Journal of Electrical Engineering and Information Technologies, Vol. **5,** No. 1, pp. 39–46 (2020)
Article 170 ISSN 2545–4250
Received: April 15, 2020 e: ISSN 2545–4269
Accepted: May 2, 2020 UDC: 004.75.056.55:004.455

Original scientific paper

IMPROVING SECURITY IN CLOUD COMPUTING WITH BLOCKCHAIN – USE CASES –

Martina Janakieska[1], Tomislav Šuminoski[2]

[1]*Ericsson Telecommunications, Skopje,*
Mito Hadživasilev Jasmin, No. 7, 1000 Skopje, Republic of North Macedonia
[2]*Faculty of Electrical Engineering and Information Technologies,*
"Ss. Cyril and Methodius" University in Skopje,
P.O. box 574, 1001 Skopje, Republic of North Macedonia
tomish@feit.ukim.edu.mk

A b s t r a c t: Network security has always been and remains a major topic in telecommunications and information technologies. Security plays a key role in a network and therefore it is very important to take appropriate measures to protect user data. In addition to standard protocols and security mechanisms, there are many researches and experiments with current blockchain technology. This paper presents several user scenarios for improving security in cloud computing when using blockchain and how this technology can help in cyber security within the cloud systems. Moreover, for cloud computing, we have proposed our solution, based on many analyses over different solutions, which provides higher degree of data protection and, what is important, it does not load the IoT network and IoT devices.

Key words: BaaS; blockchain; cloud; IoT; security.

ПОДОБРУВАЊЕ НА СИГУРНОСТА НА CLOUD ПРЕСМЕТКИТЕ СО BLOCKCHAIN – КОРИСНИЧКИ СЛУЧАИ –

А п с т р а к т: Мрежната сигурност отсекогаш била и останува да биде главна тема во телекомуникациите и во информациските технологии. Сигурноста игра главна улога во мрежата и затоа е многу важно да се преземаат соодветни мерки за да се заштитат корисничките податоци. Како дополнение на стандардните протоколи и постојните сигурносни механизми, постојат многу истражувања и експерименти со постојната blockchain технологија. Во овој труд се претставени неколку кориснички сценарија за подобрување на сигурноста на cloud пресметките, кога се користи blockchain, исто така е дадено како оваа технологија може да помогне за сајбер безбедноста и сигурноста во самите cloud системи. Воедно, за cloud пресметките, врз база на многу анализи од многу различни решенија, предложивме и наше решение,кое обезбедува поголемо ниво на заштита на податоци и што е најважно, тоа не ги оптоварува IoT-мрежите и IoT-уредите.

Клучни зборови: BaaS; blockchain; cloud; IoT; сигурност

1. INTRODUCTION

As technology in real world, blockchain begins to evolve few years ago, and it's supposed, that now, blockchain is changing the way IT works. Based on a peer-to-peer topology, blockchain is a distributed ledger technology that allows data to be stored globally on thousands of servers – while letting anyone on the network see everyone else's entries in near real-time. This makes difficult for one user to gain control of the network.

Blockchain can be implemented in cloud technologies to avoid problems with security. As we know, cloud is centrally organized structure, and using blockchain can provide higher security compared to storing all data in a central database like cloud servers. From the data storage and management aspect, damage from attacks on a database can be prevented. Moreover, since the blockchain has an openness attribute, it can provide transparency in data when applied to an area requiring the disclosure of data. Due to such strengths, it can be utilized in

diverse areas including the financial sector and the Internet of Things (IoT) environment and its applications are expected to expand. Cloud computing is based on Internet computing and can provide scalable services on user's demand. Using cloud computing, users can obtain hardware or software on demand, same for other computing resources.

The remainder of this article is organized as follows. Section 2 gives an overview and key concepts of cloud computing. Section 3 presents blockchain technology basic functions. Section 4 provides description of a secure blockchain solutions implemented in cloud computing. In section 5, we provide our solution based on analysis of many different solutions and models. Finally, the last section conclude the paper and gives some future works.

