Parshvanath Charitable Trust's

A. P. SHAH INSTITUTE OF TECHNOLOGY

(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

Enhancing Cloud Security Using Blockchain.

Group Number: 10

Group Members

Dhananjay Yadav : 17204015
Aditi Shinde : 16104022
Akash Nair : 16104051

Project Guide: Prof. Poonam Dhawale

Abstract

The practice of using a network of remote servers hosted on the internet to store, manage and process data rather than a local server or a personal computer is called a cloud. A proposal is made to enhance the security of data stored on cloud service by using blockchain as the technology. The protocol is used to store data on cloud in the form of chunks or blocks which are linked to each other by hash pointers which allows the data to be stored in historical format and ensures better security.

Introduction

- The cloud is just a metaphor for the internet. Cloud computing is a technology that uses the internet and central remote servers to maintain data and application.
- Cloud computing allows consumer and business to use application without installation and access their personal files to any computer with internet access.
- Security is one of the major concerns when it comes to cloud based services , our project ensures blockchain as one of the prominent technology for security.

data
BLOCKCHAIN
SECURE
dreamstime.com

Objective

- To provide effective security to the data stored on cloud.
- To maintain better integrity of data on cloud.
- To avoid fraudery of data.
- To have the consensus mechanism for the cloud group users.

Literature Review

Paper title:- Bitcoin: A peer-to-peer electronic cash system.

Author:-Nakamoto S

Publication details:- https://bitcoin.org/bitcoin.pdf

Findings:- Revised the implementation of blockchain as a technology with a wide scope and found its use in the first cryptocurreny ever created i.e. Bitcoin with blockchain as a technology and SHA-256 as its hash function. First general use of blockchain to secure transactions.

Advantages:- Provides a secure means of transaction with lowest possible chance of risks involved with tampering. Calculating hash would require a lot of effort.

Disadvantages:- Requires a good network speed and is not as cost effective when it comes to transactions. Its also complex to be implemented.

Literature Review

Paper title:-Blockchain contract: A complete consensus using blockchain.

Author:- Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami

Publication details:- 2015 IEEE 4th Global Conference on Consumer Electronics.

Findings:- Use of blockchain consensus in online or data contracts and making it more secure. Consensus mechanism allows every party in the contract to share their consent regarding the contract which provides a secure and satisfactory result.

Advantages:- The parties involved in the contract might be anonymous because of blockchain. This helps keep the information from being overunned in the cyberspace.

Disadvantages:- The consensus mechanism consumes a lot of resources, hence its hefty to be used. The anonymity because of blockchain is also a concern when dealing with the cyber fraudery.

Literature Review

Paper title:- IHIDS:Introspection-Based Hybrid Intrusion Detection System in Cloud Environment”

Author:- Amita Kashyap, G. Sravan Kumar, Sunita Jangir, Emmanuel S. Pilli, Preeti Mishra

Publication details:- 2017 IEEE

Findings:- Use of Intrusion detection system in the hypervisor layer of the cloud which allows the cloud owner and admin to be notified when in the midst of intrusion by an unauthorized party.

Advantages:- Notifies all unnatural activities to the cloud admin and also notifies internal or external attacks since all data passes through the hypervisor layer.

Disadvantages:- IDS only notifies the infiltration, it doesn’t lock it. Hence, at times it would be too late before the user or admin is notified.

Literature Review

Paper Title:- Cloud Threat Defense – A Threat Protection and Security Compliance Solution.

Author:- Bharadwaj, D. R., Bhattacharya, A., & Chakkaravarthy, M.

Publication Details:- 2018 IEEE International Conference on Cloud Computing in Emerging
Markets (CCEM).

Findings:- Investigating some of the key research challenges of cloud security solutions to secure the dynamic cloud environment and provide a practical solution to overcome the challenges that the cloud providers and consumers face securing their data and valuable assets.

Advantages:- Lets us know about the challenges faced in securing the cloud. Security issues in the cloud. The categories in with the security threats can be mitigated.

