DECENTRALIZED WEB HOSTING USING BLOCKCHAIN

GOGU SWATHI
Assistant Professor
Department of CSE
goguswathi@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

THAMMISHETTI VARUN
Department of CSE
varunwesly620@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

NARRA SANJAY
Department of CSE
sanjayreddyn21@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

PENDAM RAHUL
Department of CSE
rahupendam1234@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

ABSTRACT: This paper proposes a decentralized solution for web hosting based on interplanetary file system (IPFS) and Ethereum blockchain. Particularly, we use Ethereum smart contracts to manage the IPFS network and the web hosting service. IPFS platform is used to store data and to host websites. All storage miner nodes on the IPFS network offer the pinning service to ensure that source codes of the websites and users' data are retained long-term. Moreover, these nodes also enable the interplanetary name space (IPNS) service for creating and updating mutable links to IPFS contents. TXT record is also used in the domain name system (DNS) to map domain names to IPNS addresses for hosted websites. For privacy-preserving data storage, websites need to be deployed an encryption algorithm. The proposed model that combines between the IPFS and blockchain networks to form a platform providing the decentralized web hosting service. Experiment illustrates building and hosting a web application on the IPFS network. Experimental results show that, compared to the traditional web hosting model, the hosted web application on the proposed platform ensures the confidentiality, integrity, and availability.

Index Terms: Interplanetary file system (IPFS), Block Chain, Ethereum, Domain Name System (DNS)

I.INTRODUCTION:

A Web Hosting service is a type of internet service that makes websites available to the users over the internet, for almost a decade of internet service websites were / and are still hosted on a central server. This proposed system of hosting has made major parts of the internet "centralized". Centralization of data although has a lot of positives has raised a major question about "data privacy" as todays internet data is hosted my major central organizations. The concept of blockchain and decentralization gained popularity over the years, starting from 2010 and the introduction of bitcoin, the blockchain industry had a surge and this technology was involved in formation of a new gen web hosting technology which is purely decentralized and is known to manage and successfully run humongous websites. The decentralized package of webhosting comes with many sets of benefits and has successfully worked out a way to challenge the current widely used central server mechanism. Centralized or Decentralized web hosting have both their perks and drawbacks, and in this paper, we introduce the readers to the conceptual form of both procedures and deeply go through the perks and drawbacks of each hosting solution. The summary of the contributions of this work are listed below. a) This paper first covers the quick introduction of centralized and decentralized web-hosting. b) This paper describes the centralized architecture of web-hosting. c) This paper describes the quick comparison between centralized and decentralized architecture, and how decentralized is more secure and fast over centralized. d) This paper describes the key component required to make web-hosting fully decentralized. e) This paper elaborates the decentralized web-hosting using blockchain. The remainder of this paper is organized as follow. Section 2 Centralized architecture (client-server model), centralized web-hosting, decentralized over centralized. Section 3 discusses the components are required to make web-hosting fully decentralized, Section 4 covers the decentralized web-hosting using blockchain, Section 5 contains the conclusion of whole discussion.

II LITERATURE SURVEY:

Blockchain is an immutable digital ledger that records and verifies cryptographically signed transactions grouped into blocks in a distributed fashion without a central authority. Except for the genesis block in a blockchain, each block cryptographically points to its immediately previous one after undergoing a distributed consensus decision and validation. The blockchain platforms maintain the blocks containing the electronic cryptographic data in a distributed and consensus way. Based on a distributed blockchain and consensus-based maintenance, individually developed policing mechanisms ensure that valid transactions are added to the blockchain that allows users to be pseudonymous or anonymous; users can create accounts without identifying the authorization process. Therefore, applications built on the blockchain can enable the business to be with untrusted and unknown users. Blockchain is based on decentralized peer-to-peer networking, in which all participant nodes provide their resources fairly, alleviating one-to-many traffic flow bottlenecks. The characteristics of blockchain are to provide decentralization, transparency, non-repudiation, and traceability. A blockchain is a public registry of who owns and who transacts what. The transactions are secured through cryptography, and the transaction history gets locked in blocks of data that are then cryptographically linked together and secured. This creates an immutable record of all the transactions across this network that cannot be forged. The record is replicated on every node in the network. Unlike the existing Internet, blockchain enables users to deliver value without relying on a third party. As of now, it has been used to deliver various economic values such as cryptocurrency, stocks, computing resources, real estate, automobile use rights in a shared economic society, and intellectual property rights. Several cryptographic technologies, such as hashing and digital signature, have been used in blockchains. Hashing is a method of calculating a relative unique fixed-size output (called digest) for the input of nearly any size (e.g., a video stream, a text file, or an image) and is designed to be one-way and collision-free. Because it results in completely different digests, even if a single bit in the input data is modified, it provides the integrity of a block data in the blockchain. For digital signatures, asymmetric-key cryptography is utilized; this provides the ability to verify someone's identity who participates in a transaction. Each user possesses a pair of private and public keys. The private key, regarded as the user's identity and security credential, is used to sign transactions digitally; the digitally signed transactions are sent to whole nodes. The public key is used to validate the transactions that are signed with the private key. When a new transaction occurs, the user submits a new transaction to the blockchain ledger. The new transaction will be copied and distributed among every node in

the blockchain platform. It will be stored in a queue until a mining node adds it to the blockchain by creating a block. Blockchains allow us to write code and have binding contracts between individuals and then guarantee that these contracts will be enforced without a third party's requirement. Blockchains redefine how digital trust mechanisms work using distributed consensus mechanisms and transparent tamper-evident record-keeping. Current Web applications combine service and data and execute with a closed back-end database. Because of this coupling, an RSVP on an application event will not be reflected in the scheduler. Thus, similar or related data will be redundantly stored in multiple applications, such as the centralized Web application. The applications in the centralized Web compete in a single market based on data ownership. New innovative competitors, in the centralized Web ecosystem may struggle to enter market because of a lack of customer data. In this section, we introduce the trustworthy decentralized Web architecture and the data model and functional components for identity and data management. Fundamentally, decentralizing the Web is about enabling choice by breaking up artificially coupled decisions into individual options that can be combined at one's pleasure. In a decentralized Web, we should be able to interact with websites and other people without commitment to a single social media platform. Sensitive personal data should be decoupled from applications in terms of taking back control of it. This separation allows users to enjoy the applications they want and store data where they specify. Also, this allows service providers to develop applications without the accumulation of their own user data. An example of the data and service separation for a decentralized app application is shown on the right End-users can select any service provider to store their text, photos, and videos on their own storages on the Internet and depend on any third-party services to interact with data, regardless of storage location. As an example, identity data for a crucial identity service can be provided by Web storage. In the decentralized web ecosystem, end-users have the right to control their data, unlike the centralized web ecosystem. However, although users can control the data in the decentralized web ecosystem when the service providers utilize the user's data, they can infer the data owner and infringe the user's privacy. Besides, as data generated by wearable devices and sensors in the home network and user-generated contents become valuable, data sovereignty is becoming more critical. Hence, it is desirable that the identifier be anonymized or pseudonymized to ensure the user's privacy, and if possible, a relationship between both identifiers of data and owner must be established to claim data ownership.

III. EXISTING SYSTEM:

In centralized Architecture, a single authority is created through which all the data must pass through. The basic components of this architecture are: node (client), server and communication link.

This architecture follows the standards of client server architecture in which client sends the request to server and server responds back to those requests made by the client. Centralized system is easy to create and setup because it provides the more direct control like all the permission and processing are managed by single central server.

The server components provide services to one or many clients which make request. Server classified on the basis of service they offer, for example, a web server offers web page and a file server offer file exchange.

A single computer can offer web service and file service at a time to provide data based on the type of request created by the client. The communication between different servers is known as inter server communication and this communication is fully synchronized.