2. KEY CONCEPTS OF CLOUD COMPUTING

Cloud computing can be defined as Internet-based computing that provides multiple scalable on demand services through sharing or accessing computing resources. Those resources are coming from private systems or third-party, and users can access them locally or remotely. Using cloud means users can elastically obtain hardware, software, or other computing resources on demand. As a scalable and flexible solution, cloud computing can combines a new technologies and paradigms with existing technologies. Also, cloud usage is steadily increasing. A research [1] shows that only 20% of the workload is in the public cloud. Using cloud networks provides location-independent access and many companies are migrating to cloud, and many of them adopt SaaS cloud service model. We mentioned a service model, therefore, the basic cloud service models are listed bellow. First to define what is a service model in cloud. A service model in cloud computing refers to an agile approach of a delivering specific services that can properly meet the customer demands. Three fundamental cloud service deployments are [2]:

1. Infrastructure as a Service (IaaS) – a service model that enables end users to acquire virtualized computing resources, such as hard drives, processors and memory cards, from cloud providers. IaaS is the first layer of the layer structure. It implies that IaaS is the foundation of cloud computing.

2. Platform as a Service (PaaS) – a service model that allows web developers to utilize a complete virtualized platform for the purpose of application or platform development. This service model consists of a number of subsystems and interfaces within a common structure, involving a stream of relevant product development procedures.

3. Software as a Service (SaaS) – also known as Application-as-a-Service, which refers to leveraging cloud-based software solutions to provide users with web-based software, platform, and infrastructure services. Similar to IaaS and PaaS, the hardware or software can be hosted by a third party.

Expect those three basic cloud computing service models, there are some more specific cloud computing service models as:

- Desktop as a Service
- Storage as a Service
- Database as a Service
- Backend as a Service
- Information as a Service
- Integration as a Service
- Security as a Service
- Blockchain as a Service (Blockchain-as-a-Service, or BaaS, is a managed blockchain platform allowing users to build blockchain applications and digital services on a distributed network while the vendor supplies infrastructure and blockchain building tools), presented in Figure 1.

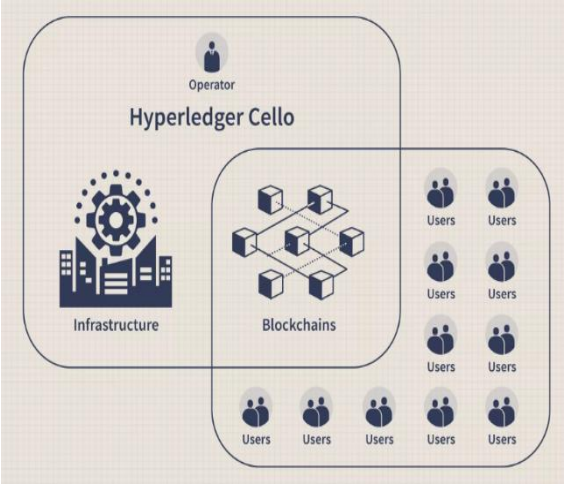

Fig. 1. Blockchain-as-a-Service

a) *Different types of cloud*

This section gives a brief description of the four main types of clouds [2]:

1. *Public cloud* – A public cloud is hosted or operated by a service provider who sells or offers a multitude of services to the public. This may include multicloud which combines public cloud services from multiple vendors.

2. *Private cloud* – is owned or leased by an individual organization and is only operated or served for the private use of the individual organization.

3. *Community cloud* – A deployment model that enables several organizations to host cloud infrastructures and sell or offer cloud services to a specific group of organizations. Therefore, the cloud-based computing resources are shared within a community with similar interests.

