Blockchain uses for Fog computing security

Darius Rudzika
Faculty of Informatics
Kaunas Technology University
Kaunas, Lithuania
darius.rudzika@ktu.lt

Prof. Dr. Algimantas Venčkauskas
Faculty of Informatics
Kaunas Technology University
Kaunas, Lithuania
algimantas.venckauskas@ktu.lt

Abstract—**Efficient and secure IoT device network communication with Cloud and security aspects of IoT devices management is an ongoing issue for quite some time. In this article we cover: a) The concept of Fog network and why we need it for efficient IoT connectivity; b) Inherent security threats of IoT networks and devices; c) Existing security implementations in IoT frameworks; d) Blockchain technology principles; e) Blockchain based solutions to implement IoT device and Fog network security framework. In Fog network part we cover IoT communication shortcomings and how they are solved using Fog networks. Further we cover most common security threats for IoT devices and networks. Then we look in to existing IoT frameworks security implementations. Further we give a short introduction to Blockchain technology and propose our solution how it can be exploited to secure Fog network and connected IoT devices.**

Keywords- Blockchain, Fog computing, Internet of Things, Edge computing, Security

I. Introduction

The world is experiencing the sprawl of connected smart devices, that are now becoming one of the main factors of commodity computing. Active development of wearable computing, connected vehicles, smart city, smart home, smart metering and variety of industrial large-scale wireless sensor network focuses the attention on the Internet of Things (IoT). This development of Internet of Things (IoT), Cyber-Physical System (CPS) and Mobile Internet, various objects, including people, machines, things, where everything is connected into information space at any location and at any time is considered a future of the Internet.

The amounts and types of data that is being generated regularly exceeds the futurist forecasts. According to the estimation and prediction of Cisco, there are more than 50 billion devices which will be connected to the Internet by 2020. And the data produced by people, machines, things and their interactions will reach 500 zettabytes, and 45% of IoT-created data will be processed, analyzed and stored at the edge of network by 2019 [1].

With the rapid growth in the amount of data, the speed of data generation is also increasing drastically. The huge data volumes result in that today's processing and storage capabilities cannot meet the demand and it is difficult to be handled by traditional computing models. For example, Cloud computing has been used as a de facto way to process IoT generated data because of its high computation power and storage capability. However, as Cloud computing is a centralized computing model, the computation must happen in the cloud. Therefore, this means that all the data for processing and requests need to be transmitted to the Cloud. While the data processing speed in the Cloud has risen with a fast pace, the network uplink bandwidth to the Cloud has not increased with the same rate.

Given this situation the Cloud uplink bandwidth became a bottleneck for IoT implementations, in response new concepts were proposed to solve this problem at the edge network.

Fog computing, which integrates network edge and cloud core, was presented as a more effective solution to enable address these limitations. Fog Computing is a new paradigm that extends the Cloud Computing to the edge of the network. It tackles the inherent Cloud Computing issues such as high latency, lack of mobility support and lack of location-awareness. Fog computing supports mobility, computing resources, communication protocols, interface heterogeneity, cloud integration, and distributed data analytics to address requirements of applications that need low latency with a wide and dense geographical distribution [2].

While Fog computing solves the aforementioned problems it still inherits the same security problems that are present in IoT infrastructures. The legacy of the client-server approach to IoT communications, drags the gamut of the known security problems that have to be solved in Fog computing space as well.

We see potential in recently popular Blockchain technology [3], especially the distributed nature of it, for solving the Fog computing security problems. While gaining its popularity in cryptocurrency and crypto-assets space the Blockchain technology can be used in variety of use cases, where decentralization, location independence and communication between untrusted parties is required.

This paper covers the IoT connectivity shortcomings that led to inception of Fog computing; Fog computing concept; Fog computing security problems and the proposed solution. This is the first communication of our work, which is aimed to develop Blockchain based Security Model for Fog computing.