Disadvantages

In centralized network, all the data of the network passes through a centralized server. Therefore here, a single organization holds the information.

Even though centralized organizations are secure and trustable; they are not 100% secure or trustable.

IV. PROPOSED SYSTEM:

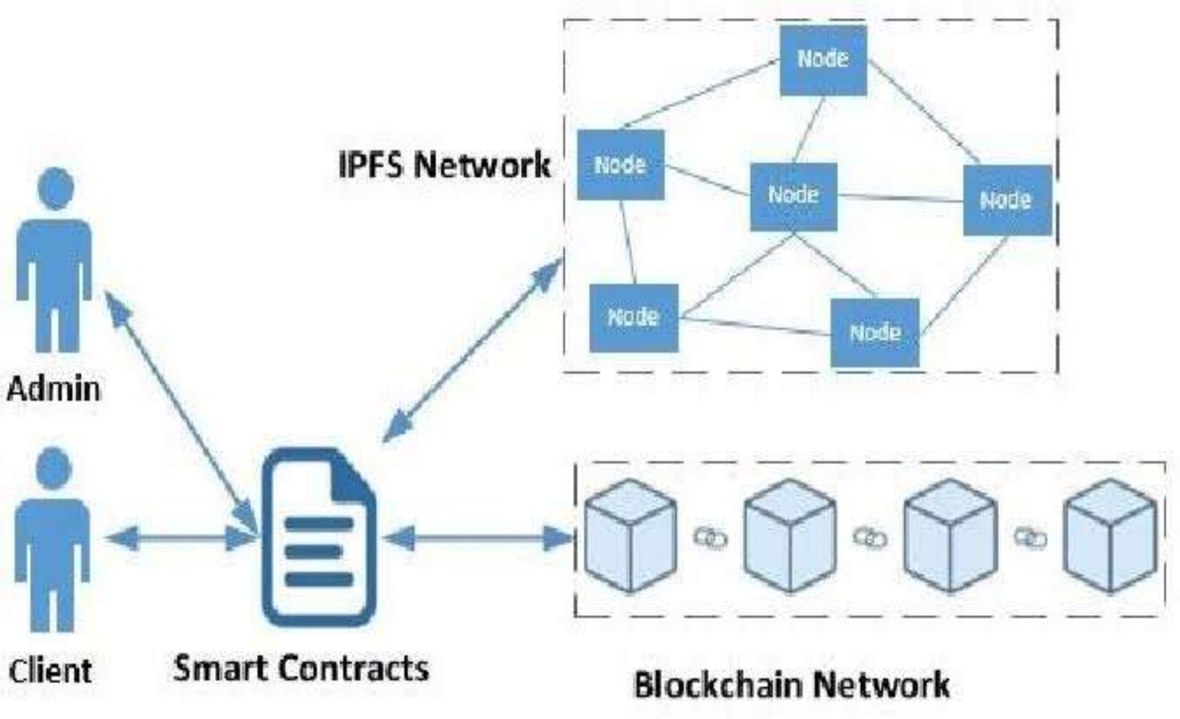
The ways to demonstrate the functioning of centralized and decentralized web hosting, keeping our main focus on comparing centralized and decentralized systems with each other. The centralized and decentralized systems with some terms and technologies then we have explained the centralized architecture followed by a comparison table for a centralized and decentralized network. The decentralized networks and technologies associated with them such as IPFS, encryption, etc.