4. *Hybrid cloud* – A deployment model that merges two or more cloud service deployments, such as the private, public, and community clouds. A hybrid cloud consists of at least one private cloud and at least one public cloud.

b) *Cloud security*

Cloud offers various forms of security to keep user's data safe and to protect their integrity, such as data classification, encryption forms, etc. But despite of that, security plays an important role when switching to a cloud solution, and some users are worried about cyber attacks and crimes. According to IEEE [3], a cybersecurity hack occurs every 39 seconds on average. Security is increasingly recognized as something that customers care about, and because of that, products, solutions and services with more security features available are required. Cloud computing is technology based on centralization. This makes cloud networks/storage to be target to many attackers. As a secured and distributed ledger, blockchain can help resolve many of the cyber security issues related to centralization. Furthermore, the next section presents few facts about blockchain and what makes this technology special.

3. BLOCKCHAIN TECHNOLOGY

Blockchain's primary goal is to free people from any form of trust they are now forced to give to intermediaries who regulate much of the user's data. Blockchain is actually a distributed, consensus-based database system that allows the transfer of values between entities. There are many consensus-based distributed systems, but only blockchain has the following three properties:

(1) *Trustless*: There is no need to have a certified digital identity. The entities involved do not know each other, but can exchange data without knowing their identities.

(2) *Permissionless*: No one decides who may or may not work on the blockchain network. There are neither permissions nor controllers, and ultimately.

(3) *Sensorship resistant*: Entities only believe in the quality of the cryptographic algorithms and hash functions that govern the operation. Anyone can transact in the network. The transaction, once sent and accepted, cannot be stopped or censored.

Mainly, the blockchain technology is based on four central concepts: (1) peer-to-peer network, (2) open and distributed ledger, (3) synchronization of ledger and (4) mining.

In mining process, miners are the only nodes in the network that can add transactions in the chain. They compete over who will take the transaction first and put it into the chain. For this purpose a mathematical problem is solved ant it's called Proof of Work, it is kind of reverse hash operation. All of these characteristics makes blockchain specific network security tool that separates it from the rest.

As it is well known, the blockchain works with transactions, therefore, blockchain transactions in cloud would be user data. Everything that happens to data, whether transport, processing or storage of data is entered into the blockchain. What happened to data, who accessed the data, where it went and how that data was governed – can be verified by anyone who has access to the blockchain. In such way, everyone will know what happend and when. In this way, data cannot be changed or deleted.

4. SECURE BLOCKCHAIN SOLUTIONS IN CLOUD COMPUTING

a) *Blockchain in IaaS – short overview in Mchain*

Data and measurements in IaaS cloud are critical evidences in the evaluation of IaaS.

Major techniques, for securing this kind of data, are: trusted hardware units and centralized data centers. But as it's presented, one of the biggest problem that cloud networks are facing is attack on central units. Thus, the one of the ways to protect data in IaaS cloud network is to use blockchain as database. The Figure 2 [6], shows architecture of so called Mchain [6] which uses blockchain as database, to store data.

Mchain introduces two-layer blockchain network. In the first layer, after the production, the data packages are the first verified by leveraging a correspondence between a package and a policy, and a one-to-one relation among a VM user and a node.