Disadvantages:- Doesn't provide you with a specific solution to a certain domain, all threats and challenges are related to overall cloud environment.

Literature Review

Paper title:- Study on data security policy based on cloud storage.
Author:- DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan.
Publication details:- 2017 IEEE 3rd Conference on Big Data security on Cloud

Findings:- Listing out all possible security threat vulnerabilities and issues regarding data storage on cloud and also regarding its associated services.

Advantages:- Provides a detailed study of security risks and technical issues regarding cloud and its services.

Problem Definition

- To provide cloud storage architecture which will ensure better security on the cloud servers thus providing secure means of data transaction.
- Our project uses blockchain as a technology to provide security.

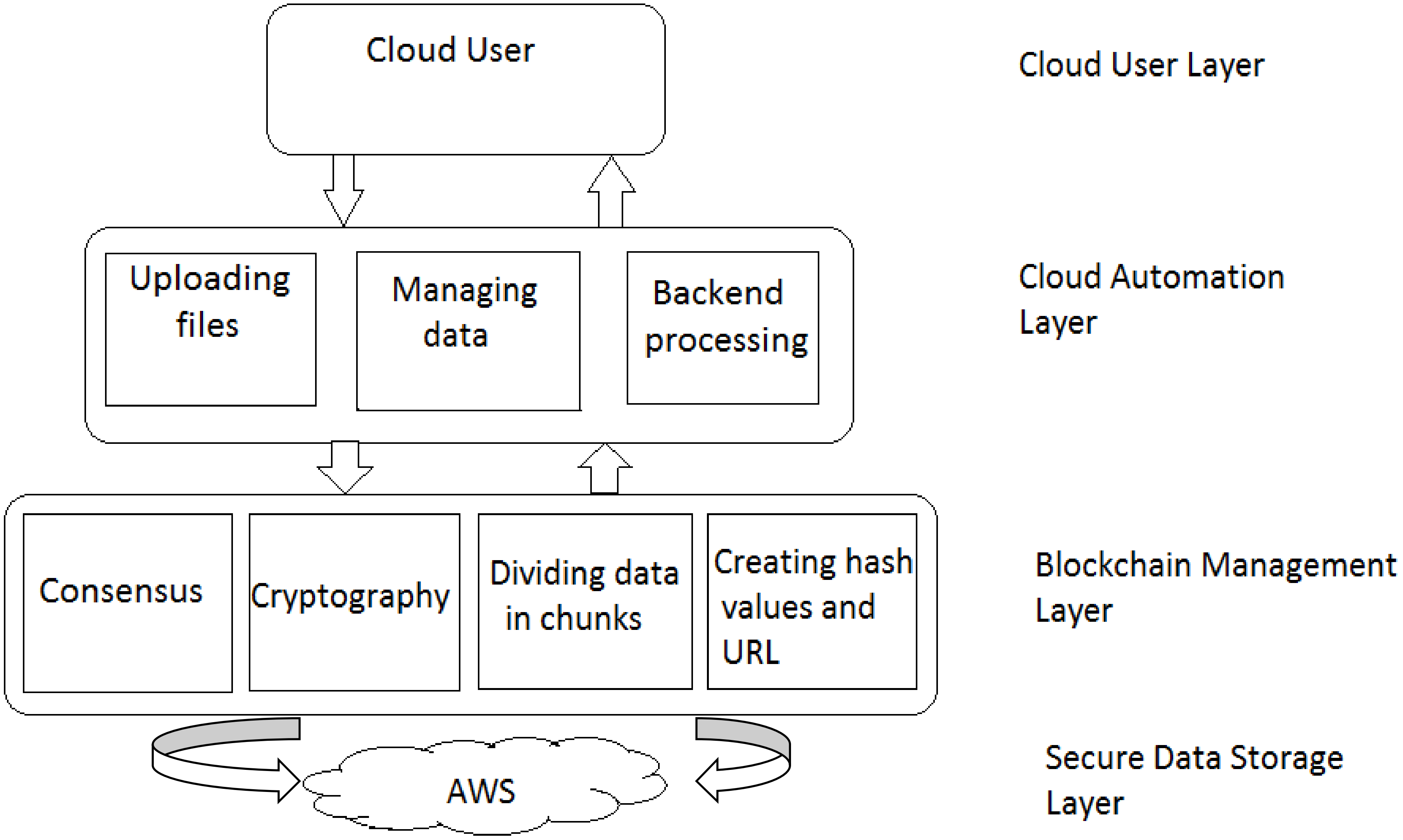
Existing System Architecture

- Current cloud services provide multilevel security which includes technologies like encryption, captcha, OTP based and Key based security.
- The encryption standards include AES-256, DES, 3-DES and RSA.
- The current cloud storage has an optional encryption facility which needs to be enabled for the data to be encrypted on the cloud. If the user is not aware of the encryption service resulting in non-encrypted data storage.

Proposed System Architecture/Working

- Securing data through blockchain.
- Applying KMS(Key Management Service).
- Applying automatic encryption to the data.

Proposed System Architecture/Working



Cloud User

Cloud User Layer

Uploading files

Managing data

Backend processing

Cloud Automation Layer

Consensus

Cryptography

Dividing data in chunks

Creating hash values and URL

Blockchain Management Layer

AWS

Secure Data Storage Layer

Technology stack

- AWS Cloud Service for storing data.
- SHA 256 cryptographic algorithm for creating hash values of data.
- Navicat- For visualization of the blocks .
- Eclipse Luna- Integrated Development Environment(IDE) for java programming.
- My SQL- For Database.
- JDK 1.6 and above- For programming as it is object oriented, easy to write, compile, debug, platform-independent.
