

A Consortied Ledger-based Cloud Computing Provider Users Reputation Architecture

Gabriel Escobar Vasques and Adriano Fiorese^{1a}

Graduate Program in Applied Computing (PPGCAP), Department of Computer Science (DCC),
Santa Catarina State University (UDESC), Joinville, Brazil

Keywords: Blockchain, Cloud Computing, Credibility, Reputation.

Abstract: Several users and organizations have been attracted by the benefits offered by the cloud computing services. However, there are still several security issues and challenges in these environments. Controlling access to providers is an important task and must be carried out safely. In this sense, this paper presents a ledger-based collaborative user reputation architecture for a cloud providers' consortium. The reputation is based in two indicators: objective and subjective ones. The objective data corresponds to the user's session data. Subjective data, on the other hand, corresponds to the providers' feedback about users and data obtained from external sources. The combination of these two indicators defines the reputation value. It aims to avoid bias in the evaluations carried out by the providers and possible conflict of interests. In order to evaluate the proposed architecture, a user cloud providers scenario was developed. Evaluation results show applicability of storing and providing users reputation values to participating providers.


1 INTRODUCTION

Several users and organizations have been attracted to Cloud Computing (CC) services in the last years. Public health questions can result in social isolation preventing organizations from carrying out their activities normally. As main benefits in the adoption of cloud services we can emphasize its ubiquitous model of working and the on demand services delivery. Besides that, the cloud services make possible cost reduction on hardware acquisition, installation, and maintenance of the hardware equipment, etc. (Liu et al., 2012). Despite the benefits offered by the CC there are several security issues and challenges that still need attention, offering research opportunity for development of proposals to solve them.

The NIST (National Institute of Standards and Technology) in its cloud reference architecture identified several issues of security (Liu et al., 2012), and had made them public through a report. It establishes necessary recommendations so that the security and privacy of services are guaranteed. Among the issues raised by NIST, the identity management and access control is an important security issue for service providers. Malicious users represents menace and are cause for great concerns in cloud envi-

ronments (Nkosi et al., 2013). In the literature it is possible to find several techniques and tools focused on authentication and control access of users. The Public Key Infrastructure (PKI) and Reputation Systems (RS) are examples of used techniques to perform these tasks. Particularly, reputation systems are widely used to estimate the credibility of service providers, e-commerce users, among others. In such cases, the risks assumed by providers and users in their relationships on computational systems are proportional to the reputation of the provider/user they are dealing with. To encourage users good behaviour in their interactions with the service providers and help on providers access control it is possible to use credibility indicators. Such indicators can be defined by a reputation calculation based in the actions taken by users in their interactions with providers. Coping with a scenario in which CC service users utilize services of multiple service providers in their activities, it is possible to utilize a collaborative reputation system shared between a consortium of providers aiming the users reputation calculation based on the performed actions on participants providers.

In this sense, this paper aims to present a cloud provider service users reputation architecture that uses as basis for the reputation value calculation, the relations of users with consortium CC service

^a  <https://orcid.org/0000-0003-1140-0002>

providers and their overall behaviour catch by external information sources. This architecture has the function of providing participating providers with users' reputation/credibility value to help them control access to their services and contribute to the management of risks and threats that users may represent. Given the scenario characteristics we intend to work on, which relies on the distributed collaboration of consortium cloud providers, blockchain technology will be used to store the values used to calculate the reputation value as well as the reputation value itself. This technology acts as a Timestamping Authority (TSA), which is responsible for ensuring the order of chronological transactions and user behaviour data integrity. Blockchain offers benefits such as data redundancy, transparency, consensus on demand, which differs from traditional reputation architectures/systems. In addition, it uses the P2P (peer-to-peer) communication model. That is, blockchain does not present a single point of failure that is common in reputation systems that relies on client/server communication.

This work is organized as follows: Section 2 presents the concepts related to cloud computing, reputation and blockchain technology. Section 3 exhibits works related to this research. Section 4 presents the users reputation architecture proposal. Section 5 discusses the scenario and experiments performed, as well as results obtained. Lastly, Section 6 present the final consideration and future work.

