Blockchain based decentralized approach for cloud computing

Anatoly Todorov Peshev

University of Library Studies and Information Technologies
119 Tsarigradsko Shose blvd., 1784 Sofia, Bulgaria
peshev@outlook.com

Abstract – **The Cloud computing concept provided solution for the always increasing demand of computing power, while keeping the costs at reasonable levels for organizations. Although, all the benefits of adopting cloud solution still there are privacy and vendor lock-ins concerns. Decentralized approach, based on the Blockchain and Edge Computing concepts can provide solution for those concerns.**

Keywords – **blockchain; cloud computing; decentralization; edge computing.**

I. CLOUD COMPUTING BENEFITS

Cloud computing is the on-demand availability of computer system resources. In general, cloud computing is used for publicly available data centers over Internet [1]. Large clouds often have functions distributed over multiple locations from central servers. Cloud computing relies on sharing of resources to achieve coherence and economies of scale. Some of the benefits of cloud computing for the organizations are:

- Decrease of the IT infrastructure costs
- Implementation of enterprise-level applications in faster manner, with improved manageability and less maintenance
- IT teams can adjust more rapidly the resources to meet unpredictable demand.

The goal of cloud computing is to allow organization to take benefit from technologies like hardware virtualization, service-oriented architecture and high-speed networks, without the need for deep knowledge about or expertise with each one of them. The main enabling technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more virtual devices, each of which can be easily used and managed to perform computing tasks. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. Autonomic computing automates the process through which the cloud provider can provision resources on-demand. By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors.

II. CLOUD COMPUTING RISKS OF CENTRALIZATION

Although, there are numerous benefits of adopting the latest cloud technology still there are privacy issues involved in cloud computing because in the cloud the data can outbreak the service provider and the information is deleted purposely. There are security issues of various kinds related with cloud computing falling into two main categories:

- Issues related to the cloud security that the cloud providers face – like software provided to the organizations, infrastructure as a service
- Issues related to the cloud security that the customers experience – organizations who store data on the cloud

Most issues start from the fact that the organization loses control of its data, because it is stored on a hardware belonging to the cloud provider. Other issues hampering the adoption of cloud technologies include the uncertainties related to guaranteed QoS provisioning, automated management, and remediation in cloud systems.

As with other changes in the landscape of computing, certain legal issues arise with cloud computing, including trademark infringement, security concerns and sharing of proprietary data resources [2]. One important problem is who is in possession of the data. If a cloud company is the possessor of the data, the possessor has certain legal rights. If the cloud company is the custodian of the data, then a different set of rights would apply. Other problem in the legalities of cloud computing is the problem of legal ownership of the data. These legal issues are not confined to the time period in which the cloud-based application is actively being used. There must also be consideration for what happens when the provider-customer relationship ends. In most cases, this event will be addressed before an application is deployed to the cloud. However, in the case of provider insolvencies or bankruptcy the state of the data may become blurred.

Another concern is that many cloud platforms and services are proprietary, meaning that they are built on the specific standards, tools and protocols developed by a particular vendor for its particular cloud offering. This can make migrating off a proprietary cloud platform prohibitively complicated and expensive. Three types of vendor lock-in can occur with cloud computing:

- Platform lock-in: cloud services tend to be built on one of several possible virtualization platforms, for example Hyper-V or VMware. Migrating from a cloud provider using one platform to a cloud provider using a different platform could be very complicated.
- Data lock-in: since the cloud is still new, standards of ownership, i.e. who actually owns the data once it lives on a cloud platform, are not yet developed, which could make it complicated if cloud computing users ever decide to move data off of a cloud vendor's platform.

- Tools lock-in: if tools built to manage a cloud environment are not compatible with different kinds of both virtual and physical infrastructure, those tools will only be able to manage data or apps that live in the vendor's particular cloud environment.

