RESEARCH ARTICLE OPEN ACCESS

An application to Detect Fake Images in social media

Jhansi Priya V [1], Dr. B.N Shankar Gowda [2]
MTech student [1], Associate Professor [2], Department of Computer Science and Engineering
Bangalore Institute of Technology, K.R. Road, V.V. Puram, Bangalore, Karnataka - India

ABSTRACT

Block chain is a currently, highly emerging technology for data sharing and application. It can exchange de-centralized information in distributed systems without mutual trust by means of data encryption, timestamp and distributed consensus, so as to improve the efficiency of data sharing and application. This technology can be fully utilized in the large data remote sensing image system, and the multi-system shared node storage system can be managed efficiently and uniformly, so as to improve the economic efficiency of the system. This paper designs the shared architecture based on block chain technology, proposes key research technologies, and provides theoretical basis for non-engineering practice.

Keyword: remote sensing, block chain, Sharing, image Cloud storage, Map Reduce technique, Hash code generation.

I. INTRODUCTION

As rapid development of aerospace remote sensing platform and technology in our country, the remote sensing data generated is exponentially increasing. Data owner is a person who will store the secret image in block chain storage which in turn accessed by the authorized Data User. Data Owner will create Data User, Data Owner can able to add or delete the Data User. Data Owner is like a Head of the Department in the Military or detective agencies, who upload secret images into secure block chain storage. Whenever the secret image is uploaded it will be encrypted by the system using Data Owner Encryption Key, encrypted secret image is Block Body and the Block Header will be formed using Previous Block Hash Code, Current Block Root Hash, Time Stamp and Nonce. Once Block Body and Block Header are created and both are compressed to form a Block and store it in Block Chain Storage.

Data User are the data access users, suppose Data Owner is a Head of the Department and Data Users are his team members. Suppose the Data User wants to download any secret image file, first he has to select the file from the list and press the download button.
Based on the Secret Image selected, its block details are fetched from database and using block chain storage credentials particular block will be downloaded.

A block chain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography.

II. LITERATURE SURVEY

Jaynil Gaglani [1] Social media has become the importand of today's lifestyle. It has a spread effect on nearly every walk of life made difficult. One of the well-known social media applications Facebook Messenger is a free and platform text or image or images information on software that also provides services for sending and receiving multimedia messages. But at the same time in years, its easy accessibility has served a way for propagating fake and news articles, blogs and messages. Fake news and messages have way for Blackmailing, suicide cases Political polarization, ethnic tensions, unwanted panic and mass hysteria.

Jamal AbdulNasir [2] The explosion of social media allowed individuals to spread information without cost, with little investigation and fewer filters than before. This field found the old problem of fake news, or image or video which became a major concern now a days due to the negative impact it brings to the communities.

Matthew Bradbury[3] Providing location privacy for such an asset is tantamount to protecting the location of a source node from hacker who is attempting to locate it.

Kyumin Lee [4] Natural disasters or crises, users on social media tend to easily believe contents of postings related to the events, and retweet the postings, hoping that the postings will be reached by many other users. Unfortunately, there are malicious users who understand the tendency and post misinformation such as spam and fake messages.

In the existing system, the user may lose control of the existing image data or video or text, while the service provider usually maintains the primary stewardship. Users' access permissions to image data or records are very limited, and users are typically unable to easily share these data with researchers or providers.
The existing system encrypts and stores images in the cloud, but it does not use the block chain framework. A hacker can gain access to those images or text or videos and replace the real image with a duplicate or fake image.

III. BLOCK CHAIN TECHNOLOGIES

Block chain was first introduced by Bitcoin system in public view. This topic was first proposed in 2008 in "Bitcoin: Electronic Cash in a PTP Network" (Nakamoto 2008), but block chain technologies is not the same as Bitcoin, it is only the bottom technologies of Bitcoin.

Blockchain is highly newly a de-centralized distributed database. The data structure of the database is a series of blocks linked by fixed formats such as Hash algorithm.

Each block contains transaction information generated in a certain period of time, or other information records, which cannot be tampered with.

Blockchain is a highly emerging technology for data sharing and application.
It can exchange de-centralized data in distributed systems without mutual trust by means of data encryption, timestamp and distributed consensus, so as to improve the efficiency of data sharing and application.

This technology can be fully utilized in the large data remote sensing image system, and the multi-system shared node storage mode can be maintained efficiently, so as to improve the efficiency of the system.

This paper designs the shared architecture based on block chain technology, proposes key research technologies, and provides theoretical basis for non-engineering practice.

Development of aerospace remote sensing platform and technology in our country, the remote sensing information generated is increasing. For different acquisition platforms, independent production systems have been established. Special remote sensing text or image or video sharing service platforms have developed systematically.

All of them adopt centralized management mode. The system is huge and the tasks are complex. The corresponding information or data are trace and cannot be hacked with.