2 BACKGROUND

This section presents characteristics and descriptions of the related technologies to the content covered by this work.

2.1 Cloud Computing

Cloud computing is a paradigm for more efficient use of computational infrastructure, being defined as a technologically ubiquitous model. Cloud computing service models are defined according to how the configurable set of computational resources can be delivered to end users. In this work, we adopted the NIST nomenclature, which is used by several researchers and organizations.

According to the NIST reference model, an important feature in computational clouds regardless of their classification and deployment model is security. NIST has developed a security guide, which provides an overview of the security and privacy challenges involved in CC (Jansen and Grance, 2011). Among the

security issues pointed out by NIST, access control is an important task and requires care by providers. This work presents a cloud providers' users reputation architecture that aims to assist the addressment of issues raised by the security guide prepared by NIST. Among these issues, the proposed architecture aims to assist service providers at managing identity and access. In addition, the architecture reputation value can indirectly assist the management of cloud providers internal risks and threats.

2.2 Reputation

Reputation is a well-known concept and applied in several areas. A widely used definition of reputation to describe its use in computer systems was developed by (Mui et al., 2002). There, the authors define reputation as: *"the perception that an agent creates through past actions on his or her huge intentions"*. Typically, reputation values are defined according to the feedback provided by users and/or comprising the results of the transactions. However, applications that use only feedback in their calculations, which are subjective in nature, can present loopholes for malicious users and common reputation system attacks such as self-promotion or defamation (collusion) (Hendrikx et al., 2014). So, in fact, the final reputation values are not affected only by feedback to prevent malicious behavior, it is possible to use other information together with them to compose the calculations. In this sense, it is possible to use objective information about users to compose the reputation calculation, such as: behavior classification, use of resources, etc. In addition, information related to the payment of monthly fees/annuities regarding the used computational resources, can also be part of the final reputation value. This way, the final reputation values will be less susceptible to malicious feedback provided by dishonest users.

2.3 Blockchain

Blockchain is a disruptive technology for conducting transactions between two entities without the need for a responsible third party to establish trust (Nakamoto, 2009). The blockchain concept consists of six main characteristics: decentralization, transparency, open source, autonomy, immutability and anonymity (Lin and Liao, 2017). In general, applications developed with blockchain can be implemented following three main models: public, private and consortium (Lin and Liao, 2017). In public blockchains, the entry of new participants in the network happens in a simple way. Users can choose to participate in the consensus pro-

cess and consequently to the addition of new blocks where all participants in the blockchain can check the transactions. A blockchain network is a technical infrastructure that provides ledger and smart contracts services to applications.

In implementations that follow the private model, the control of the blockchain network is performed by a single organization which is responsible for allowing or not allowing the entry of new participants, in addition to defining the actions that each participant can perform. The consortium model works in a similar way to the private one. However, two or more organizations have control of the network. In these models, the mechanisms used to obtain consensus and to add new blocks tend to be less computationally costly, and consequently consumes less energy. Furthermore, in these models, participants are usually well identified and only participants defined by the organization(s) can verify transactions and add new blocks (Greve et al., 2018).

Blockchain technology is used in the development of the reputation architecture proposed in this work. In turn, the architecture suits a scenario where CC service providers and their users integrate a blockchain network at the consortium model.

3 RELATED WORK

Some works such as (Xu et al., 2019) are aimed at assisting the selection of personalized CC services, based on Quality of Service (QoS) assessments carried out by users. To encourage users to provide reliable QoS assessments, the authors propose a mechanism for calculating users' reputation and reliability based on the assessments provided by them and comparing it with other assessments on the same service provided by other users. In (Zheng et al., 2018) the authors present an approach to improve the speed of classifying users' normal behavior in a cloud environment. For this, those authors present a reputation classifier, which is responsible for calculating the reputation values based on the user behavior and service use classifications obtained by means of machine learning.

