Mobile Social Network Sharing Using Secured Mechanism

Shailesh Kaple, Nikhil Rane, Nalini Walunj, Pooja Chaudhari, Prof. Sandeep Shiravale
School of Computer Engineering and Technology, MIT Academy of Engineering, Pune, India

Abstract : The Mobile social networks (MSNs) are utilized by the people to view, write and share their information. The major purpose in such information transfer is to bring likeminded people under the single roof. Besides, if a user in MSN share contents in an improper way, it makes an easy prey to malicious users who may want to purposely add false contents. In this research paper, we propose a mechanism that motivates content sharing in MSN and ensures that only trustworthy contents are shared. We consider an MSN at an exhibition with many users, who collect and share their data with their correlated members. During an encounter, agents share the metadata of the contents they wish to share. The mechanism is built on users' collective bidding technique, content cost sharing, and trust evaluation while guaranteeing individual dependency and freedom from other users. This is accomplished by introducing a distributed cryptographic hash-chained content. The proposed system in this paper will evaluate the trustworthiness of information by detecting and differentiating review-chains which will help reduce the time and cost to collect all the desired contents.

IndexTerms **- Collective bidding, content reputation, content sharing, hash-chained review, incentives, trust inference, mobile social networks.**

I. INTRODUCTION

As smart phones are now becoming more ubiquitous with wide array of sensors and communication techniques, we can develop mobile social network (MSN) apps that make possible to create virtual groups and then share your contents securely among yourselves. At a time your device can also help you with a productive method by conveying you the data and all other valuable contents that can be shared with you.

Motivating content sharing proposes various schemes built on the base of various virtual checks and participate users to ensure that correct data is send and received. While sharing also we have to assure that correct data have been shared and no one has misbehaved with the data. However in MSN such as meetings ,etc.

Where people buy their valuable contents, our motive is to encounter the content providers and share their contents who may be interested. Many end users download the contents for their use much more than the one they contribute for the same network .Some people don't want to share their data as its

values may only attach to them or a few people only. Also while sharing their may be vulnerability to privacy and other security breaches.
We can say that MSN have close similarity to P2P network but cannot be directly applied to MSN due to different methods. It is strongly built on Connection between individual encounters.

As our MSN is all a wireless concept so we can form a multiuser formation and exploit the contents and their cost among various co-located encounters. MSN is totally built on smart devices which can create and share all the contents according to the preferences from their encounters. The main objective is the participatory sensing of minimum cost such that the cost may motivate more users to come and share their contents. Also in addition only Information is private in other sensing but in MSN both the contents cost and also the content value both are private information .This all implies that in our MSN design mechanisms other than participatory sensing techniques ,it is not directly applicable to promote content sharing as we do in MSN.

II TECHNOLOGY USED

A. BlockChain :

Definition :-

The blockchain is an digital technique that can be generated just not to record all types of financial transactions but also record all types of data virtually everything which is of some value or the another.

MSN Using Blockchain Mechanism :-
Blockchain can be used in MSN to create virtual blocks of messages in network and then distribute all the messages in that network specifically. A blockchain, originally chain of blocks, is a growing list of records, called *blocks*, which are linked using some or other cryptographic methods.

By design part of a blockchain in network, a blockchain is also resistant to any kind of modification. It is an open, distributed ledger that can record transactions and also data sharing between two peoples efficiently and in efficient and permanent way. A blockchain collectively restrict to a communication protocol by validating new blocks added in the network. Though, blockchain records cannot be changed by the external sources, blockchain may be considered secured by design as well as overall working of it.

This technology is a open, replicated, as well as shared. This helps in synchronizing digital data spanning across geographically distributed multiple locations. It is completely managed by a peer to peer network. In Blockchain, the data once recorded in any block cannot be changed without alteration all other given blocks. Although the records in Blckchain are not changeable, blockchain may be considered as secured by design.