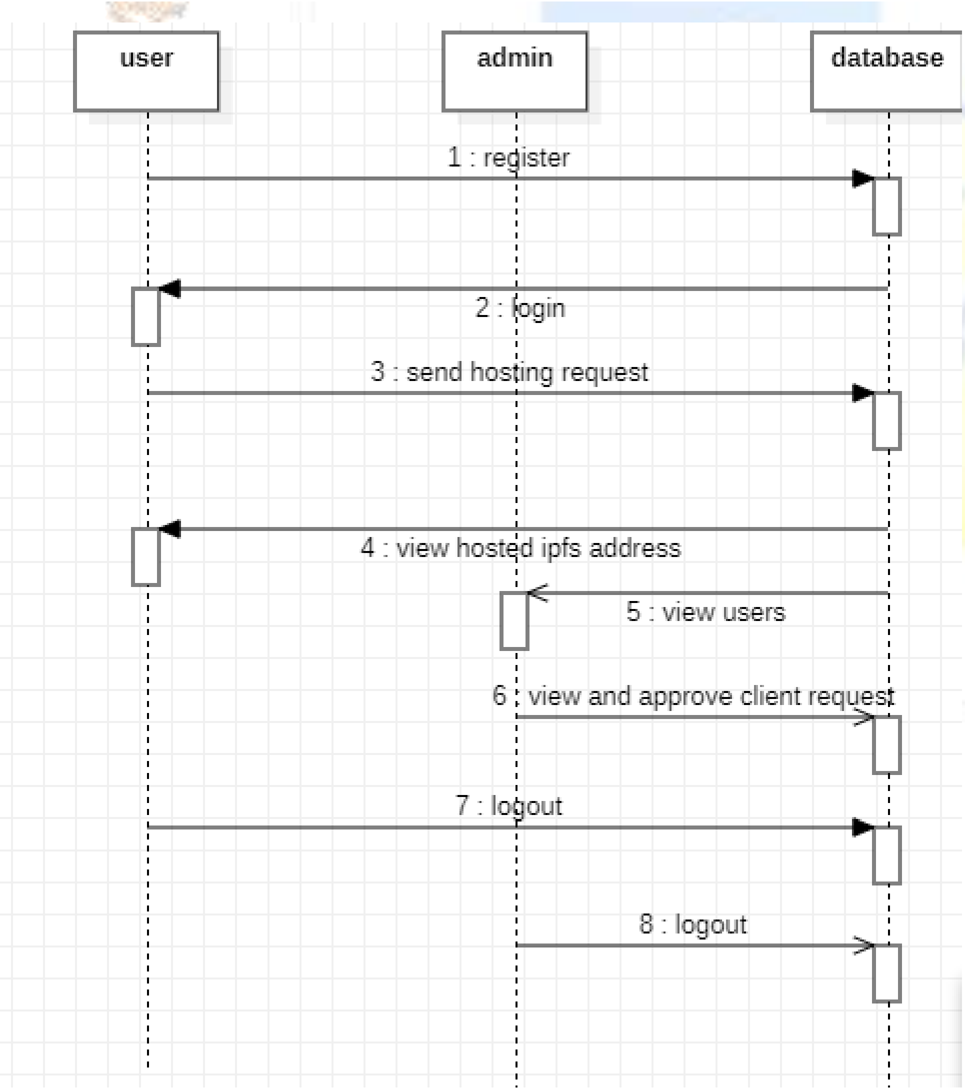
Advantages:

A decentralized network can work efficiently and the Future research includes working on the limitations of decentralized networks and providing solutions to overcome the limitations.

