CLOUTIDY: A CLOUD-BASED SUPPLY CHAIN MANAGEMENT SYSTEM USING SEMAR AND BLOCKCHAIN SYSTEM

Nafa Zulfa[1], Hafara Firdausi[2], and Rakha Asyrofi[3]
[1, 2, 3] Department of Informatics, Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia 60111
e-mail: nafazulfa.19051@mhs.its.ac.id[1], hafara.19051@mhs.its.ac.id[2], asyrofi.19051@mhs.its.ac.id[3]

ABSTRACT

Supply chain management (SCM) system is an essential requirement for companies and manufacturers to collaborate in doing business. There are many techniques to manage supply chains, such as using Excel sheets and web-based applications. However, these techniques are ineffective, insecure, and prone to human error. In this paper, we propose CLOUTIDY, a cloud-based SCM system using SEMAR (Service Market) and Blockchain system. We modify JUGO architecture to develop SEMAR as a broker between users and cloud service providers. Also, we apply the Blockchain concept to store the activity log of the SCM system in a decentralized database. CLOUTIDY system can solve several common cases: service selection, resource provisioning, authentication and access control. Also, it improves the security of data by storing each activity log of the supply chain management system in the Blockchain system.

Keywords: Blockchain, cloudity, cloud as a service, smart contracts, supply chain management.

CLOUTIDY: SISTEM *SUPPLY CHAIN MANAGEMENT* BERBASIS *CLOUD* MENGGUNAKAN SISTEM SEMAR DAN *BLOCKCHAIN*

Nafa Zulfa[1], Hafara Firdausi[2], dan Rakha Asyrofi[3]
[1, 2, 3] Departemen Teknik Informatika, Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia 60111
e-mail: nafazulfa.19051@mhs.its.ac.id[1], hafara.19051@mhs.its.ac.id[2], asyrofi.19051@mhs.its.ac.id[3]

ABSTRAK

Sistem *Supply Chain Management* (SCM) merupakan kebutuhan pokok bagi perusahaan dan produsen untuk berkolaborasi dalam melakukan bisnis. Ada banyak cara untuk mengelola *supply chain*, misalnya menggunakan Excel *sheets* dan aplikasi berbasis web. Namun, cara-cara tersebut tidak efektif, tidak aman, dan rentan terhadap kesalahan manusia. Pada *paper* ini, kami mengusulkan sebuah sistem SCM baru bernama CLOUTIDY, yakni sistem SCM berbasis cloud menggunakan sistem *Service Market* (SEMAR) dan Blockchain. Kami memodifikasi arsitektur JUGO untuk mengembangkan SEMAR sebagai penghubung antara pengguna dan penyedia layanan *cloud*. Kami juga menerapkan konsep Blockchain untuk menyimpan log aktivitas sistem SCM ke dalam basis data yang terdesentralisasi. Sistem CLOUTIDY dapat menyelesaikan beberapa kasus umum, yaitu pemilihan layanan, penyediaan sumber daya, serta autentikasi dan kontrol akses. Selain itu, sistem ini juga mampu meningkatkan keamanan data dengan menyimpan setiap log aktivitas dari sistem SCM ke dalam sistem Blockchain.

Kata kunci: Blockchain, cloudity, cloud as a service, smart contracts, supply chain management.

I. INTRODUCTION

People used to use Excel sheets to update data of the current stage in their supply chains [1]. However, this traditional supply chain management method is ineffective, insecure, and prone to human errors. It must be replaced by an automated system that requires less human intervention. Currently, a better approach to manage the supply chain emerges by using a web-based application hosted on a server owned by a company or hosted on the virtual server provided [1].

Setting up and hosting applications at servers are not a good choice because there are many technical aspects to consider, such as load balancing, scaling, failure detection, etc. Therefore, cloud service providers (CSP) come as a solution. The cloud service providers deliver services to their users directly with preconfigured services. However, this mechanism is sometimes detrimental to users because they have to pay for certain services they do not need

and use [2]. On the cloud service providers side, vendor lock-in is a major problem [3]. It is a situation where users are stuck with one vendor because the cost of switching to a different vendor is very high. Also, resource fragmentation is a big problem in allocating cloud service provider resources [4].

The current supply chain management (SCM) system retrieves and stores data in a centralized database. It is a database usually stores data or information at a single location within a network. It makes every organization member could retrieve, update, and analyze the stored database [5]. Unfortunately, it has several shortcomings. First, the centralized database has no failure-tolerance mechanism since it is located and maintained in a central computer or database system, such as a server or a desktop computer. If a failure occurs on the server, all data will be lost. Second, the centralized database is prone to data modification by irresponsible people because of its advantages to ease sharing, updating, or analyzing [6]. Finally, the centralized database is unable to handle a high capacity of data, let alone to process it [7].