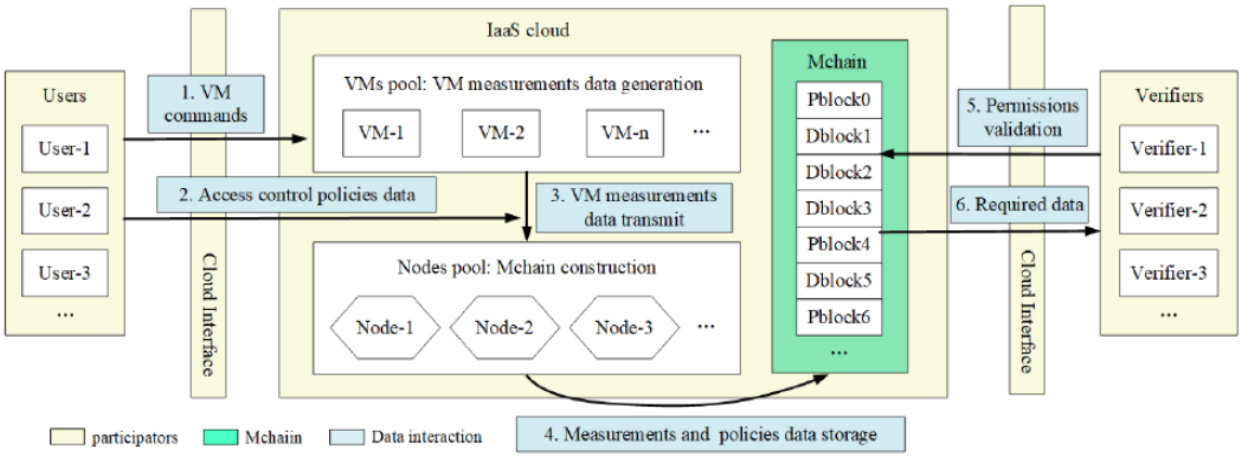

Fig. 2. Blockchain as database in IaaS

After that, consensus achievement algorithm is proposed, to construct a semi-finished block on a candidate block arranged by data packets. The semi-finished block is distributed to all nodes, which can provide a certain integrity. In the second layer, tamper-resistant metadata is generated by performing PoW tasks on the semi-finished block, resulting in strong integrity. Further, KP-ABE encryption method [6] is proposed for encrypting the data. It helps to have a control over authorized verifiers. There are six procedures in Mchain: (1) VM commands; (2) Access control policies – users define the policies to restrict the exposure scope of data; (3) VM measurements data – these data is spread through cloud; (4) Data storage – storing the VM measurements and policies in Mchain; (5) Permissions validation – verifiers are verifies against the policies to check the permissions; (6) Required data – only users that are verified can access the Mchain data.

Simply, before storing data in Mchain both users and virtual machines need to be verified. Their credentials are created when they are registered, and then public-private identification key pairs are used. An encryption key is also needed to protect the data being sent. When a data is ready to be stored in Mchain, it is encrypted, signed by the user and the VM from which the data is extracted, and a hash function is created for the corresponding policy. This package is sent through the cloud network and the nodes are validated using validation algorithms, moreover, the validity of the keys and hash is checked. Then a candidate block is formed to reach consensus with PoW in the second layer.

By separating a consensus achievement process from the original blockchain and hiding the time-intensive PoW tasks in the background, the confirmation latency of data packages could be reduced greatly from users' perspective.

Challenges that Mchain architecture facing with are poor access control and time intensive PoW task.

b) *Blockchain in IoT*

First of all, due to the scarcity of memory, power and computational resources of IoT devices, they always delegate IoT application tasks to cloud computing, which gives birth to the Cloud of Things (CoT) paradigm [4]. The CoT offers unlimited storage capabilities, unlimited processing power, flexible robust cloud computing environment and dynamic data integration.

The following features are the key ones for the resulting motivation to integrate blockchain Internet of Things and Cloud:

- Blockchain brings the capability of storing and managing cloud IoT data through its secure distributed ledge. More importantly, blockchain can provide a series of security features such as integrity, transparency and privacy, all of which promise to tackle efficiently security issues of current Cloud of Things networks. Thus, the main points of blockchain here are its security benefits to Cloud of Things and the need for scalability improvement.
- Cloud computing with its large resources can offer powerful computation and massive storage services with efficient data management, while IoT provides the ability of sensing, interconnecting and communicating with physical devices across different applied scenarios. Therefore, the main points of Cloud of Things

here are its advantages of providing scalable services and the need for security improvement.

Figure 3 shows the evolution of the network communications [5]. In the early stages of networking, there was only simple communication between users and server. Further development aims to the transition to network decentralization.

Figure 4 gives an overview of simple IoT architecture, with a brief description of the constituent layers. Perception layer is the lowest layer in this architecture. Network layer, where data is transmitted and processed, is the middle layer and finally, application layer.