II. The concept of using Fog network for efficient IoT devices connectivity

The term "Internet of Things" (IoT) was originally coined by Kevin Ashton in 1999 during a presentation on supply-chain management [4].

Today IoT is still considered an emerging paradigm with underlying vision that promises ubiquitous computing where "Things" and people are connected in an immersive networked computing environment, where "Things" provide utility service to people, enterprises and their digital shadow, through intelligent services. IoT envisions a new world of connected devices and humans in which the quality of life is enhanced because management of city and its infrastructure is less cumbersome, health services are conveniently accessible, and disaster recovery is more efficient. At purely technical infrastructure level the Internet of Things (IoT) paradigm promises to make “things” including consumer electronic devices or home appliances, such as medical devices, fridge, cameras, and sensors, part of the Internet environment [5].

Because of limited storage and computational resources on "Things" in its original architecture IoT considers Cloud as an elastic primary source of computing power and storage. Cloud computing frees the service provider and the end-user from solving of many service-enabling details. However, this becomes a problem for latency-sensitive applications, that require resources in the vicinity of the device to meet service requirements. The latest generations of IoT devices demand for mobility support, geo-distribution, low latency and location awareness [6].

By its own nature IoT devices, sensors and other "Things" are highly distributed at the edge layer of the network along with real-time and latency sensitive requirements, while Cloud data-centers are geographically centralized. Because of such architecture Cloud often fails to satisfy capacity, though-put and processing demands of billions of IoT "Things". This often leads to congested network, high latency and poor Quality of Service [7].

To address these technological gaps, the IoT demanded a new architecture known as Fog computing.

Fog computing is an emergent computing paradigm that extends cloud computing to the edge of networks and makes it virtually appear closer to Device (a.k.a. Thing). It is a virtualized platform that provides computing, data storage, and networking services between end devices and traditional Cloud Computing Data Centers, usually located at the edge of network [6].

Fog network provides low latency, location awareness and improves quality-of-services (QoS) for streaming and real time applications. Fog computing provides the cloud an alternative method to handle large amounts of data generated daily from the Internet of Things. When data is processed closer to where it is produced and used, it better deals with the challenge of exploding data volume, variety, and velocity.

Typical implementation examples include industrial automation, transportation, networks of sensors and actuators, augmented reality devices. Worth mentioning that, this new paradigm supports heterogeneity as Fog devices is a wide spectrum of end-user devices, access points, edge routers and network switches [8].

While Fog and Cloud provide the same resources (networking, compute, and storage), and share many of the same mechanisms and attributes (virtualization, multi-tenancy) the Fog network extension is a non-trivial replication of same functions from Cloud to Edge. When compared to Cloud computing, Fog computing puts emphasis on factors such as proximity to end-users, alignment to client objectives, resource geographical distribution and local pooling, communication latency reduction and bandwidth savings to achieve better quality of service (QoS), resulting in improved user-experience and improved redundancy in case of failures.

Fog computing can be presented as three-layer hierarchical architecture: Cloud - Fog - End Nodes.

The most time (latency) sensitive data is analyzed on the Fog node closest to the End Nodes generating the data. Data that can wait seconds or minutes for action is passed along to an aggregation node for analysis and action. Data that is less time sensitive is sent to the Cloud for historical analysis, Big Data analytics, and long-term storage.