Blockchain was invented to serve as a public transaction ledger for a crypto currency bitcoin. This helps in solving the problem of double spending. This problem can be solved by blockchain without the need trusted authority central administrator or central server. For businesses Private blockchain are proposed. Now Blockchaining is almost used by all businesses where the central admin or central server technology is used currently.

Bitcoin has a specially designed data storage structure ,and transactions in the network could not happen without a core technology Blockchain. All the transactions in it are stored in list of blocks. The chain is continuously growing as a new block is added to previous block. For user security Asymmetric cryptography and distributed consensus algorithm are used. To save the cost and improve efficiency, decentralization, persistency and anonymity are used. Transactions in the blockchain cannot be tempered back hence the businesses that have high reliability and honesty can use Blockchain to attract customers.

This technology is facing certain technical challenges. Scalability is huge concern. Now the size of a bitcoin block is 1 MB while the block is need to be mined after every 10 minutes. The larger blocks occupy larger space for storage and also slow down the propagation in the network. This can lead to the need of centralization as very few users would like use this technology.

Blockchain and mobile social network connection **:-**

When we talk about blockchain technology then it mainly refers to cryptocurrency transactions and it has total opposition to centralized record keeping method of all the transactions, data and records that all the traditional banks are performing currently.Each transaction, each record is being kept in a separate node itself and is currently used by bitcoins technology.

At seeing a glance we may not think that there is any link between Blockchain and Mobile social network but there is a great connection between them. Blockchain Technology initiates all the individuals to have more privacy when using Internet based methodologies. We know that social media creates viral contents ,then they will receive a compensation to that.

For example ,Social media site is a big concern and sites like facebook ,Instagram have a total access to our all conversations and all other data through our Whatsapp app. These are some of the examples where privacy being affected and there are some others that we may not even aware of it.
By using blockchain technology only sender and receiver are aware of the content of the transaction. Many social media platform are exploring their own payment platforms. For example, Facebook is providing a payment feature through its messaging platform. As you may imagine, Facebook records all the transactions that you are made. This is major drawback of privacy that may make some users unwilling to use this technology.

The Blockchain will be helpful to give a high end security to websites providing financial exchanges. It could even protect privacy for communication between private users also and many more. This will also help to increase the number of social media platform users and there satisfaction with the same. When these platform use safe exchanging transactions rather than current available platforms they will be able to automate many processes through the use of smart contract. These platform could also analyze and maintain the data in more secure and convincing manner.

The Blockchain in mobile social network could also save a lot of time and energy, and also generate better overall result. These type of technology can be used in wide range of industries and also in various beneficial ways.

Blockchain as a middleman in MSN :-

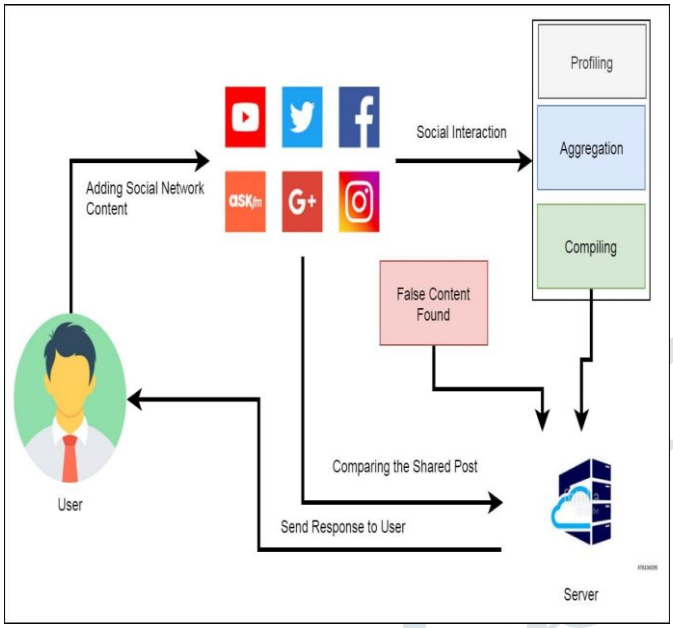
We can see today social media content creator are losing a significant amount of money because of social media's as a middleman. However, the inclusion of Blockchain technology could disrupt the whole process by taking the middleman out of the social media platforms and enabling all the social media creators to get paid for managing and sharing all the users contents.
However, all the social media users have the power to get know about where all the contents are distributed. This facility gives the users improved ability to make profit from the production of passive income. Some users may not be currently producing their contents because they could not match with the social media platform.
In todays scenario, many social media platforms are getting the huge amount paid for the contents that they produce which the users provides them and also they make advertisement space so that they can get additional profit from the users who use social media platform. When you look to this Blockchain technology it become clear that the current practice in the social media platforms needs to be change instantly.