In this paper, we present CLOUTIDY, a cloud-based supply chain management system using SEMAR and Blockchain system to solve the abovementioned problems. The SEMAR system functions as a broker between users and CSPs [8]. It will select CSPs with the highest compatibility and lowest price based on user requirements. CLOUTIDY system also utilize the concept of Blockchain to improve the security of data by storing each activity log of the SCM system in a decentralized system [1]. It uses a peer-to-peer network to enforce transactional integrity as well as security [9]. We design a CLOUTIDY system that can solve several common cases: service selection, resource provisioning, authentication and access control, also blockchain. This way, the proposed CLOUTIDY system can be more secure and effective in managing supply chains.

The rest of this paper is organized as follows: Section 2 presents some works related to the topic of this paper. Section 3 explains the detailed mechanism of the proposed CLOUTIDY system. Section 4 describes the operational model of this proposed system. Section 5 discusses the difference between the proposed system and the previous system, and Section 6 summarizes this paper.

II. RELATED WORK

Cloud service management is an essential building block of cloud architectures [10]. It can be extended to act as a broker service layer between consumers and cloud service providers (CSP). A lot of research conducted to develops third-party broker architecture for selecting cloud services based on user requirements [11]. However, these works did not consider a platform composed of multiple CSPs with different service capabilities. Therefore, research conducted by [8] develops a generic architecture for delivering composite cloud services based on user requirements called JUGO. It provides service negotiation, delivery, and management between different types of cloud resources and users. We adapt JUGO architecture to develop a broker architecture built specifically for managing supply chain called SEMAR (Service Market). The SEMAR system connects companies and manufacturers with several CSPs that host Supply Chain Management (SCM) system and Blockchain system.

Blockchain system is a peer-to-peer network containing several participants that are connected one each other via the Internet. Blockchain allows each participant to retrieve, store, and validate records in the database [12]. However, any stored record cannot be altered, without the alteration of all subsequent blocks. Also, each participant checks the log history whether any discrepancy or difference in each node. This mechanism makes the Blockchain system is resistant to the modification of data [13].One research stated that information of the order and update in tracking details, as well as details of customers, sellers, raw material manufacturers, assemblers, and others, must be centralized [1]. However, the existing supply chain management (SCM) system has a shortcoming, that is each member (i.e. company and manufacturer) in the SCM system stores data separately, making it difficult to integrate data. Currently, data integration still a challenge because of (1) Volume: there are a huge volume of data to store and process; (2) Variety: there are many types of data and their sources; (3) Velocity: there are requirements for speed in data analytics since the data flows quickly; and (4) Veracity: there are requirements for understanding the data you can trust for financial reports, etc [14]. A cloud integration approach can lead to better data management, more accurate analysis, and ensure consistency of data across the systems. However, this approach still vulnerable to the modification of data. Therefore, we utilize the concept of Blockchain to improves the security of data in the cloud [15].