The work of (Thakur and Breslin, 2019) proposes a mechanism for managing the reputation of IaaS-type service providers in a federated/hybrid cloud. The proposal aims to encourage providers to classify their users' behavior correctly, differentiating them between good and malicious users. The reputation of providers is estimated through feedback from providers about other providers, feedback from users about providers and feedback from providers about

users.

The work developed by (Wu et al., 2015) introduces a reputation mechanism and designs a reputation-based identity management model for CC. The authors developed a model, in which users receive pseudonyms generated from a reputation signature in order to guarantee the non-traceability of pseudonyms and proposes a reputation calculation mechanism to help identify malicious users. The work of (Du et al., 2019) proposes an online reputation calculation method to efficiently provide a personalized reputation for each user, within the context of cloud applications based on service-oriented architectures. The work (Donghong et al., 2016) presents a dynamic access control framework based on reputation and attributes for privacy protection in the CC environment.

These works analysis shows that there is a gap for works that present approaches related to the reputation of users of cloud providers. Moreover, it is also noticeable a lack of works where providers' users reputation is shared with other providers, allowing them to assess the risks that eventually malicious users can to offer.

4 PROPOSAL

This paper models and proposes a reputation architecture for users of cloud providers, as a collaborative tool between them.

4.1 Reputation Architecture

The proposed architecture is presented in Figure 1. It is composed of several modules that perform the functions related to the calculation of the reputation value. For the implementation, blockchain technology was used as a mechanism for data persistence, taking advantage of its benefits as immutability to protect data against attacks on the reputation system, as well as ensuring the traceability and auditing of any conflicts. The reputation architecture has three main components: the reputation system (RS), the cloud provider and external data sources. The RS consists of the reputation calculation module and the blockchain itself. The data is validated and stored in a distributed and redundant way using a blockchain in the consortium model through distributed consensus. The blockchain has the important role of acting as a distributed TSA, being responsible for ensuring the temporal ordering of the records inserted in the chain of blocks.

The proposed architecture usage and behaviour is given by the following interactions between its mod-

ules. Upon receiving the request, the access control module of the cloud provider can perform a query to the reputation calculation module to obtain the user reputation value. Upon receiving the user's reputation value, the provider may or may not allow the user access to its services, applying access and security policies according that value. If access is allowed, user uses the provider's services and at the end of his session provider makes available the data from that session to the reputation system so that they can be used in the proper credibility indicator calculations. After receiving the session data from the user, the RS performs consultations with external sources to obtain information from public databases that are also used in the calculations. After receiving all the previously mentioned data, they are saved in the ledger and calculations of the objective and subjective credibility indicators are performed. The values that compose the objective credibility indicator come from resources utilization offered by the providers to the users like RAM memory, processors, the user connection stability and payments. Thus, the higher these values, which indicates an active, stable and well payer user, the higher the objective credibility indicator and consequently the reputation value. The contrary is also directly related. The values that make up the subjective credibility indicator come from the external sources and user evaluation given by the providers feedback. The final reputation value is calculated by combining these two indicators.

The sources of external information are used in the reputation calculation together with the providers' feedback to compose the subjective credibility indicator. These kind of external sources should provide info that can be used to marginally infer a particular portion of the user social behavior. Queries to these external (to the architecture) databases return the respective number of issue items that user has. Originally, as proposed by default, it should be four external data sources and each one of them represents 25% of the external issues indicator.

However, providers can assign agreed weights to external data sources at their own discretion.

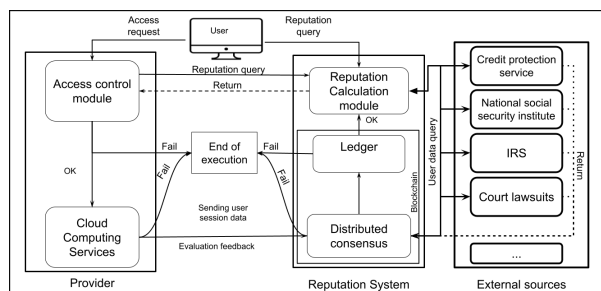


Figure 1: Reputation Architecture.