III MSN ARCHITECTURE USING BLOCKCHAIN

The project will detect the false content from the social sites.
It will follow the steps that are mentioned below:

1. The system will first ask the user to register himself on the particular website.

2. Now he would be able to share content on various social sites like Facebook, Twitter, Instagram, etc.



3. After sharing the content, it will go through two phases:

i. In first phase there would be social interaction in which it will perform three operations which are mentioned below:

Profiling: In this operation we construct a user's profile using his or her publicly and voluntarily shared social data. In short, it refers to the data science process of generating a person's profile with computerized algorithms and technology. We can share this information through many mediums and platforms with the help of increasing number of successful social networks.

Aggregation: This is an operation of collecting content from multiple social network services into one unified presentation. Social Network Aggregator performs this task which helps to put the information in a single location. There are number of tools and widgets which are provided by various aggregation services to allow users to consolidate messages, track friends, combine bookmarks, see when their name is mentioned on various sites, etc. In short, aggregators simplify the user's social networking experience.

Compiling: It is a process of producing a list by assembling information collected from various sources. This process is performed by using a compiler. A compiler is a computer program that transfers computer code written in one programming language into another programming language. It is primarily used for programs that translate source code from a high level programming language to lower level language to create an executable program.
After performing all these operations, the data will be stored in the database.

ii. In second phase the shared content is compared with the data which is in the database.

4. After data comparison, if the content is not matched with the database, the user will get a warning. And if the content is matched with the database the user will be ready for the interaction.
In this way the user would be responded by the system server.

IV APPLICATIONS

Applications where MSN Mechanism can be applied can be same as that of blockchain applications and cost effectiveness can be advancement to those applications.

1. Payment processing.
   The most logical use for blockchain is as a means to expedite the transfer of funds from one party to another. However, banks removed from the equation, and validation of transactions ongoing 24 hours a day, seven days a week, most transactions processed over a blockchain can be settled within a matter of seconds.

2. Monitor supply chains.

When it comes to monitoring supply chains, blockchain also comes in particularly handy. Further, blockchain would allow businesses, and possibly even consumers, to view how products performed from a quality control perspective as they traveled from their place of origin to the retailer.

3. Digital ID solutions.

Now a days many people worldwide face identity challenges. So many big companies is looking to change that. This would allow folks in impoverished regions to get access to financial services or start their own business. In the early stages, industries attempts to create a decentralized digital ID.

4. Digital voting.

Well, blockchain technology resolved the problem of voter fraud. It offers the ability to vote digitally, but its transparent enough that any regulators would be able to see if something were changed on the network. It combines the ease of digital voting with the immutability.

5. Food safety.

Another intriguing use for blockchain could be in tracing food from its origin to your plate. You would be able to trace the transport of food products from their origin to super market, since blockchain data is immutable. Blockchain would allow the source of the contaminant to be found considerably quicker than it can be now.

6. Immutable data backup.

Blockchain technology might also be the perfect way to back up data. Even though cloud storage systems are designed to be a go-to source for data safe keeping, they are not immune to hackers, or even infrastructure problems.