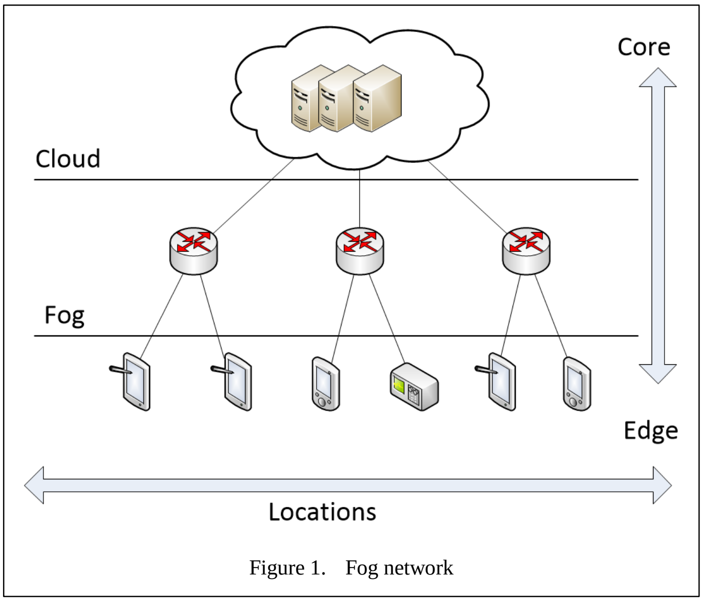

Figure 1. Fog network

III. Inherent Security Issues of IoT Devices and Fog Networks

Being a non-trivial extension of cloud computing, fog computing is expected to be more secure than traditional Thing - Cloud (Client - Server) architecture. The features that add on to security of Fog are - "local" data storage and independence from continuous internet connection. Not having persistent connection to device from internet also adds extra protection from Internet originated attacks.

While having the potential of improved security the Fog network still cannot be considered to be secure, because it inherits security risks from traditional IoT networking and communications to Cloud. For example, the IoT devices have constrained computing, storage and battery resources, hence cannot hold modern security features. Often being publicly accessible IoT devices are easy to be hacked, broken or stolen. IoT devices and services expand the surface area for cyber-attacks on businesses, by turning physical objects that used to be offline into online assets communicating with enterprise networks. Businesses will have to respond by broadening the scope of their security strategy and solutions to include these new online devices.

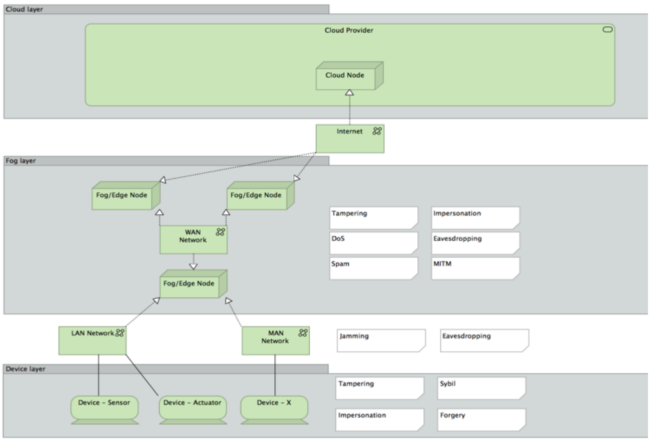

Figure 2. Inherent security issues in Fog networks

Different problems are brought by Cloud computing. While having unlimited resources, Cloud is vulnerable to external attacks, mostly because of the centralized data storage and computing framework. Attacks are often successful because of misconfiguration of services when consumed by inexperienced users.

The current IoT ecosystems rely on centralized, brokered communication models, otherwise known as the Client-Server. All devices are identified, authenticated and connected through cloud servers that hold large processing and storage capacities. Connection between devices have to exclusively go through the internet, even if they happen to be a few feet apart.

Existing brokered cyber security solutions based on Client-Server model are no longer adequate for addressing security challenges in the emerging Fog computing.

The existing modern security technologies play a role in mitigating IoT risks, but they are not enough. The primary goal is to get data securely to the right place, at the right time and in the right format.

The most common issues and attack type inherited from brokered communications model are listed in Table 1.