Thus, the reputation (R) of users is given by the combination of two historical indicators of credibility: the objective and subjective ones, as observed in Equation 1.

According to the definition adopted for reputation, I_{obj} is the historical and current objective credibility indicator (if any) for user s , I_{sub} is the historical subjective credibility indicator and ω_{obj} , ω_{sub} are weights defined for the respective indicators.

Equation 2 represents the user's objective credibility indicator, which is composed of the average percentage of computational resources use (\overline{upr}) in n sessions, the connection stability (EoC) calculated by the n sessions latency ($ping$) value average and the ratio calculated between the number of payments made on time and the total number of monthly/annuity payments (pay), for each user. These indicators correspond respectively to 35%, 25% and 40% of the objective credibility indicator value.

The \overline{upr} variable corresponds to the percentage of resource use, which is calculated by means of the arithmetic average between the percentage averages of CPU usage (mcp) and corresponding RAM memory usage (mmr) in the last n user sessions. Equation 6 is responsible for calculating the percentage value of resource usage according to the user's history (\overline{upr}). The percentage of use of each CPU (processing core) ($pcp(s)$) is captured during the user's session and through it the average percentage of CPU usage of that session is calculated. Thus, the mcp variable, which corresponds to the average percentage of CPU usage, is obtained by adding the percentages of use of each CPU (pcp) used, from the first core ($i = 1$) to the last one (npc), and dividing that sum by the total number of cores (npc). Equation 3 is responsible for calculating the user's CPU usage percentage ($mcp(s)$).

The mmr variable corresponds to the average RAM memory usage in MB, which is calculated as the ratio between the sum of the memory usage value every second during the user session, and the total duration of the session tf , in seconds. Equation 4 is responsible for calculating the average RAM memory usage for that session. The pur variable corresponds to the percentage of RAM memory usage, calculated by the ratio between the average RAM memory used (mmr - Equation 4) and the amount of RAM memory allocated (amr). The amount of allocated RAM (amr) is the amount originally purchased by the user. Equation 5 is responsible for determining the percentage of RAM memory usage.

In turn, variable (EoC) present in Equation 2 corresponds to the historical average of the user's connection latency. To obtain its value, the user's connec-

tion latency value should be initially obtained from each user's sessions. In this case, the ping application is used for polling, by means of the Internet Control Message Protocol (ICMP), between the cloud provider and a host on the user's network, making it possible to obtain the latency value in the communication between provider and user. Thus, every ping operation during the user's session at the provider adds value 1 for the latency accumulator, if its value is less than or equal to 150 ms. At the end of the session, this accumulated value is divided by the number of times that the latency value was recovered (n), according to Equation 7. This is the user connection latency when he is using a cloud provider. The user s historical average latency ($\overline{EoC}(s)$), used in the composition of the objective indicator, according to Equation 2, is calculated using the p last (therefore historical) values of the user's connection latency (EoC), as shown in Equation 8.

In turn, variable (pay), also Equation 2, corresponds to the user's punctuality in paying the monthly fee for the cloud provider's services. Variable (pay) corresponds to the ratio between the number of payments up to on time (npd) and the total of payments made (ntp), as described by Equation 9.

On the other hand, Equation 10 is responsible for calculating the subjective credibility indicator value. This value results from the difference between the feedback from the providers and the results of consultations with external sources.

The second component of the subjective credibility indicator comprises the results from consultation with external sources, and it is called external issues indicator ($I_{pex}(s)$). Equation 11 is responsible for calculating that indicator. For the calculation of the external issues indicator, normalization is carried out involving the sum of the values obtained from external sources (Fe_j) weighted by the cloud providers (default weight is 0.25 each external source), and the sum of weighted maximum values from each external source, according each user s . Equation 12, on the other hand, is responsible for calculating the average of n values of the external issues indicator for each user, making the final external issues indicator a historical indicator. The n value, representing the historical period (how many external issue indicator values are used), should be agreed among the cloud providers belonging to the consortium.