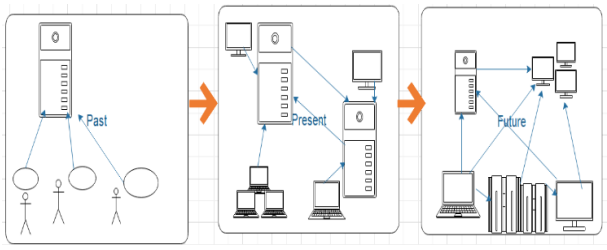

Fig. 3. Past, present and future of network communication

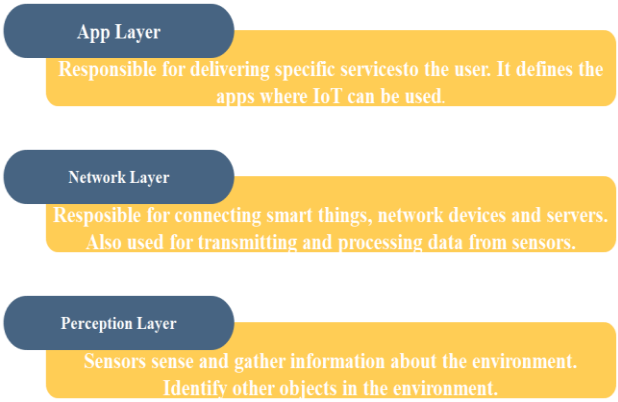

Fig. 4. Simple 3 layer IoT architecture

For sure can be said that blockchain is the missing part from the puzzle for resolving the security issues in IoT.

As is known, IoT devices caries very sensitive data, therefore, they are the target of many attackers. Many different solutions, including blockchain, offer protection for this kind of data.

Decentralized and autonomous characteristics of blockchain makes this technology suitable for deployment in several different scenarios like “Smart Home”, “Smart City”, “Smart Industries” etc. For example, blockchain can lead an unchanging history of smart devices, it can allow autonomous operation of intelligent devices, removing the presence of centralized organ or human control, using smart contracts. Blockchain can also create a secure way to exchange messages between smart devices.

The implementation of blockchain in the IoT network brings challenges as well as opportunities. In addition, list of opportunities are:

- Privacy/anonymity.
- Monetary data exchange and calculation.
- Account transactions and audit records.
- Smart contracts.

And the challenges are:

- Limited resources.
- Bandwidth demands.
- Security.
- Latency.
- Transaction fees.
- Allowed against public.
- Tolerance for sharing intermittently connected devices.
- Volume of transactions.
- Weakness of physical interfaces.

In Figure 5, example of architecture of CoT with blockchain is presented.

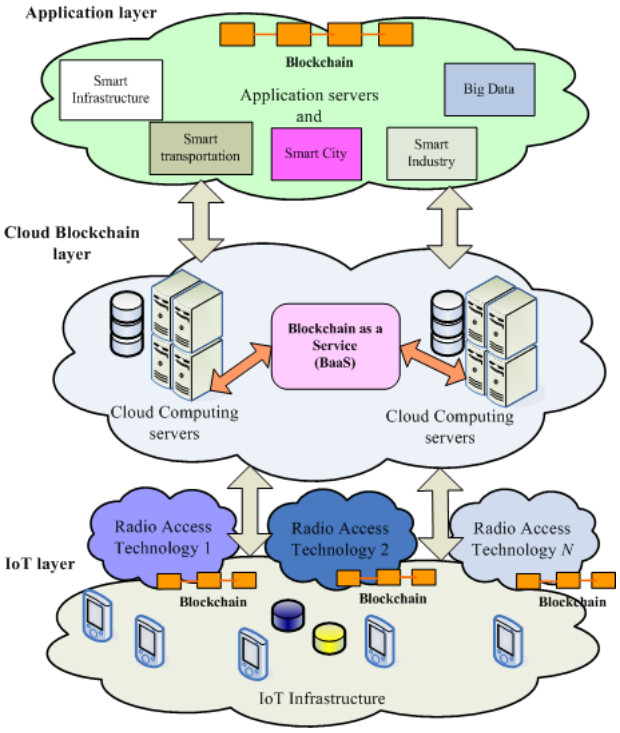

Fig. 5. Architecture of CoT integrated with blockchain

Furthermore we will discuss the challenges that BIoT applications are facing with [5].

