the extremely critical healthcare sector, and enabling distributed information access. By addressing both concerns contemporary healthcare systems may face, we suggest an attractive and efficient service, specifically designed for eHealth environments.

VI. ACKNOWLEDGEMENT

The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957406.

REFERENCES

[1] Zhou, L., Jianxin Chen, Baoyu Zheng, de la Torre, I., and Misra, S. "On asynchronous flow scheduling for wireless body sensor networks," 2013
[2] Roy, S. K., Misra, S., and Raghuvanshi, N. S. "SensPnP: Seamless Integration of Heterogeneous Sensors with IoT devices," 2019
[3] S. Bera, S. Misra, S. K. Roy, and M. S. Obaidat, “Soft-WSN: Software-Defined WSN Management System for IoT Applications”, IEEE Systems Journal, vol. 12, no. 3, pp. 2074-2081, Sept. 2018
[4] Mustafa Abdullah Azzawi, Rosilah Hassan, and Khairul Azmi Abu Bakar, "A Review on Internet of Things (IoT) in Healthcare," 2016.
[5] Anna Triantafyllou, Panagiotis Sarigiannidis, and Thomas D. Lagkas, "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends," 2018.
[6] S. Misra, S. Sarkar, “Priority-Based Time-Slot Allocation in Wireless Body Area Networks During Medical Emergency Situations: An Evolutionary Game Theoretic Perspective”, IEEE Journal of Biomedical and Health Informatics, Vol. 19, No. 2, March 2015, pp. 541-548.
[7] jenna, A., and Eddine Saidouni, D. "Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure," 2018.
[8] (2020) herjavecgroup [Online]. https://www.herjavecgroup.com/wp-content/uploads/2019/12/Healthcare-Cybersecurity-Report-2020.pdf
[9] Chon Abraham, Dave Chatterjee, and Ronald R. Sims, "Muddling through cybersecurity: Insights from the U.S. healthcare industry".
[10] Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures, ENISA, 2016
[11] Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," 2018.
[12] Eric D. Perakslis, "Cybersecurity in Health Care,".
[13] Katherine Booth Wellington, "Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions".
[14] Ensuring Data Integrity in Health Information Exchange, AHIMA Thought Leadership Series, American Health Information Management Association, 2012 p.2
[15] Ziben Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends".
[16] G. Cerullo, V. Formicola, P. Iamiglio and L. Sgaglione, "Critical Infrastructure Protection: having SIEM technology cope with network heterogeneity", arXiv preprint arXiv:1404.7563, 2014.
[17] R. Leszczyna and M. Wrobel, "Evaluation of open source SIEM for situation awareness platform in the smart grid environment", IEEE World Conference on Factory Communication Systems (WFCS), 2015.
[18] "OSSIM: Open Source SIEM." [Online]. Available: http://www.alienvault.com/open-threat-exchange/projects"
[19] "Cyberoam iView : The Intelligent Logging Reporting Solution." .
[20] "Prelude-IDS: Prelude Universal Open-Source SIEM project.".
[21] B. S. Sahay and a. K. Gupta, “Development of software selection criteria for supply chain solutions," Ind. Manag. Data Syst., vol. 103, no. 2, pp. 97–110, 2003.
[22] R. Leszczyna, R. Malkowski and M. Wróbel, "Testing Situation Awareness Network for the Electrical Power Infrastructure", Acta Energetica, vol. 28, no. 3, pp. 81-87, 2016
[23] Alhqabani, Bandar and J. Fidge, Colin. (2007). Access Control Requirements for Processing Electronic Health Records
[24] J. P. Cruz, Y. Kaji and N. Yanai, "RBAC-SC: Role-Based Access Control Using Smart Contract," in IEEE Access, vol. 6, pp. 12240-12251, 2018. doi: 10.1109/ACCESS.2018.2812844
[25] (2020) Ethereum. [Online]. https://ethereum.org/en/