Communication between consumers and CLOUTIDY system needs a modeling mechanism for collecting data. A research conducted by [16] introduces a prototyping model to collect the patient's vital signs continuously, then unify the data by sending it to microcontrollers. Furthermore, the microcontrollers send the data to fog devices alternately. We can use this model to collect log activities of SCM system and send them to the SEMAR system.
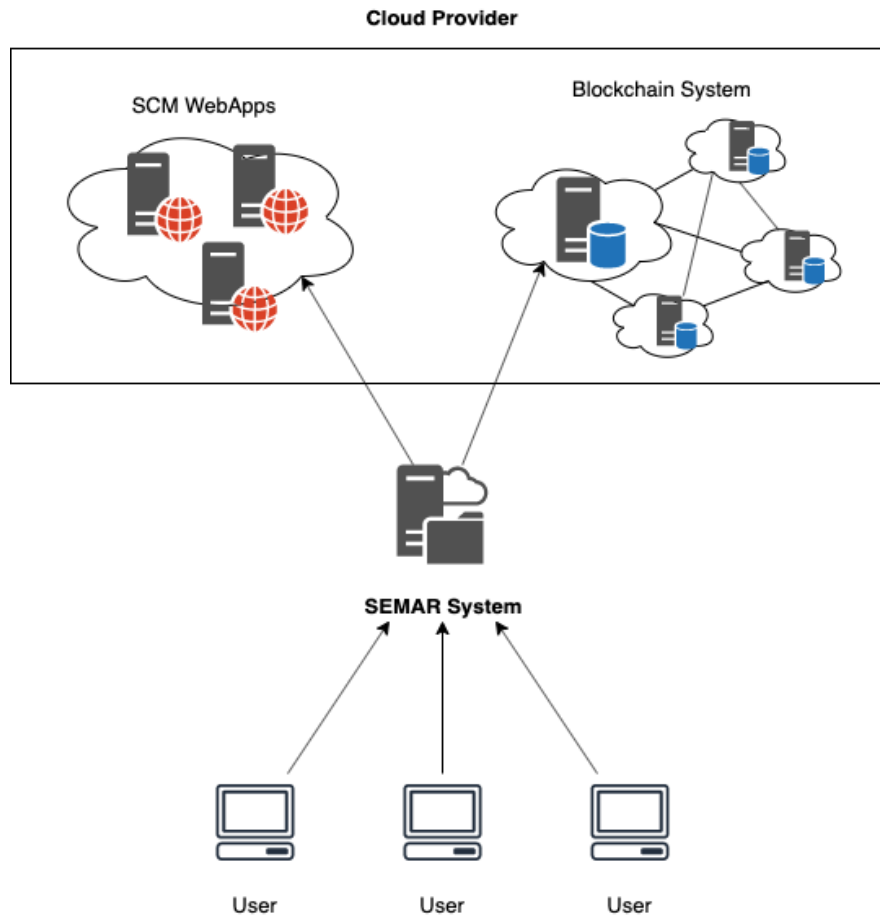
Fig. 1. CLOUTIDY system architecture.

As a future work, we can utilize several container engines to support CLOUTIDY system. Container engines employed because its efficiency and portability because containers virtualize the operating system instead of hardware [17].

III. METHODOLOGY

The proposed CLOUTIDY system contains four main parts: (1) the SCM system, (2) the SEMAR system, (3) the Blockchain system, and (4) various CSPs. First, the main company builds a SEMAR system that can be deployed together with other related companies or manufacturers in the supply chain network. They utilize the SEMAR system to select CSP with the highest compatibility and lowest price based on the required specifications.

In the process, SEMAR provides a list of CSP recommendations to users instead of directly determine the CSP. The user selects the preferred CSP from the recommendation list, then the SEMAR system sends a request to the selected CSP to build and deploy the SCM system on the virtual servers. The same mechanism also applies to build and deploy the Blockchain system. After both SCM and Blockchain systems have been built and deployed, the SEMAR system functions as a portal with authentication and access control to connects users and the SCM system. The overall CLOUTIDY system architecture illustrated in Figure 1.

A. Service Market (SEMAR) System

One research [8] proposed a generic architecture for composite cloud as a service called JUGO. We modify JUGO architecture to develop a new broker architecture system called Service Market (SEMAR). It functions to select CSPs with the highest compatibility and lowest price based on user requirements for delivering composite cloud services. The main difference between SEMAR and JUGO is its CSP selection mechanism. SEMAR provides a list of CSP recommendations to users instead of directly determine the CSP. Figure 2 illustrates the architecture of SEMAR system.

SEMAR works as a bridge between users and cloud providers. First, users request for cloud resources. The users send a request that contains requirements, specifications, and budget for a cloud service. SEMAR responses to the request by recommends several CSPs that meet the user's request. Finally, the users select a CSP in the recommendation. Upon the selection, the users will be redirected to the selected CSP. The SEMAR system is divided into three main parts which explained as follows:

1) *Cloud Consumer*

   Different from JUGO, the utilizes of SEMAR services are focused on the business sector, which is supply chain management (SCM). Initially, an SCM system contacts SEMAR to find a suitable cloud service provider to host the SCM system.

2) *SEMAR Cloud Controller*

   a) *Service Catalog (SC)*

   SC has a mechanism as follows: (1) SC sends a request to Ads to get assets from many CSPs; (2) Ads receive some specifications of assets from CSPs; and (3) SC shows the information of assets owned through the asset advertisements.

   b) *Service Integration (SI)*

   SI integrates several services provided by the CSPs.

   c) *Service Provisioning (SP)*

   Resources can be proactive or reactive based on specifications the user wants. Hence, the load balancer will be active and trigger replication and migration. The SCM system can use resources from many CSPs based on the required specifications.

   d) *Event Management (EM)*

   EM consists of two modules as follows: (1) Monitoring, a module that periodically checks and verifies SLAs and QoS that occur; and (2) Alarming, a module that notifies the user when the resources usage has reached the limit, so that users can take the next step.