This mode of decentralized construction and independent support seriously affects the ability of data sharing services, which is incompatible with the development trend of data integration and comprehensive utilization, and at the same time restricts the application.

Block chain technology has the characteristics of de-centralization, data trustworthiness and non-tampering. It has great application potential in guaranteeing the security, integrity, traceability and non-tampering modification of data sharing application process.

Usability: Several users are going to use the system simultaneously, so the usability of the system should not get affected with respect to individual users

Reusability: Modules should be divided so that other types of system without essential much of work.

Security: Gives secure performance as much as possible but unauthorized people can't been access the information from the system without permission.

Reliability: Once a user has made some changes, the changes must be made visible by the system.

Performance: Since the system will be hosted on a single web server with a single database server in the background, performance becomes a major concern.

The system should be web-based Application which has to be developed using advanced Java technology with Tomcat web server and Mysql database server. This system has 2 actors- Data owner and Data user. Owner is the user who can able to create the data user. Data owner can able to upload the image file into block chain server. There should be a separate block creation process which has to generate block header, block body and compress these files into single block.

Data user can able to login to his home page using credentials which are provided by Data owner. Data user can download an image file, while downloading it will check whether an image is real image or fake image.

If it is a fake image he will be notified (as an image is fake), if it is real image then image will be downloaded. Block contains a timestamp, so called it has been orderly arranged. Each block contains transaction information generated in a certain period of time, or other information records, which cannot be tampered with.

Blockchain provides a secure and an immutable platform where this data can be stored and accessed by every participant. It can be implemented in the following area, Creative arts, Advertising, Film production and Video games etc.

This technology can be fully utilized in the large data remote sensing image system, and the multi-system shared node storage mode can be maintained efficiently, so as to improve the efficiency of the system.

It can exchange de-centralized data in distributed systems without mutual trust by means of data encryption, timestamp and distributed consensus, so as to improve the efficiency of data sharing and application.

Drawbacks of Existing System

- ✓ User access permissions to image data are very limited, and users are typically unable to easily share these data with researchers or providers.
- ✓ Less security.
- ✓ Can't identify Fake image.

Blockchain is considered as a highly technological revolution that was introduced. It is a PTP distributed ledger technologies to record transactions, agreements, and sales.

The advantages of the blockchain technologies are decentralized maintenance, data or information saving processing in block-then-chain structure, secure transporting and accessing of data or information in the form of text or image as well as anti-tamper and undeniable data security.

The proposed system uses blockchain storage to store images or text or video. A hacker can replace a fake image with the original. When a user attempts to download an image, the user is notified if the image is fake. If the image is real, it will be downloaded.

Advantages of Proposed System:

- ✓ Can identify Fake Image
- ✓ Security is more.

Cryptography Technique

Using cryptography technique, we are going to secure our outsourcing data. To secure the data can use asymmetric or symmetric algorithms.

FTP Protocol

FTP (File Transfer Protocol) is built on a client-server-based design model and uses different control and data connections between the client and the server designs.

It makes users to authenticate for their self with a proper text sign-in protocol, they in the form of a username and password, but can connect anonymously if the server is accepted to allow it otherwise not allowed.

FTP make uses the Internet's TCP/IP protocols to enable data transformation.

FTP promotes sharing of files through remote computers with reliable and efficient data or information transformation.

To present an analysis of the technics for Image integrity verification, that is, the detection of manipulated images or text of videos in cloud storage.

A block chain, is a developing list of records, called blocks, which are linked each other to using cryptography. Block contains cryptographic hash of the Previous Block Hash Code, Current Block Root Hash, Time Stamp and Nonce data.

Architecture

It is so called as software design pattern for developing web applications. This Architecture is described following parts of figure as shown in parts below:

- **Model** - The lowest level is representing the pattern which for maintaining the data.
- **View** – This middle level is responsible for showing all or a portion of the data to the user.
- **Controller** - Software Code that controls the interactions between the Model and View which are in the middle and lower part of diagram.

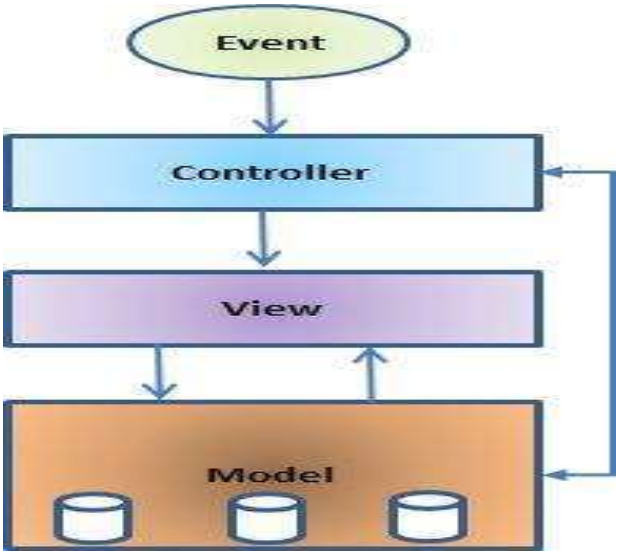

Figure 1: The MVC Architecture for Data maintaining, displaying.

MVC is well known as it isolates the application logic from the user interface layer and support separate layer. Here the Controller receives all requests for the application and then works with the Model to prepare any data needed by the View as shown in figure. The View then uses the data or information prepared by the Controller to generate a final presentable response.

Cloud Technology

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet.
Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility. Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance.
To present an analysis of the methods for Image integrity verification, that is, the detection of manipulated images in cloud storage.

Data Owner

Data owner is a person who will store the secret image in block chain storage which in turn accessed by the authorized Data User. Data Owner will create Data User, Data Owner can able to add or delete the Data User. Data Owner is like a Head of the Department in the Military or detective agencies, who upload secret images into secure block chain storage. Whenever the secret image is uploaded it will be encrypted by the system using Data Owner Encryption Key, encrypted secret image is Block Body and the Block Header will be formed using Previous Block Hash Code, Current Block Root Hash, Time Stamp and Nonce. Once Block Body and Block Header are created and both are compressed to form a Block and store it in Block Chain Storage.

Data User

Data User are the data access users, suppose Data Owner is a Head of the Department and Data Users are his team members. Suppose the Data User wants to download any secret image file, first he has to select the file from the list and press the download button. Based on the Secret Image selected, its block details are fetched from database and using block chain storage credentials particular block will be downloaded. Once the block downloaded, system has to extract he block body and block header separately, block body has to decrypt using authorized key and secret image will be produced. To verify whether the secret image is fake or real, block chain verification process will take place and result shown to the data user.

Block chain Technology

A block chain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

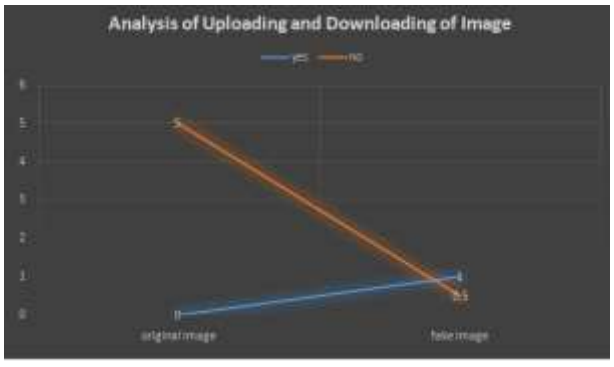

Figure 2: To store images, if hacker can replace a fake image with the original. When a user attempts to download an image, the user is notified if the image is fake. If the image is real, it will be downloaded.

VI. CONCLUSION

In this paper, block chain technology is briefly introduced, and the application prospects of its technological advantages in large data sharing services of remote sensing images are analyzed. Several key technologies and the whole service architecture that need to be solved are planned. The design concept of the system conforms to the nature of the block chain, which can fully guarantee the efficiency of the system and enhance the application service ability of remote sensing images.

VII. REFERENCES

[1] Wang B, Li B, Li H. Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud[C]// International Conference on Applied Cryptography and Network Security. Sprinter-Verlag, 2012:507-525.

[2] Till N, Philipp A, Hannes H. A simulation model for analysis of attacks on the Bitcoinpeer-to-peer network[C]// Ieee/ifip Workshop on Security for Emerging Distributed Network Technologies. 2015:1327-1332.

[3] Swan M. Blockchain: Blueprint for a New Economy [M]. O'Reilly Media, Inc. 2015.

[4] Huh S, Cho S, Kim S. Managing IoT devices using blockchain platform[C]// International Conference on Advanced Communication Technology. IEEE, 2017:464-467.

[5] Haber S, W. Stornetta W.S. How to time-stamp a digital document [J]. Journal of Crypt- ology, 1991, 3(2):99-111.

[6] Hao J J, Guo H. Digital Signature Based on Elliptic Curve Encryption Algorithm [J]. Modern Computer, 2008(1):57-59.

[7] Zhang Z W. Delegated Byzantine Fault Tolerance[0L].[2017-12-09]. http://www.8btc.com/onchain-paper-antshares.

[8] Slamanig D, Hanser C. On Cloud Storage and the Cloud of Clouds Approach[C] //Proceedings of the 7th International Conference for Internet Technology and Secured Transactions, London: IEEE, 2012: 649-655.

[9] S, Kim S. Managing IoT devices using blockchain platform[C]// International Conference on Advanced Communication Technology.

[10] Hannes H. A simulation model for analysis of attacks on the Bitcoinpeer-to-peer network.