A Semantic Model with Self-Adaptive and Autonomous Relevant Technology for Social Media Applications

Zahra Najafabadi Samani*, Alexander Lercher, Nishant Saurabh, and Radu Prodan

Institute of Information Technology, University of Klagenfurt, Austria.
{zahra,alexander,nishant,radu}@itec.aau.at

Abstract. With the rapidly increasing popularity of social media applications, decentralized control and ownership is taking more attention to preserve user's privacy. However, the lack of central control in the decentralized social network poses new issues of collaborative decision making and trust to this permission-less environment. To tackle these problems and fulfill the requirements of social media services, there is a need for intelligent mechanisms integrated to the decentralized social media that consider trust in various aspects according to the requirement of services. In this paper, we describe an adaptive microservice-based design capable of finding relevant communities and accurate decision making by extracting semantic information and applying role-stage model while preserving anonymity. We apply this information along with exploiting Pareto solutions to estimate the trust in accordance with the quality of service and various conflicting parameters, such as accuracy, timeliness, and latency.

Keywords: semantic information, community detection, Pareto-trust, decentralized social media, role-stage model.

1 Introduction

Recently, decentralized social media applications (e.g. crowd journalism, car sharing, collaborative video creation) is gaining traction. Such systems with underlying decentralized social media orchestrate diverse actors into a permission-less peer-to-peer network with threefold benefits. First, it improves users control with a secure, permanent and unbreakable link to their data. Second, it allows users' content to be secured from any central authority, third parties or unauthorized individuals through a smart contract. Third and foremost, it provides a democratic environment where a user can join or leave the network at any time (based on peer-to-peer principle) with the same right for decision making and voting for a consensus. This will facilitate global availability and decentralized control and ownership. Although such systems truly democratize the technical world of social media, yet they pose some serious challenges [1, 2].

Essentially, decentralized social media is often described as a trust-less system. While inherently they do not actually eliminate trust, they instead minimize the amount of trust required from any single actor in the system. Primarily, such permission-less based social media hinder the process to tackle prominent issues such as fake news, cultural barriers, biased propaganda, trolling, identifying malicious content, and bad social media actors. To mitigate such challenges, there is a need to research for intelligent design addressing trust based on various social media requirements [3]. By contrast, in most previous works trust does not address all the service requirements [4]. Hence, we propose a Semantic Model with self-adaptive and Autonomous Relevant Technology (SMART) architectural framework applying trust through various parameters according to quality of service (QoS) metrics such as accuracy, timeliness, and latency. SMART exploits Pareto solutions and game-theory based optimization approach to find the right and trustworthy subset of users participating in consensus process and social media applications.

However, integrating trust in a permission-less network requires utilizing the contextualized activity traces over the time [5, 1]. More precisely, if activity traces are semantically linked at contextual levels, this would (i) significantly improve detection of the correct set of audience, interested groups and relevant communities, (ii) provide adaptive infrastructure provisioning for time-critical events (e.g. corresponding to an accident via news) across the right subset of user's geo-location, and (iii) inject intelligent insights across different communities, groups, and users into pattern prediction, recommendation and decision making. Finally, it will significantly improve trusted participation in collaborative social media applications.

Several studies were proposed to analyze decentralized network and identify network construction. To the best of our knowledge, those methods mostly focus on link analysis without content analysis to infer activity traces [6–8], while network topology alone can not precisely reveal peers behavior pattern in the network. Hence, SMART adopts a novel community detection approach based on a role-stage model to precisely identify implicit and explicit behaviors and interactions of participants in the network by dynamically extracting semantic information along with network topology while preserving peers privacy and anonymity. In order to give better control over the design, implementation and evolution of the system, we design SMART based on microservices [9].

The paper is organized as follows. Initially, we survey in Section 2 the research background related to our work. Section 3 outlines the architecture of the proposed model, further discussed in Section 4 and followed by possible future directions and open issues. We conclude the paper in Section 5.