7. Medical record keeping.

The good news is for record keeping purposes, the medical store has already been moving away from papers for years. Since, blockchain offers even more safety and convenience. In addition, to storing history of patient, patient records, the patient, who passes the key to access these digital records, would be in control of who gains access to that data.

8. Weapons tracking.

One of the most bigger/dangerous topics on any news network at that moment is the gun control or weapons accountability. Keeping a record of weapons sold privately, blockchain create a transparent and unchanging registry network that allows law enforcement and the federal government to track gun or weapon ownership.

9. Tracking prescription drugs.

Lastly, blockchain could be a means of transparently tracking prescription medicines. Blockchain offers a drugmakers the ability to track their products based on serial and batch numbers to ensure that consumers are getting the real deal when they pick up medicine from the pharmacy. Merck is currently testing such a system for prescription drug returns.

10. Managing Internet of Things network.

The IoT describes wirelessly connected devices that can send and receive data. Such an application could determine the trustworthiness of devices i=on a network and continuously do so for devices entering and leaving the network, such as smart cars or smartphones.

V CONCLUSION

A solution for creating a mobile social network of the users using social media platform to manage, control and secure the contents provided by them was presented in this paper. In the above points it has been seen that decentralization, anonymity, traceability and censorship resistance of the Blockchain technology will support such a platform. These will also support offline encryption of data and mechanism. The four main components are used to deliver this fuctionality : The blockchain technology will keep record of the ownership of data items and the number of shares made, and a relationship system which would enable programmable code will be executed on the blockchain and control the number of allowed shares for a data item, a hash table that stores encrypted data that the user shares and, then finally a local personal certificate authority that can manages a user's circles, the encryption keys and the controls access to the content.

In order to establish the relationship system, scripting capabilities for frameworks would be assessed. Number of applications for identity management for blockchains would be another area of investigation.

References:-

1. K. Gai, M. Qiu, Z. Xiong, and M. Liu, Privacy-preserving multi-channel communication in Edge-of-Things, Future Generation Computer Systems, 85, 2018, pp. 190-200.

2. K. Gai, M. Qiu, and X. Sun, A survey on FinTech, Journal of Network and Computer Applications, 2017, pp. 1-12.

3. A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, A cloud based health insurance plan recommendation system: A user centered approach, Future Generation Computer Systems, vols. 43- 44, pp. 99-109, 2015.

4. A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, Incremental proxy re-encryption scheme for mobile cloud computing environment, The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.

5. R. Wu, G.-J. Ahn, and H. Hu, Secure sharing of electronic health records in clouds, In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom), 2012, pp. 711-718.

6. A. Abbas and S. U. Khan, A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds, IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, 2014.

7. M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, A general framework for secure sharing of personal health records in cloud system, Journal of Computer and System Sciences, vol. 90, pp, 46-62, 2017.

8. J. Li, Electronic personal health records and the question of privacy, Computers, 2013, DOI: 10.1109/MC.2013.225.

9. D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, A research agenda for personal health records (PHRs), Journal of the American Medical Informatics Association, vol. 15, no. 6, 2008, pp. 729-736.

10. S. Yu, C. Wang, K. Ren, and W. Lou, Achieving secure, scalable and fine-grained data access control in cloud computing, in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9.

11. S. Kamara and K. Lauter, Cryptographic cloud storage, Financial Cryptography and Data Security, vol. 6054, pp. 136149, 2010.

12. T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, Secure Dynamic access control scheme of PHR in cloud computing, Journal of Medical Systems, vol. 36, no. 6, pp. 4005 4020, 2012.

13. K. Gai, M. Qiu, Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers, IEEE Transactions on Industrial Informatics, 2017, DOI: 10.1109/TII.2017.2780885..

14. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131143.

15. Health Insurance Portability and Accountability, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/, accessed on October 20, 2014