Cloud providers send feedback values, regarding their users, to allow the user behaviour assessment by the reputation architecture. These feedback values comprise different activities users perform at the cloud provider. Each of these activities is represented by an indicator, for instance (I_1, I_2, \dots, I_k), where k is

the total number of activities/indicators. This work proposes three so called feedback indicators. First indicator (I_1) corresponds to the provider's feedback due to the user's login attempts. Second indicator (I_2) corresponds to the provider's feedback due to the login path, in which the IP address and the user agent are verified. According to (Yu et al., 0108) and (Berrached and Korvin, 2006) these two indicators represent factors that influence the user's login behavior and credibility. Third indicator (I_3), on the other hand, corresponds to the provider's feedback due to the attempts of users to access improper data. Providers assign values from 0 to 10 for each of these indicators according to the user attempts to execute the corresponding activities. All providers must be in line with the feedback evaluation model in order to avoid indicator value bias. Thus, a user feedback provided by all nfp providers, in a time period, corresponds to the ratio between feedback indicators' sum from all providers [$1..nfp$], and the sum of maximum values for each of these indicators, from all providers [$1..nfp$]. Equation 13 shows user feedback ($Fp(s)$) calculation.

In turn, Equation 14 transforms the single period of time user feedback indicator ($Fp(s)$) into a historical (average) user feedback ($\overline{Fp}(s)$). To accomplish that, it performs the ratio between the sum of np single user feedback indicators and the number of already (past) calculated single user feedback indicators for that historical period (np). This np value also must be agreed among providers' consortium participants. It is important to note that the historical user feedback is one of the subjective credibility indicator components (Equation 10).

$$R_s = \omega_{obj} * I_{obj}(s) + \omega_{sub} * I_{sub}(s). \quad (1)$$

$$I_{obj}(s) = (\overline{upr} * 0.35 + \overline{EoC} * 0.25 + pay * 0, 40). \quad (2)$$

$$mpcp(s) = \frac{\sum_{i=1}^{n_{pc}} pc p(s)_i}{n_{pc}} \quad (3)$$

$$mmr(s) = \frac{\sum_{i=1}^{t_f} umr(s)_i}{t_f} \quad (4)$$

$$pur(s) = \frac{mmr(s)}{amr(s)} \quad (5)$$

$$\overline{upr}(s) = \frac{\frac{\sum_{i=1}^n pur(s)}{n} + \frac{\sum_{i=1}^n mpcp(s)}{n}}{2} \quad (6)$$

$$EoC(s) = \frac{\sum_{i=1}^n 1[ping_i \leq 150ms]}{n} \quad (7)$$

$$\overline{EoC}(s) = \frac{\sum_{i=1}^p EoC(s)_i}{p} \quad (8)$$

$$pay(s) = \frac{npd}{ntp} \quad (9)$$

$$I_{sub}(s) = \overline{Fp} - \overline{I_{Pex}} \quad (10)$$

$$I_{Pex}(s) = \frac{\sum_{i=1}^{Nfe} Fe_i * \omega_i}{\sum_{j=1}^{Nfe} \max(Fe_j * \omega_j)} \quad (11)$$

$$\overline{I_{Pex}(s)} = \frac{\sum_{i=1}^{nfp} I_{Pex(s)_i}}{nfp} \quad (12)$$

$$Fp(s) = \frac{\sum_{i=1}^{nfp} I_{1,i} + I_{2,i} + I_{3,i}}{\sum_{j=1}^{nfp} \max_j(I_1) + \max_j(I_2) + \max_j(I_3)} \quad (13)$$

$$\overline{Fp}(s) = \frac{\sum_{i=1}^{np} Fp_i}{np} \quad (14)$$

5 SCENARIO & EXPERIMENTS

The performed experiments are based on a scenario, in which 15 users use the services of 3 different cloud providers. These cloud providers compose a blockchain network coping with the consortium model, and they use the proposed reputation architecture. The experiments were carried out using *Hyperledger Fabric* version 2.2 framework developed by the *Linux Foundation*. To create and configure the blockchain network, *Docker* containers and the container orchestrator *Docker-Compose* were used. The blockchain network reaches consensus by means of the Byzantine Fault Tolerance (BFT) mechanism, which allows the consensus process to be carried out even if some nodes fail or act maliciously. To develop chaincodes (smart contracts), *JavaScript* programming language was used. *Node.js* framework runs *JavaScript* code. To manage packages for *JavaScript* language, the *Node Package Manager* was used, which is already included in *Node.js* framework. In addition, *cURL* (Client URL) software that provides a library and a command line tool for transferring data, providing support for various protocols, was used.