Energy efficiency. – Energy efficiency is key to enable a long-lasting node deployment. Most of the consumption is due to two factors: Mining Involves PoW; P2P communications – Require edge devices that have to be powered on continuously, which could lead to waste energy

Throughput and latency. – IoT deployments may require a blockchain network able to manage large amounts of transactions per time unit. This is a limitation in certain networks. For instance, Bitcoin's blockchain has a theoretical maximum of 7 transactions per second, although it can be increased by processing larger blocks or by modifying certain aspects of the node behavior when accepting transactions. Regarding latency, it is important to note that blockchain transactions take some time to be processed. For example, in the case of Bitcoin, block creation times follow a Poisson distribution with a 10-minute mean, although, for avoiding double-spend, merchants are recommended to wait for about an hour, since five or six blocks usually need to be added to the chain before the transaction is confirmed

Blockchain size, bandwidth and infrastructure. – Lightweight nodes, which are able to perform transactions on the blockchain, but who do not have to store it; Another alternative would consist in the use of a mini-blockchain; Transaction and block size have to be scaled according to the bandwidth limitations of IoT networks: many small transactions would increase the energy consumption associated with communications, while a few large ones may involve big payloads that cannot be handled by some IoT devices; Regarding the infrastructure, certain elements are required to make the blockchain work properly, including decentralized storage, communication protocols, mining hardware, address management or network administration.

5. MIXING THE USE CASES AND PROPOSING A DIFFERENT SOLUTION

From the challenges presented in in the previous section, we can see that the best way to protect sensitive IoT data, while not ignoring the challenges, is to form Mini-blockchains. The mini-blockchain solution is the first proposed for bitcoin [7]. Therefore, our solution proposes to use mini-blockchain within IoT and cloud computing.

Mini-blockchain is the standard blockchain technology discussed in the sections above, with one difference, mini-blockchains does not keep a copy of all blocks and transactions (historical blocks). The idea behind mini-blockchains is to separate blockchain functionality into different mechanisms. In this way it can provide increasing bandwidth, improved flexibility, higher transaction speed and reduced latency. Another question is, why we propose mini-blockchains? Simply, mini-blockchains can be used in industries where users need to get access to their data quickly and in a secure way. This also includes the IoT industry. No less important fact is that with the growth of the network and the number of users, blockchain network's growths too, which is one of blockchain's major problems, keeping a history of blocks and transactions.

IoT devices had low computing power, and are collecting small and sensitive data. They can work at certain intervals, for example when it is necessary to include a period continuously, and in certain periods they are in a so-called "sleep" period when they do not need to collect data. In doing so, IoT users needed fast access to their data which must be protected. On the other hand, all of the reasons, opportunities, and challenges of merging blockchain with IoT are somehow contradictory, but one way to take advantage of blockchain's security benefits is precisely the mini blockchain solution. Blockchain actually stores huge amounts of information, blocks and transactions that are not even needed after a certain period of time, which can lead to "congestion" in the network after a certain period or longer processing time, etc. "It requires you to store a lot of data which doesn't really need to be stored forever. Breaking up the functions of the blockchain is the key" [7]. Figure 6 shows our proposed solution. The mini-blockchain will contain a group of IoT devices, which allows them to exchange data in a secure way, for example, devices that has the same function, or maybe devices that are in same region.