TABLE I. ATTACK TYPES

Risk	Description
Forgery	The attacker may forge the data collected or transmitted by the IoT device, attacker also may forge their identities and user profiles
Tampering	The attacker may maliciously drop, delay or modify transmitting data to disrupt the services or degrade service efficiency.
Spam	In general sense spam definition refers to the unwanted or unrequested content, such as excessive information or misleading information, false collected data from users, which is generated and spread by attackers.
Sybil	The attackers either manipulate fake identities or abuse pseudonyms in order to compromise or control the effectiveness of Fog computing
Jamming	This attack is mainly directed at the communication channels, the attacker generates a huge of bogus messages to jam communication channels or computing resources, such that other users are prohibited from normal communication or computing resource usage.
Eavesdropping	Attacks, when data on communication channels can be captured and contents examined for valuable information.
Denial of Service	DoS and DDoS attacks are very common in IoT space, they can be put in action exploiting large numbers vulnerable IoT devices or IoT devices can fall as targets of the attacks.
Man-In-The-Middle	A malicious attacker stands in the middle of two parties to secretly relay or modify the exchanging data between these parties.
Impersonation	Attacker pretends a legitimate user to enjoy the services provided by fog nodes or impersonates a legitimate fog node.

IV. EXISTING SECURITY IMPLEMENTATIONS FOR IOT FRAMEWORKS

There has been a tremendous effort in recent years to cope with security issues in the IoT paradigm. Some of these approaches target security issues at a specific layer, whereas, other approaches aim at providing end-to-end security for IoT. We'll concentrate on the pillar security features - Authentication, Authorization and Access Control and Secure Communications [9], [10].

A. *Authentication*

X.509 certificates are the most popular method to verify identity in IoT infrastructures. X.509 are digital certificates that depend on the public key cryptography and are issued by a trusted party called *a Certification Authority* (CA). These certificates are SSL/TLS-based to ensure secure authentication. Certificates can be used for mutual authentication between client and server or for client authentication only.

OAuth/ OAuth2 are another popular authentication protocol option. While OAuth is an authorization protocol it is often used on its own as an authentication method that may be referred to as pseudo-authentication. Generally, OAuth provides to clients a "secure delegated access" to server resource on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials.

B. *Authorization and Access Control*

The authorization in IoT frameworks is often policy based, this means that only devices or applications specified in policy rules can have access to the corresponding resource.

This may be implemented using the rules engines, directory services (Active Directory, LDAP) or local authorization methods such as flat file databases or JSON format files.

Access Control implementations varies from kernel based (SELinux), sandboxing of device or separate applications within device or traditional operating system UID, GUID schemas.

C. *Secure Communication*

IoT application communication protocols as those of HTTP, MQTT, CoAP, or XMPP, or even protocols related to routing as those of RPL and 6LoWPAN, are not secure by design. Such protocols have to be wrapped within other security protocols such as SSL/TLS or TLS/DTLS for messaging and application protocols to provide secure communication.

SSL/TLS is a de facto standard communication channel for World Wide Web and another network communication. When used in IoT context it ensures confidentiality for the application protocols such as MQTT, HTTP. This approach requires least implementation effort because of widely applied standards and is available out of the box in most development environments.

TLS/DTLS combination is popular where devices have limited capacity and computing power. It *provides* security mechanism in order to secure and protect communication, by supporting Transport Layer Security (TLS) and the related Datagram TLS (DTLS) protocol. DTLS is often more suitable for lossy, non-persistent IoT network communications. Both protocols are the state of the art standards for securing communication over the World Wide Web. This means preventing eavesdropping, tampering and message forgery and ensuring integrity.

Both protocol combinations can use spectrum of cyphers which are often selected as per manufacturers discretion, most popular options being AES-128-GCM and SHA-256.

V. Blockchain Principles and Applications

By definition, Blockchain is a trusted, distributed ledger which has a shared set of processes across all the members of the network. This ledger is replicated through peer-to-peer replication technologies across all the different members of this network. Modern blockchain for services is usually made out of four core components.

The first is the shared ledger - an append only distributed system of records that is used and shared across the network.