Experiments were carried out on a computer with an *Intel Core-i5-7200U* 2.50 GHz processor, 8 GB of RAM memory with *Linux Mint* 19.2 operating system. A simulation of a hypothetical case was conducted, in which each user performs 10 sessions at one of the participating providers. In addition, five different users are assigned to each provider. The values used to compute the objective and subjective indicators like memory use, processors use, user latency,

external issues values, and providers feedback were generated randomly, following a normal probability distribution function using the *Math.random* floating point random number generation function available in the *JavaScript* programming language. All values were generated 10 times to enable averages to be calculated. Values between 35 and 95 were used for the CPU and RAM memory percentage indicators.

Average of 10 values between 20 and 200ms is used for the connection stability indicator (user latency). Values between 0 to 10 were generated for each feedback indicator from the providers. These values were generated 10 times and added, then these values were normalized to obtain values between 0 and 1, according Equation 13. In this case, *nfp* equals to 10. Comprising data from each external sources, values between 0 and 10 were generated taken into account one external data request per session and a historical period of ten sessions (*n* in Equation 11 is 10). The payment amounts correspond to the payments on time divided by the total number of total payments (historical period) resulting in a value between 0 and 1. The values were generated for a period of 10 months, where the value 1 corresponds to the payment on time and 0 for late payment. When the payment was made the value 1 is added, otherwise the value 0 is added. The values of the indicators that make up the objective and subjective indicators are obtained through the summation and subsequent calculation of averages of data of 10 last sessions. To calculate the averages of the indicators, values corresponding to 10 session of each user were generated. These values were used to calculate the historical average values of the $\overline{I_{Pex}}$, \overline{Fp} and \overline{EoC} indicators.

5.1 Results

Tables 1, 2, 3 show results from simulation. In all tables, user identifiers (1 to 15) and provider identifiers (1 to 3) are present in the first two columns. Table 1 presents the information about the CPU use percentage averages, RAM memory use average, resource usage percentage average, ratio between the number of payments on time and total number of payments, and connection stability indicator historical value, i.e., user session latencies average. Table 2 presents average (historical) user feedback, and the average values returned by the external data sources (F1, F2, F3 and F4) presented in Section 4.1. These values represent the historical average obtained by the summation of the 10 simulations data to each external data source.

Table 3 presents Objective and Subjective credibility indicator values, according data from previous

Table 1: User session data provided by cloud providers.

User ID	Provider ID	CPU average	RAM average	Resources use average	Payment	Connection stability
U1	P1	66%	64%	65%	1	0,92
U2	P3	74%	70%	72%	0,83	0,87
U3	P3	71%	66%	68,2%	0,75	0,64
U4	P1	60%	53%	56,5%	1	0,98
U5	P2	79%	71%	75%	0,9	0,86
U6	P2	58%	50%	54%	0,6	0,90
U7	P3	64%	58%	61%	0,87	0,69
U8	P1	70%	64%	67%	1	0,79
U9	P2	78%	73%	75,5%	0,9	0,93
U10	P1	59%	50%	54,5%	0,83	0,99
U11	P1	62%	57%	59,5%	0,8	0,99
U12	P3	40%	30%	35%	0,5	0,99
U13	P2	53%	44%	48,5%	0,85	0,97
U14	P3	80%	78%	79%	0,88	0,87
U15	P2	73%	70%	71,5%	1	0,923

Table 2: Data obtained from external sources.