2 Related work

In this section we introduce the state of the art barriers existing in the social networks with relation to our research.

Decentralized social media Centralized social media creates critical issues of trust and privacy [1, 2, 10]. Towards this issue, decentralized social media have been proposed to provide more control over private data. While decentralized social media is widely documented to demonstrate availability, democratic decision making, and ownership in the social media, they face their own problems and challenges such as identifying malicious content and bad social media actors, tracking peers behavior pattern and network analyses, and Trust in social media platforms [1, 2, 5]. Here, we briefly review some recent proposed solutions to address these problems.

Identification of malicious actors The anonymization of identities across self sovereign identity in decentralized network make them vulnerable to misbehaviour in the network for illegal interests. Therefore, several studies were proposed to analyse decentralized network for identifying malicious actors. Maesa et al. [11] inferred unusual behavior of outliers by analyzing the Bitcoin users graph. The authors illustrated that these behaviours are a consequence of unusual chains of transactions, which indicated the existence of outliers in the in-degree of frequency distribution and the high diameter of the users graph. To identify attacks, Meiklejohn et al. [12] grouped Bitcoin users by adopting a heuristic based on changed addresses to cluster addresses belonging to the same user. However, this approach considered static network which is in conflict with the reality.

Tracking peers behavior pattern and network analyses To provide appropriate services, it is crucial to have a clear understanding of evolving relationships among data and predict their future trend. However, tracking users behavior in an anonymized heterogeneous environment is very challenging as illustrated by several decentralized network studies. Most of them extracted the user link graph to track users behavior, while transaction graph alone does not declare all of the relationships in the network. The authors in [6, 7] introduced a method for tracing users behavior in decentralized network based on the similarity of sequences extracted from the transactions over the time.

The authors in [6] clustered nodes by exploiting a behavior pattern clustering algorithm after measuring the sequences similarity, while in [7] they adopted an end-to-end neural network to classify peers. The work in [8] provided analyses of the user link graph in Bitcoin to trace users behavior and derived the user graph from the transaction graph by a clustering process. The research in [13] provided a community detection approach (SONIC-MAN) within ego-network of the users to track peers behavior pattern in distributed online social networks. SONIC-MAN is based on a Temporal Trade-off approach adopting a set of super-peers, chosen from the nodes in the ego networks, to the manage communities over time.

Trust in social media platforms Trust plays an important role in decision making, recommendations and consensus reached between multiple users [3].

Therefore, there have been several researches that introduced trust based on different value to offer more relevant services. Azadjalal et al. [4] proposed a method to identify the most trustworthy users for the recommendation process by exploiting a reliability measure and Pareto solution. The authors calculated the unknown rating values to identify trust relationships, however, they did not take into account QoS factors to identify trustworthy users. Alhanahnah et al. [14] provided a trust framework considering factors according to both service characteristics and user perspective in making recommendation, however, they did not assumed dynamic nature of the network, while trust in such dynamic network is a dynamic concept which changes over the time and requires continuous updates [5].

3 SMART Architecture Design

We propose a framework underlying decentralized social media called SMART, capable of finding relevant interest communities without violating users' privacy and anonymity. Its objective is to improve trust and eliminate malicious actors in participatory exchanges and collaborative decision making. To fulfill this goal, we adopt a role-stage model inspired by [15] integrating various facets of social media to define users based on social information and content attributes. We apply this information to estimate trust using game theoretic approaches in accordance with various QoS conflicting parameters, such as accuracy, timeliness, latency, and anonymity preservation. The output of the SMART architecture enables social media applications engage with the correct subset of users based on their QoS requirements. The architecture also improves democratic decision making by choosing trustworthy agents to vote for consensus and reduce cost and latency by analyzing previous voting outcomes and preferences.