Second - privacy services to control who can see what across the network and to maintain property of immutability across the blockchain.

The third - trust, achieved through consensus, provenance, immutability and finality.

The fourth is a smart contract - the way that the add-on service logic is actually embedded in the blockchain. Often a smart contract is taking the terms of a traditional contract, encoding them up in the form of shared process and sharing them around blockchain network.

Technologically at the base of the Blockchain concept is the cryptographic hash function. The typical hash function takes any size string as input and produces a defined fixed-size output. The hash function has to be efficiently computable, so the output can be calculated in reasonable amount of time.

The Blockchain suitable hash function must meet certain security properties. Hash function has to be:

- collision free, meaning no two input strings can generate identical hashes.
- hiding, meaning the initial string data cannot be regenerated from its hash output.
- puzzle-friendly, meaning part of hash function input has to be chosen in a suitably randomized way, that it's very difficult to find another value that hits exactly same input if attempted to calculate.

Blockchain is similar to linked list of series of blocks and each block has data as well as a pointer to the previous block in the list. On the blockchain the previous block pointer will be replaced with a hash pointer, so it defines where it is and what the value of previous block was. This turns a linked list in to a tamper evident log - a structure that stores data. So, we can add data onto the end of the log and if attacker later modifies data that is in the log we're going to detect it, because the hash pointer chain will be incorrect. To go unnoticed the attacker would need to recalculate all hash pointers down to the first (genesis) block in the list and that’s where hiding properties and puzzle-friendliness of the hash algorithm plays its role by complicating the hash recalculation process.

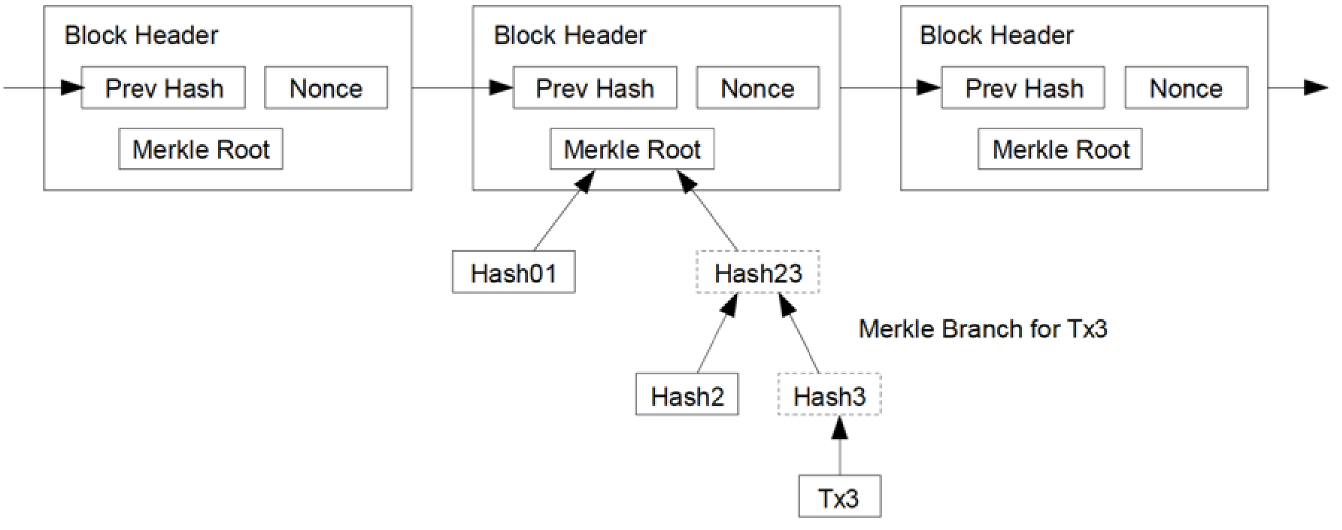

Figure 3. Blockchain and Merkle tree [3]

VI. Blockchain technology based solution to improve IoT device and Fog network security

A. Authentication

We propose using PUF (physical unclonable function) to provide a unique identity string for device and further use it to derive a device-unique cryptographic key, which would be used to perform service actions on the blockchain.