   e) *Security*

   Security is used to record all activity logs that occur. There are also authentication methods to restrict the access rights of the user.

   f) *Service Billing and Reporting*

   Service billing is used to allocate a bill against cloud service providers who registers the service through SEMAR, while service reporting is used to display reports related to SEMAR usage and existing Service Level Agreement (SLA).

   g) *Management and Operation Console (MO)*

   MO is an interface or console where users can operate SEMAR and use the features in it.

   h) *Authentication Service (AS)*

   AS is used to authenticate the user that will access the service. Therefore, only genuine users can access the account.

   i) *Service Audit (SA)*

   SA is related to the user's activity log and all information in the user's account.

   j) *Access Control (AC)*

   AC controls the access rights of each user to the services (access control).

3) *Cloud Service Providers (CSP)*

   a) *Reusable Assets*

   Reusable assets are CSP's essential assets. SEMAR architecture stores the data of reusable assets in the database, so it is not necessary to check the data regularly.

   b) *Asset Discovery*

   SEMAR provider creates a contact to CSP to get new assets information. Hence, SEMAR can get access to retrieve assets information by checking the asset discovery of CSP.

   c) *Billing and Reporting*

   Billing and reporting related to CSP billing fund report.

B. Blockchain

   The utilize of Blockchain concept in the CLOUTIDY system is to improve the security of data by storing each activity log of the SCM system on the decentralized database. The detailed mechanism of Blockchain system described as follows:

1) *Set-up Etherium Node*

   Ethereum is a blockchain network. Each entity must set up a high computational power machine called Ethereum node to create an Ethereum blockchain. One of the applications we can use to create an Ethereum
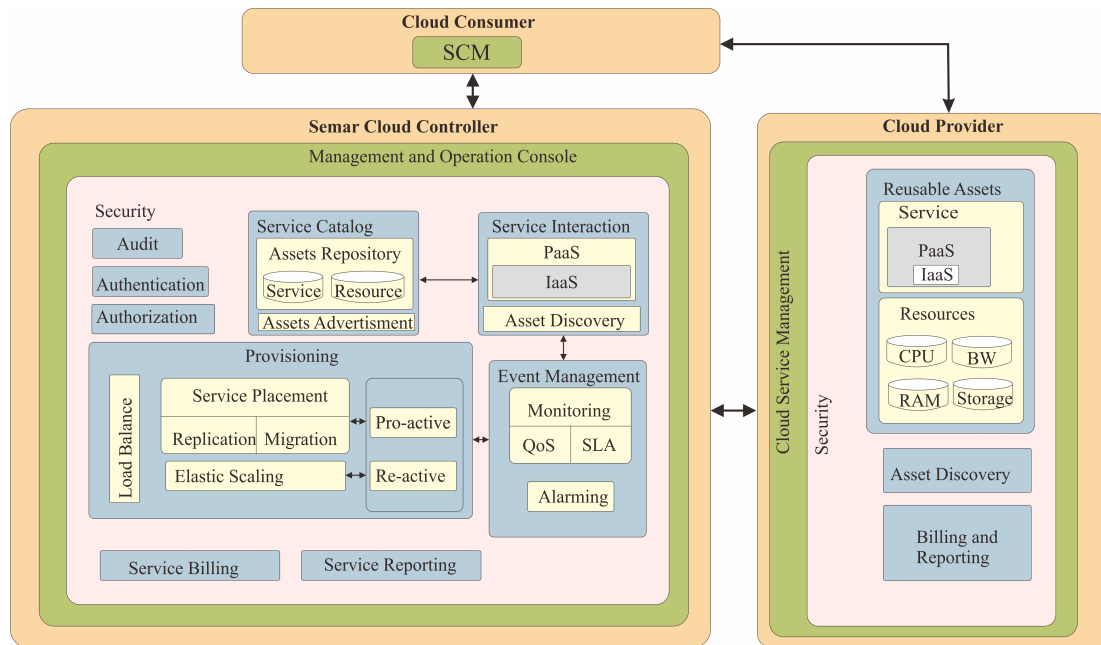
Fig. 2. SEMAR (Service Market) system architecture.

node is GoEthereum or 'that available to various platforms.

2) *Create Smart Contract*

Smart Contracts are floating databases found on all the participants at a particular address. The address is the contact point to the actual database. Smart Contracts written in a language known as Solidity that compiled through online compilers, such as RemixIDE.