Coping with the heterogeneous and dynamic social media infrastructure requires continuous updates and integration of new features without interrupting system operation [9]. To achieve this goal and overcome the limits of a monolithic architecture, we designed the SMART architecture shown in Figure 1 using sixteen different sets of microservices: two for input transactions hub, nine for evolutionary semantic contextual data hub as the main part of architecture, and five for smart results in SMART transaction hub (out). The API gateway takes all the requests and routes them to the message broker for transparent transaction management and communication through message validation, transformation, routing and guaranteed delivery.

3.1 SMART Transaction Hub (In)

SMART transaction hub provides an input interface to schedule and manage input queries and information to SMART framework consisting of trace retrieval and network metrics retrieval microservices.

Trace retrieval microservice provides an input interface to extract the experiential anonymized activity traces required by SMART framework.

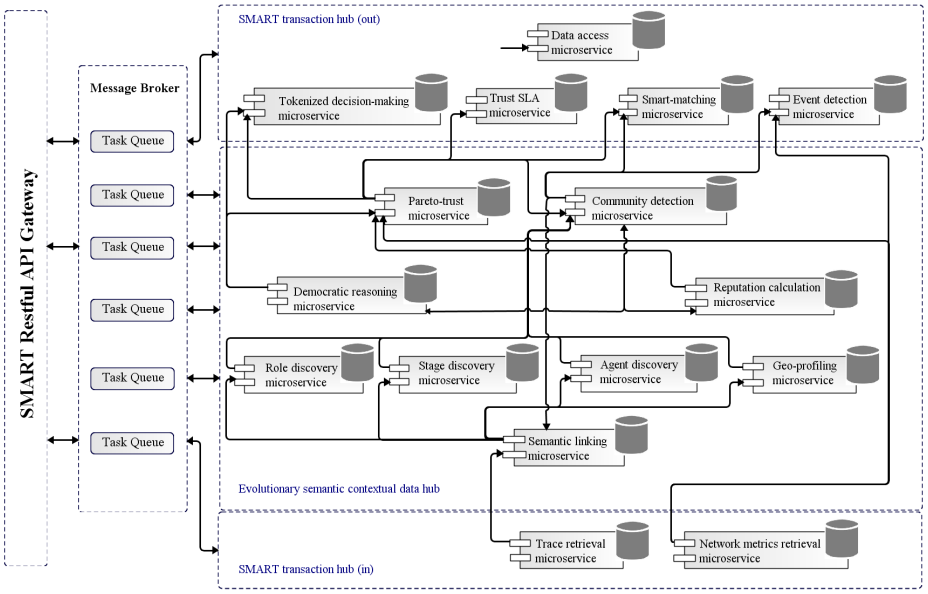

Fig. 1: SMART architecture proposal.

Network metrics retrieval microservice provides an interface for the network-related QoS and quality of experience metrics and runtime information, including their physical network distribution to calculate the Pareto trust. Additionally it will help the event detection service by assigning geo-locations to events.

3.2 Evolutionary Semantic Contextual Data Hub

This hub represents as the main part of the SMART architecture offering intelligent heuristic outputs for crowd-cooperative applications through nine following microservices.

Semantic linking microservice explores complex and evolving relationships among data to have a clear understanding of the network and predict their trend in the future. We formulate the problem to extract semantic data combining event and link analysis for representing peer behaviors in decentralized social media considering dynamic network. Several sequences are usually extracted as the roles and stages for each user over the time to gain valid and valuable insights and information from user patterns, while guaranteeing for preserving users anonymity and privacy when releasing aggregate statistical personal information of individuals. This microservice improves community detection and reveals network properties and role of users in social media by defining implicit and explicit behaviors and interactions of participants in the network.

Agent discovery microservice defines the concept of agents as users and participants in decentralized social networks, where they usually have equal rights in querying, sending transactions, and participating in decision making. We apply this microservice for identifying users to understand the network more deeply and assigning tasks to them in accordance with their roles in the social network.