B. Authorization and access control

For our solution we selected to use private blockchain (ledger database) to keep the IoT device accounting information, authorize the devices and manage access control. We selected the – Proof-of-Authority consensus model for the solution. In Proof-of-Authority based networks, transactions and blocks are validated by approved accounts, known as validators. This way the managing organization retains control over the infrastructure.

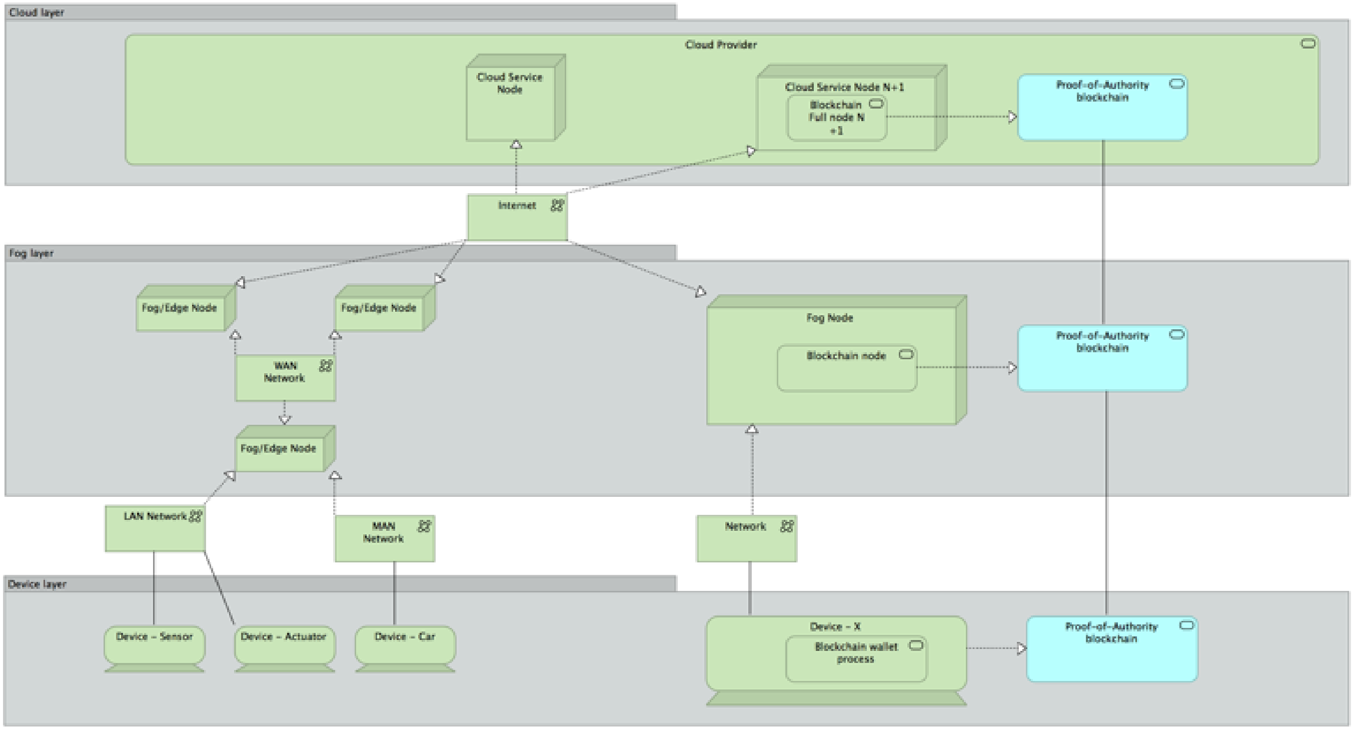

Figure 4. Blockchain implementation for Fog network security management

The proof of concept implementation is based on open source Hyperledger project software [13]. The Cloud layer nodes run Full node (full copy of the Blockchain), the Fog nodes run partial copy of the blockchain holding the copies of the most recent blocks and interface communications to the Things device layer. The Things run the lightweight client.