3) *Create a Distributed Application*

Distributed Application (DAPP) is a web application which created specifically to fetch or upload data from or to a Smart Contract ledger. It is built using HTML/CSS, MeteorJS, and an API [1] called Web3JS as a gateway to the Etherium blockchain network.

The advantages of these three methods are: (1) decentralized data distribution, (2) increasing transparency, (3) making the system more flexible, (4) increasing the flow of data collection, and (5) displaying product histories from the beginning of production until the process.

IV. OPERATIONAL MODEL

In this section, we present four types of sequence diagrams and corresponding operational models for the proposed CLOUTIDY system.

A. Service Selection

Service Selection is a buying service process using the SEMAR system. First, users send a service specification request for SC through MO as the interface. Then, MO forwards the service request to SC. SC analyzes the user request based on available assets in several CSPs stored in the database. SC calls SI to interact CSPs and SEMAR. CSPs send feedbacks of asset lists to SI. SI sends the asset list from CSPs to SC. SC processes searches the matches CSP according to service specification. After finding the matches CSP, SC sends the recommendation to MO. Then, the user can select the best suitable CSP for the user. SEMAR interacts with SP to allocate the asset. Finally, the user is notified on which asset is ready to use. Service selection process on the SEMAR system is illustrated in Figure 3.

B. Resource Provisioning

Periodically EM will be monitoring the performance and the allocated service status of CSP using SEMAR system. Event management evaluates the service status of CSP using Service Level Agreement (SLA) and activates the alarm when there is a change in Quality of Service (QoS). Provisioning is used to improve the performance and maintenance of the SLA and the QoS. Resource provisioning process on the SEMAR system is illustrated in Figure 4. First, EM receives the service status based on service ID from CSP. Then, CSP populate status from the database and sends it to EM. Subsequently, EM evaluates the status of service ID against SLA and invokes alarm service to notify the user. Afterward, Users request provisioning to EM. EM forward the requests provisioning to PS and PS retrieves actions and provisioning options. Finally, PS performs provisioning to the CSP.
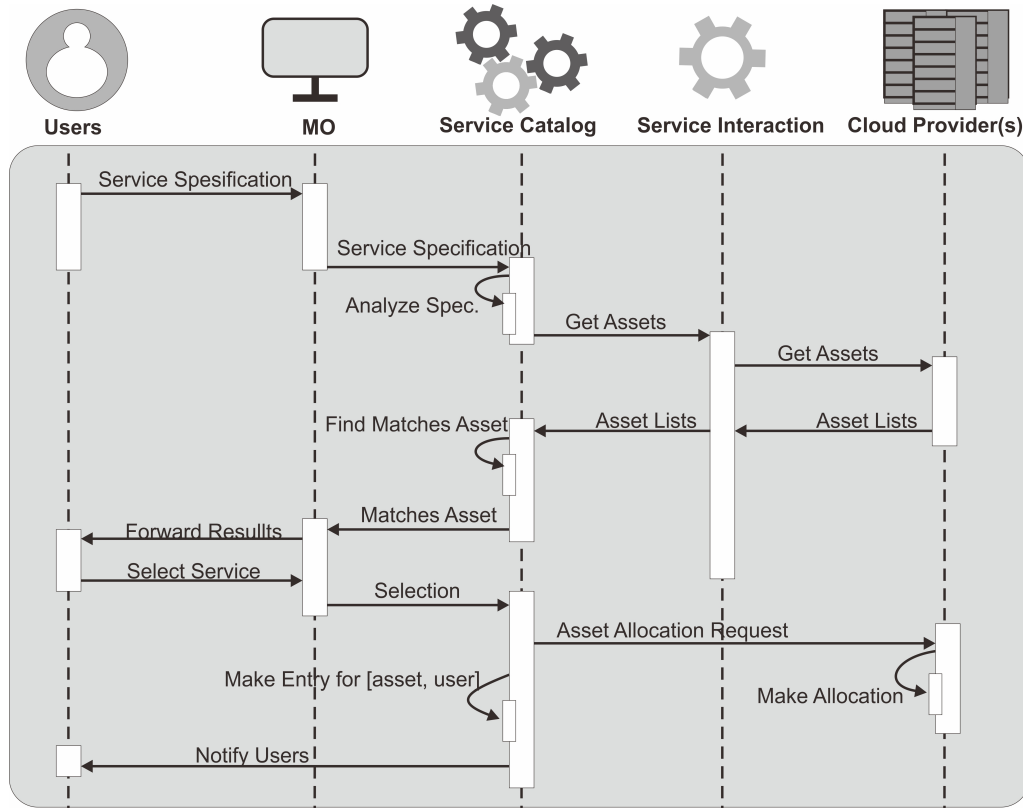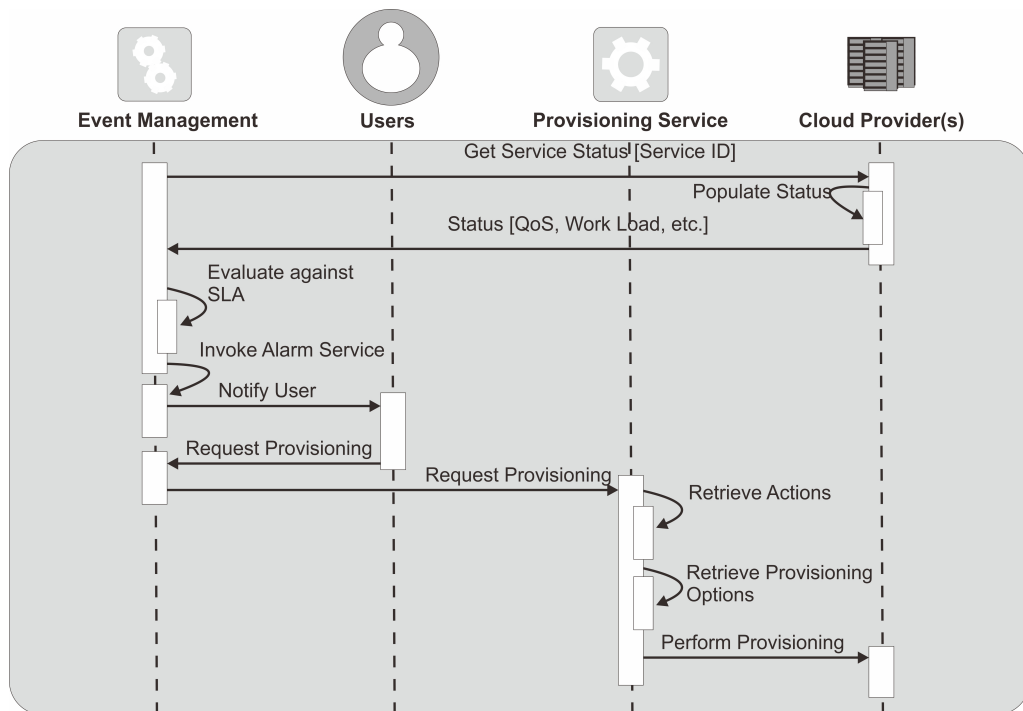
Fig. 3. Service selection on SEMAR.
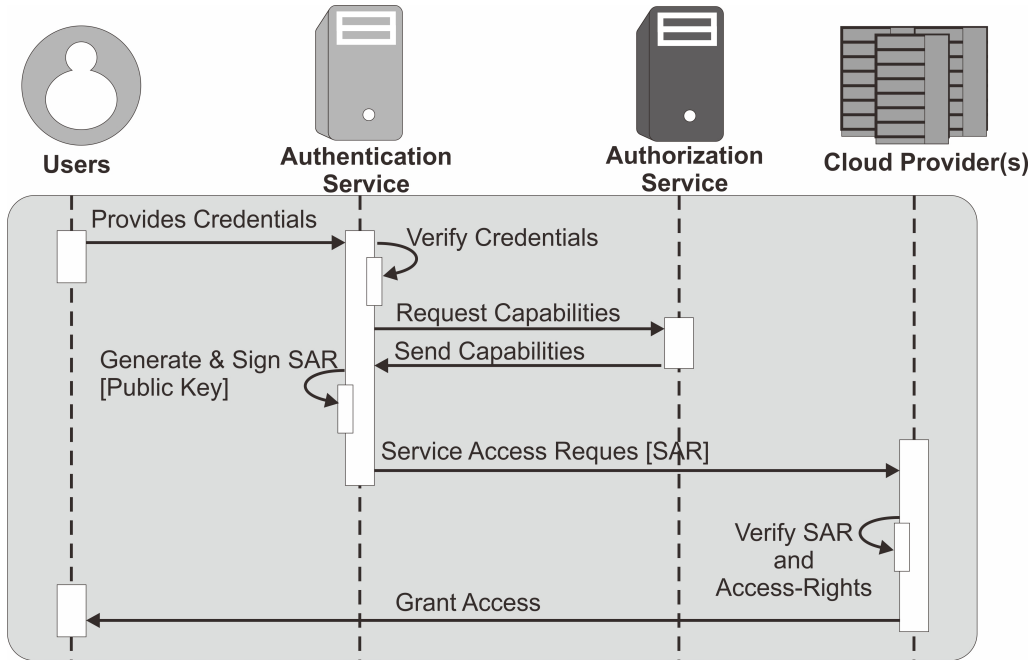
Fig. 4. Resource provisioning on SEMAR.