Role discovery microservice aims to precisely discover communities by specifying agents according to their roles in the social network. The concept of roles improves the conceptualization and community detection in social media since roles can reveal semantic information and interaction between agents. Therefore, we define roles as properties and behaviors assumed by agents over time and place. In this microservice, we characterize agents by multiple roles as also taken by people in the real world [16]. For example, a person usually belongs to several social groups such as family, friends, and colleagues.

Stage discovery microservice detects the interaction between different roles in the social media represented as sequences of stages, where each stage contains the details of the role's actions. Detection of these stages can be beneficial for discovering communities and agents based on their role in the social media.

Community detection microservice helps in deeper network understanding and reveals interesting properties shared by the members [1, 13]. Detection of these communities can be beneficial for numerous topics such as recommendation systems, link prediction, anomaly detection, information spreading, and finding of like minded marketing users [16]. Existing studies on community detection mainly focus on link analysis or topological network structure that ignores content analysis for community finding. The drawback is that each community identified by these methods can only reflect the strength of the connections, while in reality a social network community is a group of users not only sharing common events and friends, but also having similar interests [17]. Moreover, the amount of covert information extracted from a network is very limited. On the other hand, most of these studies assume that every node belongs to exactly one non-overlapping community, while people in a real social network naturally belong to multiple community. Thus, it is more reasonable to cluster users into overlapping communities [16]. We propose a novel approach that combines event clustering and link analysis to detect communities along with clustering users into overlapping communities via agent, role, stage discovery microservices.

Reputation calculation microservice that increases trust is an essential factor of a successful social network [3]. Generally, the security provided by decentralized social media is better than by a centralized data management, however, there are still trust issues as attacks are inevitably growing by exploiting decentralized ownership vulnerabilities. The reputation measures the amount of community trust achieved based on previous interactions.

Nevertheless, integrating trust in complex and dynamic scenarios where users are heterogeneous and anonymous is very difficult. Moreover, trust is a dynamic concept which changes over the time [5]. Hence, we provide a model for trust computing in accordance with the temporal factor of user's interactions. Reputation systems on decentralized social media have different goals, from choosing reliable resources to the quality of content of a shared file [3]. Therefore, the reputation needs to be addressed in many different ways according to the various services over time. For example, in crowdsourced journalism reporting on recent events, (in contrast to other informational content shared online), news is valued much more in terms of timeliness, accuracy, geo-location. Therefore, we propose efficient trust based heuristics using a game theoretic approach and community detection to estimate devices' trustworthiness considering various conflicting parameters, such as accuracy, timeliness, latency, and high anonymity preservation.

Pareto trust microservice considers trust through various parameters according to domain of services and QoS performance metrics such as accuracy, timeliness, and latency. However, these conflicting trust-based factors need to be simultaneously optimized to achieve an optimal solution.

To solve this multi-objective optimization problem where there is a trade-off between trust-based elements, we adopt cooperative game-theory based optimization algorithm to obtain the true Pareto-optimal frontier. Cooperative game theory is a mathematical model providing multi-objective optimization where multiple decision makers are involved in decision-making exploiting learning approaches to find an elitist spread of solutions [18].

Democratic reasoning microservice serves as a central knowledge-based component providing all facts and rules for other microservices. Hence, other microservices follow this rules for evaluation and execution.

Geo-profiling microservice provides a mapping of agents location in the network over the time. This microservice will help classify agents depending on their locations to improve community detection and enable social media applications engage with smart devices closest in proximity to the event locations.

3.3 SMART Transaction Hub (Out)

This hub offers outputs and elicit solutions for various social media applications taking advatage of evolutionary semantic contextual data hub as an input to facilitate and improve trustworthiness and democratic decision-making.

Tokenized decision-making microservice is essential in public decentralized social media, where everyone is open to join or leave and all entities have the same power. Therefore, in a trustless environment, nodes need to run a consensus protocol to ensure that they all agree on the transactions. A consensus

algorithm helps deciding the validity of the transactions and avoid the forking problem in decentralized social media. However, decision-making to reach consensus in such anonymized environments without any centralized authorities is a challenge and current algorithms still have many shortages. To address this issue, we provide heuristic decision-making algorithm for the decentralized social media consortium that predicts future results and helps the decentralized social media reduce costs and latency by analyzing previous voting outcomes and preferences.

Trust SLA microservice needs to take optimized decisions according to conflicting objectives to suggest relevant communities for various services over the time, in order to improve the recommendation quality and eliminate malicious actors in participatory exchanges. Service level agreements (SLAs) are contracts between agents in social media to guarantee expected quality levels of services via elitist solutions [14]. Therefore, we offer SLA trust microservice adopting Pareto solution to negotiate trustworthy agents with precise targeting in decentralized social media. This microservices enabling social media applications engage with the right subset of users based on system requirements and QoS over the time.

Smart-matching microservice preserves security in this distributed environment through decentralized consensus based on voting among the recommended list of reputable agents to express their acceptance of valid transaction[3, 2]. However, finding such nodes is another challenge in decentralized social media. Towards this issue, we apply Pareto-trust microservice as an input and introduce appropriate agents for voting in consensus through a selection of relevant, reachable and credible ones.

Event detection microservice publishes information about events to its subscribers. If new communities are detected, for instance if the geo-profiling algorithm assigns a group of users to a physical location, this event of forming a physical group is broadcast to consumer services.

Data access microservice offers the heuristics and data from SMART to enable other components apply evaluation and cognition for different use-cases.

4 Discussion

Centralized social media do not offer a sufficient level of privacy due to singular data management. This leads to critical trust and privacy concerns across the large scale social media user-base. Decentralized social media can keep privacy over the network [1, 2], however, data distribution among peers in the decentralized network poses new issues. To preserve system security, the nodes need to run a consensus protocol to ensure that they all agree on the transactions. However,

finding trustworthy nodes to vote for the valid transactions makes a challenging issue in decentralized environment. In addition, in such anonymized system without any central authority, malicious actors have more freedom to spread fake information over the network. Thus, decentralized social media needs to consider trust as an important factor to ease users interactions. As different applications may have different requirements in social media, trust needs to be addressed in different ways according to the requirement of services[3], while in most previous works trust does not address all the service requirements [4]. To tackle with this problem, we apply a Pareto-trust microservice enabling consensus process and social media applications engage with the right subset of users. Our model applies trust through various parameters according to domain of services and QoS performance metrics such as accuracy, timeliness, and latency. Nevertheless, integrating trust in complex social networks scenarios with uncertain knowledge is not achievable without having a clear understanding of the network. Therefore, a system needs to extract the users behavior to discover the networks more deeply. Discovering community structures can help us reveal network properties, role of users, and their interactions. The existent studies on community detection mainly focus on one non-overlapping community for each node and only link analysis without content analysis [6–8], while these can not reflect whole information of the network. To do so, we propose a novel approach clustering users into overlapping communities which combines event clustering and link analysis to detect communities precisely through role-stage model considering various aspect of social media. Our proposed model improves community detection in social media by defining implicit and explicit behaviors and interactions of participants in the network without disclosing individual‘s information.

5 Conclusion

Nowadays, decentralized social media attract many attention to maintain users privacy. However, in the absence of a central authority, it is difficult to identify malicious actors and reach a consensus agreement. In this paper, we proposed an adaptive framework to improve trust and group decision making in decentralized social media through applying multi-objective trust model. To do so, we applied different microservices enabling social media applications engage with relevant and most trustworthy users based on services requirements. We provided a role-stage model to precisely infer network construction and communities based on semantic information, users roles, and their transactions while preserving users privacy and anonymity.

Acknowledgments.

This work was accomplished as a part of project *“ARTICONF”* [1], funded by the European Union’s Horizon 2020 research and innovation program under grant

[1] `http://www.articonf.eu/`

agreement No 644179. The authors would also like to thank anonymous reviewers for their valuable comments.