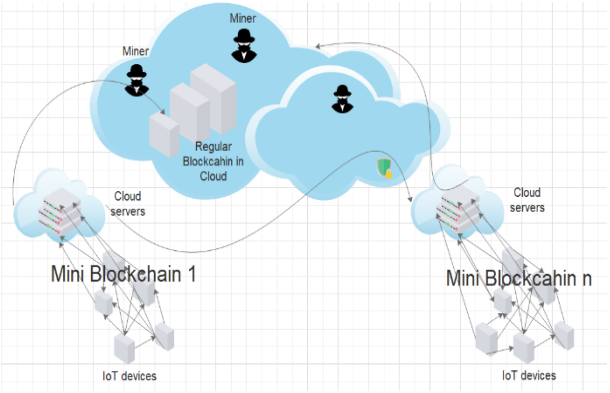

Fig. 6. Mini-blockchain cloud solution in IoT

All devices are represented on the network with an identifier and pair of public and private encryption keys. When an IoT device (for example a smart meter) generates metering data, it should encrypt it using cryptographic algorithms. In this case we will take the ECC encryption algorithm. The ECC has a significant advantage in this aspect [8]. Moreover, the device will generate a transaction with the data to be stored and will sign this transaction, therefore, everyone will know which device/sensor produced this data. The sensor will indicate as transaction output the public keys with the right to data read. It sends this transaction to network miners, which authenticate and include it in the next block. As the blockchain is public, all users have access to transactions and know that a particular user has the right to read the history produced by the presence sensor. However, only those who have the private keys will be able to read the measured data which was released by the device/sensor. But it our case, mini-blockchain is "public" only for devices that are connected to it, but for the whole network, mini-blockchain will be private. It means that mini-blockchain only allows a certain users/entities/devices to participate in that network. Participants have specific rights and restrictions.

If some devices simultaneously generate metered data, then a block with transactions of that data is created. With the cryptographic algorithm, hash for that block is generated and stored in the block header to ensure that the data remains unchanged. The network can be configured by setting up a block of "transactions" after specified time, no matter how many devices have generated metered data. The blocks are interconnected with hash functions (same as in regular blockchain) and are sent to the blockchain defined in the cloud network (all blocks), thus, IoT devices are freed from storing the history of all previous block transactions. All verified users in the mini-blockchain network will be able to access the necessary data. Blockchain has so called ledger who keeps track of all transactions. Each peer in the network has a copy of that ledger and the ledger is periodically updated. If devices are with better performace, than every device can store copy of a ledger on a daily or weakly basis. Because mini blockchain is private and has only verified devices, than those devices don't have to do the PoW tasks. PoW is done in the regular Blockchain. Actually, the idea is to free those devices form PoW tasks, as they don't have the capacity to do it.

A question arises: Can users get access to data that is stored in the regular blockchain? – Yes, users that are verified to get access to data in mini-blockchain, they can do the same in regular blockchain. The one way this can be done is using cloud blockchain application.

With this proposed solution, the three requirements (confidentiality, integrity and availability) that guarantee system security are fulfilled. *Confidentiality*: The most sensitive information are protected from unauthorized accesses. *Integrity*: It guarantees that data are not altered or deleted by unauthorized parties. It is also usually added that, if an authorized party damages the information, it should be possible to undo the changes. *Availability*: Data can be accessed when needed. The same solution may be used for billing, but then all devices/peers who want to send a digital currency transaction will have to pay to the blockchain. It is called transaction fee and it is one of the main tools used to speed up crypto transactions, which are often slow due to high congestion on the blockchain network. The lower the blockchain fee, the lower your transaction's priority in the blockchain network will be. But this is not the goal of this paper. It's mentioned for future researches and works. Of course this is not the perfect solution either, but it does provide a higher degree of data protection and what is important, it does not load the IoT network and IoT devices.

Another way to use blockchain within the IoT is in the smart transport, i.e. charging electric vehicles. In Figure 7 is shown the four-step charging protocol [12]. In the first step, research, EV sends a request to blockchain. In the second step, bidding, the charging stations send bids in response to the previous request and one of them is selected in step 3, evaluation, by the EV. The fourth step is charging and is not managed by blockchain.

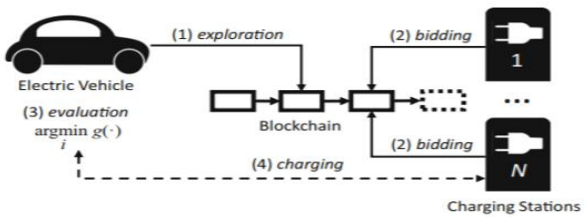

Fig. 7. Protocol for charging EV

In fact, in this case blockchain is an application and an "intermediary" for sending a request from the EV and offering it from the charging stations.

