International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9, Issue-7, May 2020

Data Authorization in Social Network using Block Chain

S.Uma Maheswari, B.Sai Adharsh, P.Shanjeev, K Vignesh, M.Thanigai Bharathi

***Abstract:** In India most of the people are into social networks. Some people are taking advantage of this and spreading fake and irrelevant news in the society. Due to these major riots, culture oriented problems, fake medical messages are spreading over the people. Still there is no technology to identify these problems. Here we are introducing block chain to overcome all the above mentioned problems. Our method finds the solution for these major issues. Using the above mentioned explanation with SHA256 algorithms supports block chain a lot to implement. In case of any changes done in the mid node, using the hash function and SHA 256 algorithm, the man in the middle can be identified. The entire hash should be exactly match with the primary hash. So that data cannot be changed in the middle. In case of any changes occurred the data owner will be get notice.*

***Keywords:** bitcoin , hashing ,analysis.*

I. INTRODUCTION

Some people are taking advantage of this and spreading fake and irrelevant news in the society. Due to these major riots, culture oriented problems, fake medical messages are spreading over the people. Still there is no technology to identify these problems. To overcome the problem Blockchain technology have been introduced. Now days it has become promising and revolutionary technology.

In our project we used SHA-256 hashing and Rijndael algorithm key generation. It consists of individual behaviour specifications with hash functions, a large set of rules that are programmed into it. It is a distributed, peer-to-peer and secured information database. Input information for every hash number has to include the previous block's hash number. It is capable of seeing every transaction and its hash value.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
Umamaheswari G*, Assistant Profeesor, Department of Computer Science And Engineering, Sri Shakthi Institute of Engineering and Technology Coimbatore
Sai Adharsh B UG Student , Department of Computer Science And Engineering ,Sri Shakthi Institute of Engineering and Technology, Coimbatore
Shanjeev P, UG Student , Department Of Computer Science And Engineering ,Sri Shakthi Institute of Engineering and Technology, Coimbatore
Vignesh K UG Student , Department of Computer Science And Engineering ,Sri Shakthi Institute of Engineering and Technology, Coimbatore
Thangai Bharathi M UG Student Department of Computer Science and Enginerring Sri Shakthi Institute If Engerring And Technology,Coimbatore .

- Rijndael – used for encryption with key for security with block cipher
- SHA256- Used for comparing the computed hash to a known and expected hash value

II. EXISTING SYSTEM

The already existing system or the system that has been used to detect the spread of fake messages is not so efficient in controlling the spread in initial stages.

There is no admin in any social network to control the spreading of fake messages Even the Data owner or the source person could not able to identify or to stop spreading their own messages.

These are the main disadvantages which are caused due to not using the block chain technology. If it make use of block chain it could use to detect the problem in early stages.

III. LITERATURE SURVEY

[1]. **Performance Analysis of the Raft Consensus Algorithm for Private Block chain:**

The Blockchain is peer to peer system. It is a decentralized system. It can used from anywhere at time we want from any devices. But the consensus is the main problem of the blockchain. It is fault- tolerant mechanism. It is currently has been used in computer and blockchain systems in order to achieve single data value or single state among the multiple systems. That can be a cryptocurrencies. Raft consensus is one of the advanced and widely used consensus algorithm.

By using this algorithm we can achieve high accurate and efficient results. It has packed with a lot of advantages when compared to other consensus algorithm.

[2]. A practical system for binary transparency in Data Privacy Management, Crypto currencies and Block chain Technology:

Transparency is very important and crucial in highly secure applications on the side of authoritative information. If it is highly secured then only it can provide robust solutions for holding the authorities accountable for their own actions. Otherwise it cannot provide the robust solutions. Bitcoin is the key or important example for how to enforce transparency in a financial setting. In our proposed system or model we are shifting to new and highly effective mechanism. This highly secured mechanism is called as binary transparency. In this binary transparency mechanism the issuance is deployed in X.509 certificates. By issuing these kind of certificates we can easily monitor all the activities that has been going on the system. Using this certificate it is very easy to expose and identify the misbehavior and fraudulent activites.

IV. THE MODEL

ASP.NET as front end, C# as coding language and SQL server as backend. Java Script has been used for scripting language.

A. Data Transfer between blocks

This module deals with post, comment and chat. User can access these options from their login. User can post or share their details to their friends. All the details will be work under social network policy. While transferring the data the data will be converted into blocks for further usage. Here the user shared details will be stored as blocks. These blocks will be interconnected between users as block chain.

B. Implementing Block chain with keys

Now the blocks will be internally linked with data processing also. Each blocks and data will be created as a hash function under the block chain concepts. Using SHA256 Algorithm the hash function will be executed. All the hash consists of a key reference for further usage. Each and every transaction will be notified and comes under has function.

C. Split Hash Blocks

This is core process of the project. All the users and data can be furnished as a track able format. Using SHA256 algorithm, the data reference will be added with the user reference. Now the data related users will be under hash function. Now the user and data is under split hash blocks

D. Verifying hash using rijndel key

This is the final module of this project. Here using the rijendal key, the admin can track the users using the block chain method. Admin can able stop a forward message. As well admin can fetch a entire block of a forwarded message. As well as user can stop forward their own message.