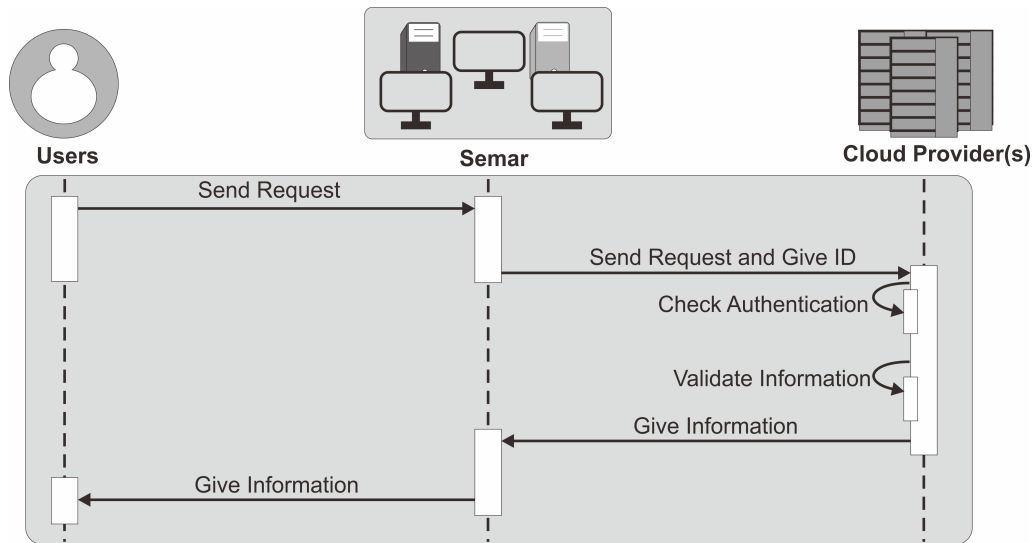Fig. 5. Authentication service and access control on SEMAR.

Fig. 6. Getting information from blockchain system in CSPs.

C. Authentication Service (AS) and Access Control (AC)

There is an AS and AC process in SEMAR to protect the user accounts that illustrated in Figure 5. AS used to confirm the person who is login to SEMAR is the right person. ATS used to determine every user account function. Every user has different credentials that makes SEMAR more secure. The credential used to login to SEMAR. First, user logins to SEMAR system using his credential. The credential sent to SA. SA verifies the credential to the database. After verifying the credential, SA makes request capabilities to ATS. ATS sends feedback capabilities to AS. Then, AS generates Service Access Request (SAR) and registers it into SEMAR. Upon the registration, AS sends an issue SAR to CSP. Then, CSP gets the public key from AS and verifies SAR to verify Access-Rights. Upon verification, CSP sends Grant Access to the user.

D. Blockchain

Blockchain is used to secure the database records on many CSPs. Before update the database record, the record will be checking on every member of the blockchain. Blockchain not only checking the record before updating but also permitting every member to validate record on the database when it needed. The Blockchain process is illustrated in Figure 6. The user requests the required information to SEMAR. SEMAR sends ID and request to

specific CSP. CSP checks user authentication, finds information and validates the information. Upon the validation, CSP gives the information to SEMAR. SEMAR forwards the information to the user.

V. Discussion

The proposed CLOUTIDY system requires architecture to act as a broker service layer between users and cloud service providers (CSPs). There is a generic architecture named JUGO that delivers composite cloud services based on user requirements. This architecture is efficient because it selects CSPs with the highest compatibility and lowest price based on user requirements. Regardless of efficiency, this architecture is scalable too. Therefore, we utilize JUGO architecture as a broker service layer of the proposed CLOUTIDY system. We name the improved-JUGO architecture as SEMAR architecture.

JUGO's security service only provides authentication, access control, and accounting for cloud users and CSPs. Authentication security service manages the user's credentials and Service Access Tokens (SAT). Hence, only verified and provisioned JUGO users can bypass the JUGO and directly access the cloud resources by presenting the SATs. While access control security service provides policies to define service and resource privileges for each user. However, JUGO does not provide the most important aspect required by the CLOUTIDY system, which is a robust mechanism of data security. Hence, we improve the data security of SEMAR against data modification by storing each activity log of the SCM system in the Blockchain system.