User ID	Provider ID	Feedback	F1	F2	F3	F4
U1	P1	0,7	0	0	0	0
U2	P3	0,8	1	3	2	5
U3	P3	0,7	2	0	3	0
U4	P1	0,6	1	1	1	1
U5	P2	0,6	0	2	0	1
U6	P2	0,3	0	3	2	1
U7	P3	0,7	2	1	2	3
U8	P1	0,4	1	1	2	0
U9	P2	0,8	3	2	3	3
U10	P1	0,7	1	2	2	5
U11	P1	0,8	6	1	1	3
U12	P3	0,2	0	1	2	2
U13	P2	0,3	2	9	2	3
U14	P3	0,9	3	2	0	0
U15	P2	0,7	5	3	4	0

Table 3: Indicator results and reputation.

User ID	provider ID	Objective	Subjective	Reputation
U1	P1	0,85	0,7	0,810
U2	P3	0,8	0,7	0,775
U3	P3	0,7	0,71	0,706
U4	P1	0,84	0,84	0,843
U5	P2	0,83	0,57	0,758
U6	P2	0,65	0,525	0,615
U7	P3	0,73	0,62	0,702
U8	P1	0,83	0,44	0,715
U9	P2	0,85	0,72	0,819
U10	P1	0,77	0,61	0,726
U11	P1	0,77	0,7	0,755
U12	P3	0,57	0,74	0,624
U13	P2	0,76	0,50	0,683
U14	P3	0,87	0,82	0,860
U15	P2	0,77	0,6	0,728

tables. In addition, Table 3 also shows the reputation values for each user.

Summing up, Figure 2 shows the users reputation values. The x axis of Figure 2 shows distribution of users at the providers, through the users' identifiers (U1 to U15) associated with the providers' identifiers (P1 to P3). The y axis presents reputation values calculated for each user, ranging from 0 to 1, where value 1 represents the best reputation. By observing values presented, it is possible to notice that user 14 (U14) who used the services of provider 3, obtained the highest reputation value among all users, whose value is close to 85%.

This value is related to the historic average use of computational resources, since U14 presents the highest resources use average (Equation 6 when compared to the other users, according Table 1. Moreover, it performs most of the monthly/annuity pay-

ments on time and presents good connection stability, as it is possible to see in Table 1. In addition, user 14 obtained high average comprising providers' feedback values, despite having a total of 5 pending issues at external sources, as shown in Table 2. Thus, for this user, objective credibility indicator is 0.87 and subjective credibility indicator is 0.82, demonstrating balancing between objective and subjective behavior. Values shown by Figure 2 for user 12 (U12), who also used services of provider 3, obtained the lowest reputation value among all users. User 12 reputation value is close to 62%.

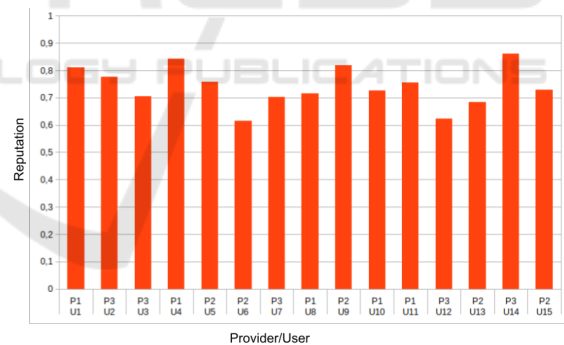


Figure 2: Reputation results.

This value is related to the use of computational resources, which obtained the lowest average when compared to the other users, with the accomplishment of half of the monthly/annuity payments on time, but with a high value for the connection stability indicator, as can be seen in Table 1. In addition, user 12 obtained a low average of the provider's evaluation feedback values, and has a total of 5 pending issues with external sources, as shown in Table 2. Thus, for this user, the objective credibility indicators obtained a value of 0.57 and the subjective credibility indicator obtained a value of 0.74. Thus, the reputation value R(s) for this user is 0.444. Weight of each of these

indicators was defined as 0.7 and 0.3 respectively for all participating providers.