EVs cannot be monitored over time because the network presents IDs that can be changed with

each subsequent request. Moreover, in the request do not specify the location they are in, but the region in which they want to find a charging station. This solution excludes the Proof of Work section and the formation of blocks. Blockchain only serves to verify the authenticity of the offers coming from the charging stations and cannot be modified.

As we can see, blockchain can be implemented to IoT and cloud in a different ways. It's up to us how we will use it's benefits and properly secure the network.

One more note, since end-devices and edge devices do not have the capacity to execute all blockchain processes, the server level is ideally suited to modern the entire blockchain technology. Such an approach could link centralized IoT deployment to a decentralized blockchain network, where the server level will act as an access point to the blockchain network.

6. CONCLUSION

In this paper are given use cases where blockchain is used within the cloud computing and IoT. In the last years, blockchain is one of the most popular technologies that leads to improved security. It's somehow hard to implement it in it's full functionality with IoT, but if we try to mixed them all, then a solution can be found which will significantly improve the security and authenticity of data. From the analysis given in this paper, can be concluded that in the context of IoT the best solution is to use blockchain as unchanging database. This is due to the challenges we face when integrating both technologies. Another idea is to use multiple "small"-blockchains in order to communicate with IoT users, and one "main"-blockchain implemented in cloud, that will communicate with all of these small blockchains.

From aspect of the cloud computing, the best solution for using blockchain is dividing it in two layers. The first layer will just verify packages (reduces latency) and second layer will do the complex task Proof of Work. Moreover, for cloud computing, we have proposed our solution, based on many analyses over different solutions. According to our solution, a usage of mini-blockchain within IoT and cloud computing is proposed. Thus, as Section V elaborates – our solution provides satisfied level of data protection and, what is important, it does not load the IoT network and IoT devices.

Finally, the blockchain can be used in its true sense, without impacting the system, in payment methods (where cloud is also used) and in many other methods including cloud and mobile computing.

REFERENCES

[1] Crystal, Bedall: Information Week, 1 September 2019.

[2] Keke Gai, Meikang Qiu: *Mobile Cloud Computing, Models, Implementation and Security*, Pace University, New York, USA, CRC Press, 2017.

[3] IEEE – Tech Fact: *Cybersecurity hackers attack every 39 seconds*, March 14, 2020.

[4] Mohammand Aazam, Eui-nam Huh, Imran Khan: *Cloud of things: Integrating internet of things and cloud computing and the issues involved*, Conference paper, January 2014.

[5] Tiago M. Fernandez-Carames, Paula Fraga-Lamas: *A Review of the Use of Blockchain for the Internet of Things*, Department of Computer Engineering, Faculty of Computer Science, Campus de Elviña, s/n, Universidade da Coruña, 15071 A Coruña, Spain, July 6, 2018.

[6] Bo Zhao, Peiru Fan, Mintago Ni: *Mchain: A Blockchain-Based VM Measurements Secure Storage Approach in IaaS Cloud with Enhanced Integrity and Cotrollability* Wuhan University, Wuhan, China, August 28, 2018.

[7] J. D. Bruce: *The Mini-blockchain scheme*, March, 2017 www.cryptonite.info.

[8] Emanuel Ferreira Jesus, Vanessa R. L. Chicarino, Célio V. N. de Albuquerque, Antônio A. de A. Rocha: *A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack*, April 8, 2018.

[9] https://www.investopedia.com/terms/b/blockchainasaservice-baas.asp

[10] https://innovationatwork.ieee.org/growing-cloud-computing-utilization-in-2019/

[11] https://medium.com/@ppio/understanding-cross-chain-technology-e36b9c0cfaf3

[12] Fabian Knirsch, Andreas Unterweger, Dominik Engel: *Privacy preserving blockchain based electric vehicle charging with dynamic traffic decisions*, Josef Ressel Center for User Centric Smart Grid Privacy, Security and Control, Salzburg University of Applied Sciences, Urstein Süd 1, 5412 Puch b. Hallein, Austria, Septemeber 2017, page 2–8.