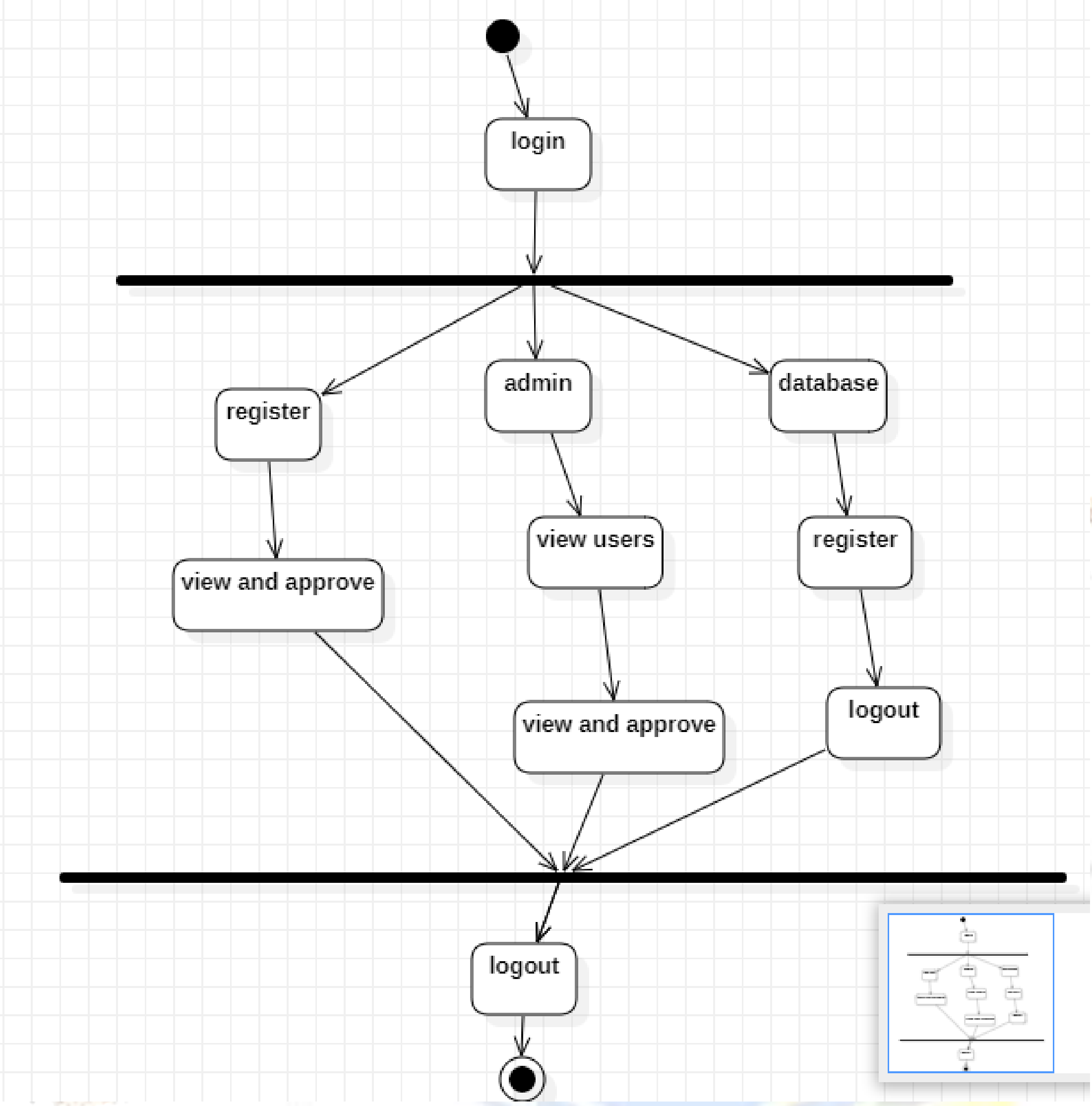
Thus, decentralized web hosting network can be applied efficiently to overcome the limitations of centralized network.

V.SYSTEM ACHITECTURE





Sequence Diagram



Activity Diagram

VI. CONCLUSION:

A user-generated content is hosted on web servers belonging to a small group of giant companies. This trend has created the centralized Web with several issues, censorship, surveillance, abuse of curatorial power, abuse of privacy, monetize data, data breach, not the least of which is giant companies holding power through vast amounts of data. Decentralized Web has the potential to revolutionize contracts and value exchanges and to decouple data and related applications. The decentralized web basically should separate data and applications, give data rights to data producers, and ensure responsible data sharing. We discuss self-sovereignty identity, self-sovereignty data, and trustworthiness for data or value transactions that are a necessity in the trustworthy decentralized web. Therefore, we discuss self-sovereign identity, self-sovereign data, and trustworthiness for data or value transactions necessary in the trustworthy decentralized web. In this study, we reviewed the issues related to centralized web architecture, decentralized storage platform, and blockchain technology and discussed blockchain's potential for decentralized web architecture. Subsequently, we discussed a trustworthy decentralized web architecture that circumvents internet gatekeepers and takes control of our data back. In the future, we will implement the designed trustworthy decentralized Web architecture using open source blockchain technology and a decentralize storage platform.