Results show that it is possible to evaluate the users reputation based on the use of computational resources.

6 FINAL CONSIDERATIONS

This work proposed a reputation architecture for cloud providers' users reputation architecture based on blockchain consortium model. The proposed architecture aims to help cloud providers to prevent resource access to malicious users i.e., those whose reputation value is low enough to be considered malicious according to providers security policy definitions. However, it is not restricted to this context and it can be adapted and used by other computer systems. Users have their reputations calculated by combining objective and subjective credibility indicators. The objective credibility indicator is calculated with the user resources utilization like memory, processing, connection stability and payment. The subjective credibility indicator is calculated with the data obtained in external data sources and the providers feedback regarding user's activities performed on the provider. These two indicators make up the reputation value assigned to each user. Thus, reputation value can be used by participating providers to assist in their access control decisions. Results were obtained through simulations performed with hypothetical scenarios. In this way, participating providers have access to user's reputation values based on interactions with themselves and with other participating providers through a shared and collaboratively maintained reputation architecture. As future work, tests are being developed with a greater number of providers and users to assess architecture scalability and performance.

REFERENCES

- Berrached, A. and Korvin, A. (2006). Reinforcing access control using fuzzy relation equations. In *Security and Management*.
- Donghong, S., Wu, L., Ping, R., and Ke, L. (2016). Reputation and attribute based dynamic access control framework in cloud computing environment for privacy protection. In *2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, pages 1239–1245.
- Du, X., Xu, J., Cai, W., Zhu, C., and Chen, Y. (2019). Oprc: An online personalized reputation calculation model in service-oriented computing environments. *IEEE Access*, 7:87760–87768.
- Greve, F., Sampaio, L., Abijaude, J., Coutinho, A. A., Valcy, I., and Queiroz, S. (2018). Blockchain e a revolução do consenso sob demanda. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) - Minicursos*, chapter 5, page 30. Sociedade Brasileira de Computação - SBC.
- Hendriks, F., Bubendorfer, K., and Chard, R. (2014). Reputation systems: A survey and taxonomy. *Journal of Parallel and Distributed Computing*, 75.
- Jansen, W. and Grance, T. (2011). Sp 800-144. guidelines on security and privacy in public cloud computing. Technical report, U.S Department of Commerce, Gaithersburg, MD, USA.
- Lin, I.-C. and Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *I. J. Network Security*, 19:653–659.
- Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., and Leaf, D. (2012). *NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292)*. CreateSpace Independent Publishing Platform, USA.
- Mui, L., Mohtashemi, M., and Halberstadt, A. (2002). A computational model of trust and reputation. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pages 2431–2439, Big Island, HI, USA. IEEE.
- Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system,” <http://bitcoin.org/bitcoin.pdf>.
- Nkosi, L., Tarwireyi, P., and Adigun, M. O. (2013). Detecting a malicious insider in the cloud environment using sequential rule mining. In *2013 International Conference on Adaptive Science and Technology*, pages 1–10, Pretoria, South Africa. IEEE.
- Thakur, S. and Breslin, J. G. (2019). A robust reputation management mechanism in the federated cloud. *IEEE Transactions on Cloud Computing*, 7(3):625–637.
- Wu, L., Zhou, S., Zhou, Z., Hong, Z., and Huang, K. (2015). A reputation-based identity management model for cloud computing. *Mathematical Problems in Engineering*, 2015:1–15.
- Xu, J., Du, X., Cai, W., Zhu, C., and Chen, Y. (2019). Meurep: A novel user reputation calculation approach in personalized cloud services. *PLOS ONE*, 14(6):1–15.
- Yu, X., Gao, N., and Jang, W. (2010(8)). Research on the identity authentication technology in cloud computing. In *Information Network Security*, pages 71–74.
- Zheng, R., Chen, J., Zhang, M., Wu, Q., Zhu, J., and Wang, H. (2018). A collaborative analysis method of user abnormal behavior based on reputation voting in cloud environment. *Future Gener. Comput. Syst.*, 83(C):60–74.