Heterogeneous cloud computing is described as a type of cloud environment that prevents vendor lock-in, and aligns with enterprise data centers that are operating hybrid cloud models. The absence of vendor lock-in lets cloud administrators select his or her choice of hypervisors for specific tasks, or to deploy virtualized infrastructures to other enterprises without the need to consider the flavor of hypervisor in the other enterprise. A heterogeneous cloud is considered one that includes on-premises private clouds, public clouds and software-as-a-service clouds. Heterogeneous clouds can work with environments that are not virtualized, such as traditional data centers. Heterogeneous clouds also allow for the use of piece parts, such as hypervisors, servers, and storage, from multiple vendors. Cloud piece parts, such as cloud storage systems, offer APIs but they are often incompatible with each other. The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations. This has been described as a problem of vendor lock-in. The solution to this is for clouds to adopt common standards.

III. BLOCKCHAIN

A blockchain is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance [3]. Decentralized consensus has therefore been claimed with a blockchain.

IV. EDGE COMPUTING

Edge computing is a distributed computing paradigm which brings computation and data storage closer to the location where it is needed, to improve response times and save bandwidth [4]. The increase of IoT devices at the edge of the network is producing a massive amount of data to be computed to data centers, pushing network bandwidth requirements to the limit. Despite the improvements of network technology, data centers cannot guarantee acceptable transfer rates and response times, which could be a critical requirement for many applications. Furthermore, devices at the edge constantly consume data coming from the cloud, forcing companies to build content delivery networks to decentralize data and service provisioning, leveraging physical proximity to the end user. In a similar way, the aim of edge computing is to move the computation away from data centers towards the edge of the network, exploiting smart objects, mobile phones or network gateways to perform tasks and provide services on behalf of the cloud. By moving services to the edge, it is possible to provide content caching, service delivery, storage and IoT management resulting in better response times and transfer rates. At the same time, distributing the logic in different network nodes introduces new issues and challenges.

Organizations have realized that a more decentralized approach is required to address digital business infrastructure requirements. Edge computing moves some portion of an application, its data or services, away from one or more central nodes to the other “edge”, often in contact with the end users. Edge computing uses a mix of peer-to-peer ad hoc networking, local cloud computing, grid computing, fog computing, distributed data storage and other more sophisticated solutions. In computational resource sharing platforms like SETI@home, the main issue is the dependence on central nodes to distribute and manage tasks, thus encountering similar issues of centralized architectures described in this paper, alongside issues related to proper incentivization plans to computing power providers and correct verifiability of the performed computation. In this scenario, blockchain technology emerges as a strong facilitator of decentralized cloud solutions. The consensus and reward mechanisms used within blockchain-based architectures can provide distributed computing a strong support to overcome some of the issues mentioned [5]. For example, re-paying node hosts using a platform’s own medium of exchange is not only a useful incentivization method for interested parties to put their resources online, but it also helps avoid misbehaving actors.

V. CONCLUSION

The blockchain concept for decentralized cloud computing is providing a transparent and interconnected network that eliminates the need for a centralized transactional authority and solves some of the classic cloud computing’s most troubling risks.

ACKNOWLEDGMENTS

The research is supported by the KoMEIN Project (Conceptual Modeling and Simulation of Internet of Things Ecosystems) funded by the Bulgarian National Science Foundation, Competition for financial support of fundamental research (2016) under the thematic priority: Mathematical Sciences and Informatics, contract № DN02/1/13.12.2016.

REFERENCES

[1] Amazon Web Services, "What is Cloud Computing?", March 2013.

[2] M. Ryan, Cloud Computing Privacy Concerns on Our Doorstep, January 2011.

[3] The Economist, "Blockchains: The great chain of being sure about things", October 2015.
[4] E. Hamilton, What is Edge Computing: The Network Edge Explained, May 2019.
[5] Ali Ayyash, 3 Reasons Cloud Engineers Can Easily Make the Switch to Blockchain, March 2018.