VII. FUTURE SCOPE:

Our System has proposed a decentralized platform for web hosting. The proposed system takes the advantages of the blockchain technology, IPFS, and encryption. That allows clients to host websites without using any central system from service providers. We have also proposed the combination model between IPFS and blockchain, and build the workflows for managing the decentralized web hosting service and the IPFS network. Experiment results show that hosted websites on the IPFS network have high availability, ensure data security and privacy. In our future work, we will build smart contracts to provide access control features and optimize protocols to make the functions more efficient.

VIII. REFERENCES:

[1] Z. Xiao, S. Wen, H. Yu, Z. Wu, H. Chen, C. Zhang, and Y. Ji, "A new architecture of web applications-The Widget/Server architecture," in 2010 2nd IEEE International Conference on Network Infrastructure and Digital Content, IEEE, 2010, pp. 866-869.

[2] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "BlockchainBased, Decentralized Access Control for IPFS," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1499-1506.

[3] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies: A comprehensive introduction," Princeton University Press, 2016.

[4] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," in International Journal of Web and Grid Services, 2016.

[5] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper 3, 2014, 37.

[6] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," In International Conference on Principles of Security and Trust, Springer, Berlin, Heidelberg, 2017, pp. 164-186.

[7] A. Ramachandran, and M. Kantarcioglu, "SmartProvenance: a distributed, blockchain based dataprovenance system," in Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, ACM, 2018, pp. 35-42.

[8] G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," International Journal of Computer Applications, 67(19), 2013.

[9] T. Nie, and T. Zhang, "A study of DES and Blowfish encryption algorithm," in Tencon 2009-2009 IEEE Region 10 Conference, IEEE, 2009, pp. 1-4.

[10] M. A. Hossain, M. B. Hossain, M. S. Uddin, and S. M. Imtiaz, "Performance analysis of different cryptography algorithms," International Journal of Advanced Research in Computer Science and Software Engineering, 6(3), 2016.

[11] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," in International Journal of Web and Grid Services, 2016.

[12] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Communications Surveys & Tutorials, 2018.

[13] J. P. Cruz, K. Yuichi, and N. Yanai, "RBAC-SC: Role-based access control using smart contract," IEEE Access 6, 2018, pp. 12240- 12251.

[14] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25-30.

[15] X. Li, P. Jiang, T. Chen, X Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, 2017.

[16] R. A. Popa, E. Stark, S. Valdez, J. Helfer, N. Zeldovich, and H. Balakrishnan, "Building web applications on top of encrypted data using Mylar," in 11th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 14), 2014, pp. 157-172.

[17] W. He, D. Akhawe, S. Jain, E. Shi, and D. Song, "Shadowcrypt: Encrypted web applications for everyone," in Proceedings of the 2014 2019 6th NAFOSTED Conference on Information and Computer Science (NICS) 86 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2014, pp. 1028-1039.

[18] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is SSL?)," in Annual International Cryptology Conference, Springer, Berlin, Heidelberg, 2001, pp. 310-331.

[19] D. Berbecaru, and A. Lioy, "On the robustness of applications based on the SSL and TLS security protocols," European Public key infrastructure workshop, Springer, Berlin, Heidelberg, 2007, p. 248- 264.

[20] M. Dworkin, "Recommendation for block cipher modes of operation. methods and techniques," NIST Special Publication 800-38A Edition, 2001.

[21] D. Blazhevski, A. Bozhinovski, B. Stojchevska, and V. Pachovski, "Modes of operation of the AES algorithm," in the 10th Conference for Informatics and Information Technology, 2013. [22] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," IEEE network, 24(4), 2010, pp. 13-18