C. Secure communication

We selected to use telehash [14] - lightweight interoperable protocol with strong encryption to enable mesh networking across multiple transports and device platforms. Each telehash endpoint generates its own unique public-key based address (a hash name) to send and receive encrypted packets of JSON (with optional binary payloads) to other trusted endpoints. An endpoint may also provide routing assistance to others for bridging across different transports and to help negotiate direct peer-to-peer links. Because Fog layer and IoT devices create a mix of location independent endpoints and different device platforms the telehash protocol seems to be well suited for IoT communication.

D. Lifecycle

The blockchain is well suited for device lifecycle management. We will use Hyperledger blockchain to create a lifecycle records system where devices can be enrolled at the time of manufacturing or at the time of first deployment and can store information such as unique device ID, firmware version, ownership information, location, maintenance log. The framework security engine will use this information to enforce the security policies i.e. authorize only devices with the right level of firmware.

VII. Conclusion

Fog computing is a decentralized architecture that improves upon the Cloud Computing concept by extending storage, computing and networking resources to the network edge - closer to IoT devices. This enables support of spectrum of large-scale, low latency IoT applications, such as augmented reality or smart city transportation. However, Fog networks have inherent security threats, which raise various security and privacy challenges towards users and technology adopters. In our work we propose to use Blockchain technology-based solution to address the security challenges.

VIII. FUTURE WORK

The further tasks we consider in our work are as follows:

- Develop the Blockchain based security model for Fog computing.
- Develop identification and authentication method and services on the blockchain.
- Develop authorization and access control method and services on the blockchain.
- Develop IoT device lifecycle services on the blockchain
- Evaluate how proposed model responds to security challenges
- Evaluate how the proposed model responds to the heterogeneity issues, energy consumption and adoption to the limited End-Nodes computing resources.

REFERENCES

[1] Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper. Available at: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html

[2] A.V. Dastjerdi, H. Gupta, R.N. Calheiros, S.K. Ghosh, R. Buyya, Fog Computing: principles architectures, and applications. 61–75 In Internet of Things. Elsevier, 2016

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

[4] K. Ashton That 'Internet of Things' Thing, RFID Journal 2009, Available at: http://www.rfidjournal.com/articles/pdf?4986

[5] R. Buyya, A.V. Dastjerdi. Internet of Things, Principles and Paradigms. Elsevier, 2016

[6] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, In Proceedings of the first edition of the MCC workshop on Mobile cloud computing - MCC 12. ACM Press, 2012.

[7] S. Sarkar, S. Misra, Theoretical modelling of fog computing: a green computing paradigm to support IoT applications, IET Networks 5, 23–29 Institution of Engineering and Technology (IET), 2016

[8] I. Stojmenovic, S. Wen, X. Huang, H. Luan. An overview of Fog computing and its security issues. Concurrency and Computation: Practice and Experience 28, 2991–3005 Wiley-Blackwell, 2015

[9] M. A. Khan, K. Salah. IoT security: Review blockchain solutions, and open challenges. Future Generation Computer Systems 82, 395–411 Elsevier BV, 2018

[10] M. Ammar, G. Russello, B. Crispo. Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications 38, 8–27 Elsevier BV, 2018

[11] N. Kshetri, Blockchains roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy 41, 1027–1038 Elsevier BV, 2017

[12] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future to Internet of Things security: A position paper. Digital Communications and Networks Elsevier BV, 2017

[13] Hyperledger project, Available at: https://www.hyperledger.org

[14] Telehash protocol, Available at: http://telehash.org