References

1. Barbara Guidi, Andrea Michienzi, and Giulio Rossetti. Towards the dynamic community discovery in decentralized online social networks. *Journal of Grid Computing*, 17(1):23–44, 2019.
2. Leila Bahri, Barbara Carminati, and Elena Ferrari. Decentralized privacy preserving services for online social networks. *Online Social Networks and Media*, 6:18–25, 2018.
3. Raquel Urena, Gang Kou, Yucheng Dong, Francisco Chiclana, and Enrique Herrera-Viedma. A review on trust propagation and opinion dynamics in social networks and group decision making frameworks. *Information Sciences*, 478:461–475, 2019.
4. Mohammad Mahdi Azadjalal, Parham Moradi, Alireza Abdollahpouri, and Mahdi Jalili. A trust-aware recommendation method based on pareto dominance and confidence concepts. *Knowledge-Based Systems*, 116:130–143, 2017.
5. Ahlem Kalaï, Corinne Amel Zayani, Ikram Amous, Wafa Abdelghani, and Florence Sèdes. Social collaborative service recommendation approach based on user's trust and domain-specific expertise. *Future Generation Computer Systems*, 80:355–367, 2018.
6. Huayun Tang, Yingying Jiao, Butian Huang, Changting Lin, Shubham Goyal, and Bei Wang. Learning to classify blockchain peers according to their behavior sequences. *IEEE Access*, 6:71208–71215, 2018.
7. Butian Huang, Zhenguang Liu, Jianhai Chen, Anan Liu, Qi Liu, and Qinming He. Behavior pattern clustering in blockchain networks. *Multimedia Tools and Applications*, 76(19):20099–20110, 2017.
8. Damiano Di Francesco Maesa, Andrea Marino, and Laura Ricci. Uncovering the bitcoin blockchain: an analysis of the full users graph. In *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, pages 537–546. IEEE, 2016.
9. Nicola Dragoni, Saverio Giallorenzo, Alberto Lluch Lafuente, Manuel Mazzara, Fabrizio Montesi, Ruslan Mustafin, and Larisa Safina. Microservices: yesterday, today, and tomorrow. In *Present and ulterior software engineering*, pages 195–216. Springer, 2017.
10. Barbara Guidi, Tobias Amft, Andrea De Salve, Kalman Graffi, and Laura Ricci. Didusonet: A p2p architecture for distributed dunbar-based social networks. *Peer-to-Peer Networking and Applications*, 9(6):1177–1194, 2016.
11. Damiano Di Francesco Maesa, Andrea Marino, and Laura Ricci. Detecting artificial behaviours in the bitcoin users graph. *Online Social Networks and Media*, 3:63–74, 2017.
12. Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.
13. Barbara Guidi, Andrea Michienzi, and Laura Ricci. Sonic-man: a distributed protocol for dynamic community detection and management. In *IFIP International Conference on Distributed Applications and Interoperable Systems*, pages 93–109. Springer, 2018.

14. Mohannad Alhanahnah, Peter Bertok, Zahir Tari, and Sahel Alouneh. Context-aware multifaceted trust framework for evaluating trustworthiness of cloud providers. *Future Generation Computer Systems*, 79:488–499, 2018.
15. V Kathambari and Akira Sasaki. Role-stage model for design and implementation of user-centric business applications. In *2014 International Conference on Computational Science and Computational Intelligence*, volume 1, pages 235–240. IEEE, 2014.
16. Annapurna Jonnalagadda and Lakshmanan Kuppusamy. A survey on game theoretic models for community detection in social networks. *Social Network Analysis and Mining*, 6(1):83, 2016.
17. Meng Qin, Di Jin, Kai Lei, Bogdan Gabrys, and Katarzyna Musial-Gabrys. Adaptive community detection incorporating topology and content in social networks. *Knowledge-Based Systems*, 161:342–356, 2018.
18. Imma Curiel. *Cooperative game theory and applications: cooperative games arising from combinatorial optimization problems*, volume 16. Springer Science & Business Media, 2013.