V. ALGORITHM

A.Initialisation

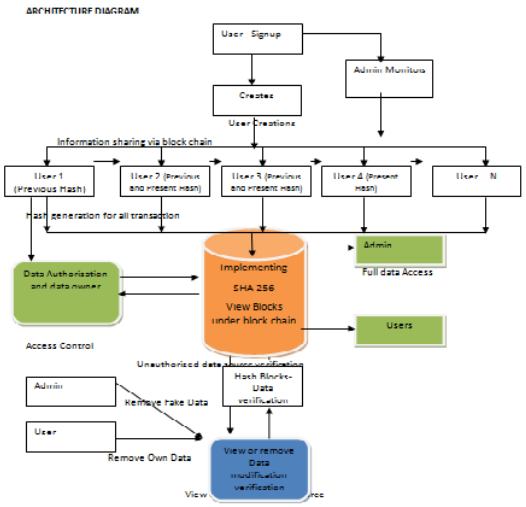
SHA256- Used for mathematical Computational hashing
c- compression function
b- message block Rijndael algorithm –used for symmetric key generation with block cipher .Based on

- Byte –by- Byte replacement
- Swap
- XOR
- B. **Process:**

SHA-256 Algorithm

Step 1: Process the given data with 256bits
Step 2: Input we get will be in the large
Step 3: Input will always be not a perfect multiple of 512 bits so some part of input will be left
Step 4: Do a padding with concatenate input with 10 multiple before it with some left input.
Step 5: Now our input is perfect multiple
Step 6: Now 512 bit input is added with 256 bit to get a total of 768 bits.
Step 7: 768 bits is passed through compression function to get the output of 256 –bit output
Rijndael process:
Step 1: Generates 10 128-bit keys from 128 bit key
Step 2: Plain texts are stored and divided in 4x4 tables
Step 3: Then each 128-bit plaintext pieces is proceeded on 10-round process.
Step 4: code is generated after 10 th round
Step 5: Then modulo 2 is applied bitwise and XOR operation
Step 6: Row of matrices are now sorted cyclically
Step 7: columns are exchanged by matrix multiplication by galois field
Step 8:XOR link is applied to the subkey for each round

Architecture Diagram



Implementation

Block Chain Social network:

Table Name: adminlogin

Primary Key: id

Fields	Data Type	Size	Constrtains	Description
Uname	Varchar	50	Not Null	Admin User
Pwd	Varchar	250	Not Null	Adime password

Table Name: Tree view

Primary Key: memid

Fields	Data Type	Size	Constrains	Description
Memid	Int	10	Primary Key	Key identification number
Name	Varchar	50	Not Null	Name of the user
Parentid	Varchar	250	Not Null	Parent identification number
Parent	Varchar	250	Not Null	Parent name

VI. RESULTS AND FINDINGS

Core findings :

- Block chain working model for internal security in Social Network Environment with multiple users Interface model.
- SHA256 hash algorithm for transaction and creating hash blocks for each users
- Stop spreading fake and old messages around social network
- Identifying fake and irreverent message or news spreaders

VII. CONCLUSION

This project has proven that Rjindael has been more effective than all other algorithm in identifying the fake messages. Most efficient in block chain technology and more advanced than existing system. With using of hash and key generation functions the unauthorized access and circulation of fake messages have been reduced. With the use of previous hash function transaction has become easily accessible. So both admin and user have authorization to stop spreading messages .Installation and setting up process complexity has been reduced and easy when compared with other algorithm and technology.

REFERENCES

1. H. Wang ,Y. Zhang,, S. Yu, A. Fu, C. Huang, *IEEE Transactions on Big Data*, 2017. A new public auditing scheme for cloud data sharing with group users,
2. Abou Elkalam, A, Ait Ouahman, vol. 9, no. 18, 2016. "Fair access: a new blockchain-based access control framework for the internet of things.
3. C. Meinel ,A. Gruner, A, T. Gayvoronskaya, , "Towards a Blockchain-based Identity Provider", *SECURWARE 2018:* pp. 73-78, 2018., *The Twelfth International Conference on Security Information Systems and Technologies*,
4. G W Peters, "Understanding Modern Banking Ledgers through Blockchain Technologies: pp. 239-278, 2016. Future of Transaction Processing and Smart Contracts on the Internet of Money[M]//" in Banking Beyond Banks and Money, Springer International Publishing,
5. P. Saxena, K. Croman, C. Decker, I. Eyal, "On scaling decentralized blockchains" pp. 106-125, 2016., *International Conference on Financial Cryptography and Data Security*,
6. O. Nathan, G. Zyskind, , , Alex Sandy Pentland "Decentralizing privacy: *2015 IEEE*, pp. 180-184, 2015.,Using blockchain to protect personal data", *Security and Privacy Workshops (SPW)*
7. Chunming Rong ,Chakravorty Antorweep, , "Ushare: user controlled social media based on blockchain", *International Conference on Ubiquitous Information Management and Communication*, 2017.
8. Pap Amanthou, , Ahmed Kosba, Andrew Miller"Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts", *Security and Privacy IEEE*, 2016.
9. W. Jiang, ,X. Yue, D. Jin, M. Li, "Healthcare data gateways: vol. 40, no. 10, pp. 218, 2016., Found healthcare intelligence on blockchain with novel privacy risk control", *J. Med. Syst.*,
10. T. Strufe, L. A. Cutillo, R. Molva, "Leveraging social links for trust and privacy in networks", *INet Sec 2009. Open Research Problems in Network Security*, 2009.

AUTHORS PROFILE

UmaMaheswari G, ME, Assistant profeesor, Department of computer science and Engineering, Sri Shakthi institute of Engineering and Technology Coimbatore

Sai Adharsh B UG student , Department of computer science and Engineering ,Sri Shakthi institute of Engineering and Technology, Coimbatore

Shanjeev P, UG student , Department of computer science and Engineering ,Sri Shakthi institute of Engineering and Technology, Coimbatore

Vignesh K UG student , Department of computer science and Engineering ,Sri Shakthi institute of Engineering and Technology, Coimbatore

Thangai bharathi M UG student Department Of Computer Science and Enginerring Sri Shakthi Institute if Engerring and Technology,Coimbatore .