JUGO architecture focuses on a unified platform for service negotiation, delivery, and management between different types of cloud resources and users. On the other hand, SEMAR architecture focuses on the security of data against data modification because this architecture specifically designed for the supply chain management system. We also make an operation model of SEMAR architecture in Section 4 which shows that the Blockchain system might work well in the CLOUTIDY system. It can resolve some common cases in cloud computing, such as resource fragmentation and vendor lock-in, service selection, resource provisioning, and security.

VI. Conclusion

The proposed CLOUTIDY system introduces a cloud-based supply chain management system that utilizes the SEMAR architecture and Blockchain system to enables companies and manufacturers in exchanging information more securely. The SEMAR architecture functions as a connector between users and CSPs. It allows users to choose CSP with the highest compatibility and lowest price based on their requirements. Also, the SEMAR system functions as a portal equipped with authentication and access control for users to access the SCM system hosted in the CSPs. The Blockchain system store the activity log of the SCM system in scattered locations. The activity logs are synchronized to maintain its validity. Based on the operational models that we have shown in Section 4, our proposed CLOUTIDY system can resolve various common cases in cloud computing, such as resource fragmentation and vendor lock-in, through the mechanisms provided: service selection, resource provisioning, authentication and access control. Also, the CLOUTIDY system improves its security of data against data modification by storing each activity log of the SCM system in the Blockchain system.

References

[1] V. Naidu, K. Mudliar, A. Naik, and P. Bhavathankar, "A Fully Observable Supply Chain Management System Using Block Chain and IOT," in *Proc. International Conference for Convergence in Technology*, 2018.

[2] R. Buyya, "Market-oriented cloud computing: Vision, hype, and reality of delivering computing as the 5th utility," in *Proc. IEEE/ACM International Symposium on Cluster Computing and the Grid,* 2009.

[3] B. S. Lee, S. Yan, D. Ma, and G. Zhao, "Aggregating IaaS service," in *Proc. Annu. SRII Glob. Conf. SRII*, pp. 335–338, 2011.

[4] L. Tomás, B. Caminero, and C. Carrión, "Improving grid resource usage: Metrics for measuring fragmentation," in *Proc. IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing,* 2012.

[5] R. Elmasri and S. B. Navathe, *Fundamentals of Database Systems Sixth Edition*. 2016.

[6] A. Mohammed and B. M. Saleh, "Centralized Database: A Prerequisite for Security and Sustainable Development in Nigeria," *Int. J. Innov. Res. Comput. Sci. Technol.*, 2017.

[7] Y. Januzaj, J. Ajdari, and B. Selimi, "DBMS as a Cloud service: Advantages and Disadvantages," *Procedia - Soc. Behav. Sci.*, 2015.

[8] M. Hossain, R. Khan, S. Al Noor, and R. Hasan, "Jugo : A Generic Architecture for Composite Cloud as a Service," in *Proc. Int. Conf. Cloud Comput.*, pp. 806–809, 2016.

[9] R. Patgiri, I. Acharjamayum, and D. Devi, "Blockchain: A Tale of Peer to Peer Security," in *Proc. IEEE Symposium Series on Computational Intelligence*, 2018.

[10] F. Fowley, C. Pahl, P. Jamshidi, D. Fang, and X. Liu, "A Classification and Comparison Framework for Cloud Service Brokerage Architectures," *IEEE Trans. Cloud Comput.*, 2018.

[11] S. Sundareswaran, A. Squicciarini, and D. Lin, "A brokerage-based approach for cloud service selection," in *Proc. IEEE International Conference on Cloud Computing,* 2012.

[12] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues," *Futur. Gener. Comput. Syst.*, 2019.

[13] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security and Privacy Workshops,* 2015.

[14] D. Zburivsky, "Dismantling Data Silos through Cloud Integration," Data Summit, Boston, MA, May 2017.

[15] L. Xu, L. Chen, Z. Gao, Y. Lu, and W. Shi, "CoC: Secure supply chain management system based on public ledger," in *Proc. International Conference*

on Computer Communications and Networks, 2017.

[16] K. Monteiro, E. Rocha, E. Silva, G. L. Santos, W. Santos, and P. T. Endo, "Developing an e-health system based on IoT, Fog and cloud computing," in *Proc. IEEE/ACM International Conference on Utility and Cloud Computing Companion*, 2019.

[17] D. Elliott, C. Otero, M. Ridley, and X. Merino, "A Cloud-Agnostic Container Orchestrator for Improving Interoperability," in *Proc. IEEE International Conference on Cloud Computing*, 2018.