- Blockchain- A blockchain has three main components: cryptography, distributed list structures and a decentralized system. Depending on these three which can be implemented through software, blockchain can be open source or proprietary . Its one of the latest technological trends now in the industry and provides a highly secure environment when used as compared to other cryptography and encryption standards.

System Specification

Software Requirement

➢ Operating System	: Windows 07 And Above
➢ Programming Language	: JAVA
➢ Java Version	: JDK 1.6 & above.
➢ Data Base	:MYSQL.
➢ Tool	:Navicat, Eclipse Luna

Hardware Requirement

➢System	:	core i3 And Above.
➢Hard Disk	:	40 GB Minimum.
➢Ram	:	2 Gb Minimum.

Scope of our project

- Can be implemented on any kind of data that is stored on the cloud.
- Can be used to provide security to any confidential data.
- Can be implemented in sectors like IT, Medical, Banking , etc.

Project Limitations

- Need to have a good internet connection constantly.
- Specific bandwidth allowance.
- Architecture may be complex to implement.

Conclusion

In this proposal we describe the use of blockchain and its related mechanism to ensure better cloud security. The consensus mechanism makes it possible to have the consent of the cloud user groups to change the data on the cloud, thus enhancing the data integrity with minimal risk of data fraudery. In future work, new protocols can be implemented for the multi-owner based cloud data groups to have a more efficient way of data authentication and making the data transactions more secure.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[2] 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) Amita Kashyap, G. Sravan Kumar, Sunita Jangir, Emmanuel S. Pilli, Preeti Mishra “IHIDS: Introspection-Based Hybrid Intrusion Detection System in Cloud Environment”.

[3] Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., &Kishigami, J. J. (2015). Blockchain contract: A complete consensus using blockchain. 2015 IEEE 4th Global Conference on Consumer Electronics (GCCEP).

[4] Zhe, D., Qinghong, W., Naizheng, S., & Yuhan, Z. (2017). Study on Data Security Policy Based on Cloud Storage. 2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS).

[5] Bharadwaj, D. R., Bhattacharya, A., & Chakkaravarthy, M. (2018). Cloud Threat Defense – A Threat Protection and Security Compliance Solution. 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM).