IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 14, Issue 4, April 2024, ||Series -2|| PP 212-223

Blockchain-Enhanved Security Framework in Cloud Computing Integration

[1.] **Masabattula. Jyothika Naga Sowmya**, *B. Tech, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY, Sowmya.masabattula2003@gmail.com*

[2.] **Marisetti. Srinivas**, *B. Tech, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY, srininvassrinivas45946@gmail.com*

[3.] **Durre. Mohan Durga Reddy**, *B. Tech, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY, durremohan@gmail.com*

[4.] **Mudhunuri. Vishnu Vardhan Raju**, *B. Tech, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY, vishnumudunuri551@gmail.com*

[5.] **Kamani. Chandran**, *M. Tech, Assistant Professor, Department of computer science and engineering, Chandran.kamani@gmail.com*

Abstract: *This paper proposes a novel approach to address data integrity concerns in cloud computing by integrating blockchain technology. With the vulnerability of cloud services to data manipulation, ensuring the accuracy and trustworthiness of data becomes paramount. By leveraging blockchain's tamper-proof nature, the proposed scheme enhances data integrity within homomorphic encryption frameworks. Through collaborative computations among Cloud Service Providers (CSPs), master hash values are generated for their respective databases. These values are then securely stored in Ethereum blockchain networks, ensuring immutability. The abstract presents a theoretical analysis of the overhead costs associated with creating master hash values across various cryptocurrencies. This innovative fusion of cloud computing and blockchain offers a robust solution to safeguard data integrity, catering to diverse application domains and addressing the evolving threat landscape.*

Index Terms: *Blockchain, cloud computing, data integrity, homomorphic encryption.*

I. INTRODUCTION

Data security in the realm of cloud computing is a critical concern, given the multitude of potential threats it faces. The amalgamation of various technologies within cloud computing infrastructure renders it particularly susceptible to vulnerabilities [1]. Thus, managing risks becomes imperative to strike a balance between security measures and the benefits of cloud computing [1].

The Cloud Security Alliance (CSA), a non-profit organization, has been established to address these concerns by delineating shared responsibilities between Cloud Service Providers (CSPs) and clients to mitigate risks associated with cloud computing [2]. Essential security controls are delineated through tools such as the Consensus Assessments Initiative Questionnaire (CAIQ) and the Cloud Control Matrix (CCM) [2]. These frameworks aid in designing and implementing security measures, ensuring that both CSPs and clients uphold their obligations in safeguarding data integrity and privacy.

Despite the efforts of CSPs to establish robust security frameworks, there remains a lingering skepticism among data owners regarding the sufficiency of these measures [1]. This skepticism is compounded by the rapid growth of cloud computing technology, which introduces new vulnerabilities while amplifying existing ones [1]. A recent survey conducted by the CSA identified the top security threats within cloud computing, categorizing them into governance and operational domains [3]. These threats encompass a spectrum of concerns ranging from strategic policy issues to tactical security challenges [3].

Foremost among these threats is the risk of data breaches, which has consistently ranked high in trend analyses conducted by the CSA [3]. A data breach, whether resulting from targeted attacks or inadvertent human error, poses a significant threat to the validity and trustworthiness of cloud-based services [3]. Such breaches entail unauthorized access, analysis, or exploitation of sensitive information, undermining data confidentiality and privacy [7].

Encryption algorithms play a pivotal role in addressing these concerns by safeguarding data confidentiality and privacy. However, traditional cryptographic methods may not be ideally suited for cloud computing environments, where data processing on external servers necessitates decryption [18]. To overcome this limitation, homomorphic encryption (HE) schemes have been proposed, enabling computations on encrypted data without revealing sensitive information [20].

Yet, the centralized management approach of CSPs introduces administrative risks, potentially compromising data integrity and security [1]. To mitigate these risks and enhance transparency in data manipulation, blockchain (BC) technology emerges as a promising solution [23]. By decentralizing control and ensuring tamper-proof records, blockchain enhances the security posture of cloud computing environments [23].

While several studies have explored the integration of blockchain with cloud computing to address security concerns [23], challenges persist, including complex configuration setups and resource-intensive implementations [23]. Despite these challenges, the synergistic integration of homomorphic encryption and blockchain presents a compelling avenue for enhancing data security in cloud computing environments.

II. LITERATURE SURVEY

Cloud computing has revolutionized the way data is stored, processed, and accessed, offering unparalleled flexibility and scalability. However, this paradigm shift also brings forth a myriad of security concerns that need to be addressed to ensure the confidentiality, integrity, and availability of data [1]. A comprehensive understanding of these security issues and the deployment of suitable cryptographic techniques are crucial for fortifying cloud computing environments against potential threats [1].

A survey conducted by Agarwal et al. comprehensively explores the security challenges inherent in cloud computing and discusses various cryptographic techniques employed to mitigate these risks [1]. The study highlights the significance of encryption algorithms in safeguarding sensitive data from unauthorized access and emphasizes the need for robust security measures to counter emerging threats [1].

The Cloud Security Alliance (CSA) identifies the "Egregious Eleven" threats to cloud computing, shedding light on the most pressing security concerns faced by cloud service providers and users alike [3]. These threats encompass a wide range of issues, including data breaches, insider threats, and account hijacking, underscoring the complexity of securing cloud-based systems in the face of evolving cyber threats [3].

Phaphoom et al. provide a foundational overview of cloud computing, examining its technological landscape and underlying principles [8]. The study elucidates the fundamental concepts of cloud computing architecture and highlights the importance of understanding the vulnerabilities inherent in cloud-based infrastructures [8].

Grobauer et al. delve into the intricacies of cloud computing vulnerabilities, offering insights into the potential security risks associated with cloud deployments [9]. The study emphasizes the need for a comprehensive understanding of these vulnerabilities to develop effective security strategies for mitigating risks and safeguarding sensitive data [9].

Modi et al. conduct a survey on security issues across different layers of cloud computing, examining the challenges posed by infrastructure, platform, and software-as-a-service models [11]. The study underscores the multifaceted nature of cloud security and explores various solutions aimed at addressing security concerns at each layer of the cloud computing stack [11].

Liu et al. present the NIST cloud computing reference architecture, offering a standardized framework for understanding and implementing cloud-based systems [12]. The reference architecture delineates the key components and interactions within cloud environments, providing a blueprint for organizations to design secure and resilient cloud infrastructures [12].

Madhubala conducts a survey on security concerns in cloud computing, highlighting the diverse array of challenges faced by cloud service providers and users [13]. The study examines the implications of security breaches on cloud-based systems and explores potential mitigation strategies to bolster the security posture of cloud environments [13].

In summary, the literature survey underscores the critical importance of addressing security concerns in cloud computing through the deployment of robust cryptographic techniques and comprehensive security measures. By understanding the vulnerabilities inherent in cloud-based systems and leveraging standardized frameworks and best practices, organizations can effectively mitigate risks and safeguard sensitive data in the cloud.

III. METHODOLOGY

a) Proposed Work:

The integration of blockchain technology into cloud computing infrastructure presents a novel solution to address existing limitations. By harnessing blockchain's decentralized and transparent nature, the proposed system aims to bolster data integrity, privacy, and security in cloud environments. Blockchain's tamper-proof ledger ensures immutable recording of data changes, establishing a transparent and verifiable audit trail. Real-time auditing capabilities foster trust and accountability among users, while granting them greater control over their data. Standardized protocols facilitate interoperability between cloud platforms and Blockchain[23-25] networks, enabling seamless integration and collaboration. Overall, the proposed system offers a comprehensive solution to enhance data integrity, security, privacy, scalability, and user empowerment within cloud computing, promising a more reliable and trustworthy computing experience.

b) System Architecture:

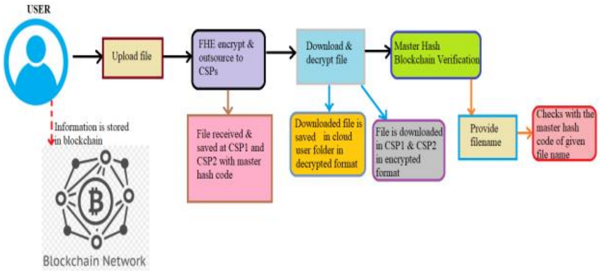

USER
Upload file
FHE encrypt & outsource to CSPs
Download & decrypt file
Master Hash Blockchain Verification
Information is stored in blockchain
File received & saved at CSP1 and CSP2 with master hash code
Downloaded file is saved in cloud user folder in decrypted format
File is downloaded in CSP1 & CSP2 in encrypted format
Provide filename
Checks with the master hash code of given file name
Blockchain Network

Fig1 Proposed Architecture

The system architecture comprises four main components: User Interface, Cloud Service Providers (CSPs), Blockchain Network, and File Encryption/Decryption Module.

User Interface: Users interact with the system through a user-friendly interface where they can upload files securely.

Cloud Service Providers (CSPs): Upon file upload, the File Encryption/Decryption Module encrypts the file using Fully Homomorphic Encryption[29] (FHE) techniques. The encrypted file is then outsourced to CSPs for storage. Each CSP saves the encrypted file along with a master hash code to ensure data integrity.

File Encryption/Decryption Module: This module handles the encryption of uploaded files using FHE and the decryption of downloaded files. Decrypted[19] files are stored in the user's cloud folder, while encrypted copies are retained at CSPs.

Blockchain Network: Information about each file and its associated master hash code is stored in a Blockchain[24] network to provide transparent verification of data integrity. Users can verify file integrity by providing the filename and comparing its master hash code with the blockchain records.

Overall, this architecture ensures secure file storage, transmission, and verification through the integration of FHE, CSPs, and blockchain technology.

c) CSP1:

CSP1 acts as a cloud service provider module in the system. It accepts encrypted files, master hashes, and filenames from the Cloud User module. Upon receiving encrypted files, CSP1 stores them securely and generates a master hash for each file. Additionally, CSP1 facilitates file decryption and participates in blockchain verification by comparing master hashes stored in the Ethereum Blockchain with those provided by users, ensuring data integrity and security.

d) CSP2:

CSP2, another cloud service provider module, receives encrypted files, master hashes, and filenames from the Cloud User module. It securely stores encrypted files and associated master hashes. Additionally, CSP2 participates in file decryption upon user request. Furthermore, it collaborates in blockchain verification, comparing received master hashes with those stored in the Ethereum Blockchain. Successful matching ensures data integrity and security within the system.

e) Cloud User:

The Cloud User uploads files, which are encrypted using FHE and outsourced to CSPs. The system generates Master Hashes for each file. Users can download and decrypt files as needed. Additionally, they can request data verification through the Ethereum Blockchain to ensure data security.

i) Upload File: The Cloud User uploads files to the system. After uploading, the files are encrypted using FHE[28] and outsourced to CSPs (CSP1 and CSP2). Before uploading, the system generates a Master Hash for each file to ensure data integrity and security in the cloud.

ii) FHE Encrypt & outsource to CSP's: The Cloud User's uploaded file undergoes FHE[27-30] encryption before being outsourced to multiple CSPs (CSP1 and CSP2). The system generates a Master Hash for each file prior to uploading it to the cloud. This ensures secure transmission and storage of data while maintaining data integrity.

iii) Download & Decrypt File: The Cloud User downloads files from CSPs and decrypts them as needed. Downloaded files are saved in the user's folder in decrypted format, ensuring access to the original content. Additionally, files are downloaded in encrypted format by CSP1 and CSP2 for secure storage.

iv) Master Hash Blockchain Verification: The Cloud User requests data verification by invoking the Ethereum Blockchain, where Master Hash codes for all files are stored. The Blockchain calculates the stored file's Master

Hash[33-37] and compares it with the one received from the user. Successful matching ensures data integrity and security.

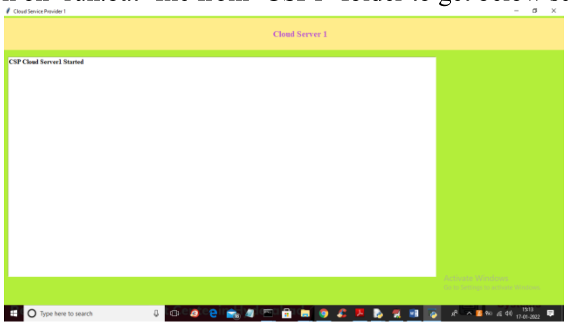
f) Blockchain Integration:
Blockchain's smart contracts are deployed specifically to securely store Master Hashes generated for each file. These Master Hashes act as tamper-proof references for the associated data, ensuring that the data remains intact and unaltered.

Blockchain technology provides both data security and decentralization. Data is distributed across multiple nodes within the blockchain network, making it highly resistant to tampering. Altering data on one node would necessitate altering it on all nodes, an impractical and near-impossible task.

Blockchain technology enables real-time alerts for users concerning data integrity. Users can actively verify the authenticity of their data by comparing the Master Hashes stored on the blockchain with the corresponding data. This process ensures that any unauthorized changes are immediately detected and can be addressed.

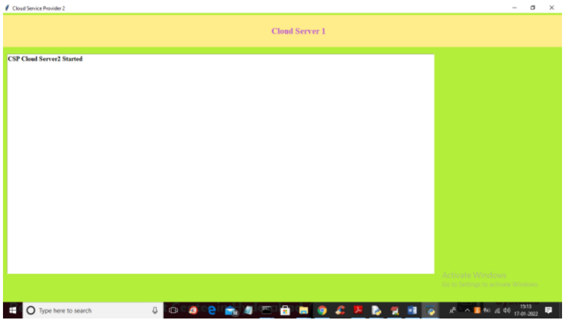
IV. EXPERIMENTAL RESULTS

To run project first double click on 'run.bat' file from 'CSP1' folder to get below screen



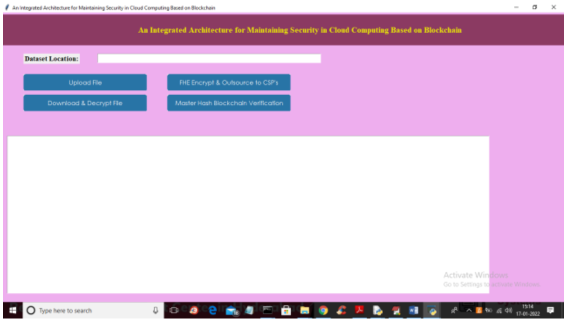
CSP Cloud Server1 Started

In above screen CSP1 server started and now double click on 'run.bat' file from 'CSP2' folder to get below screen

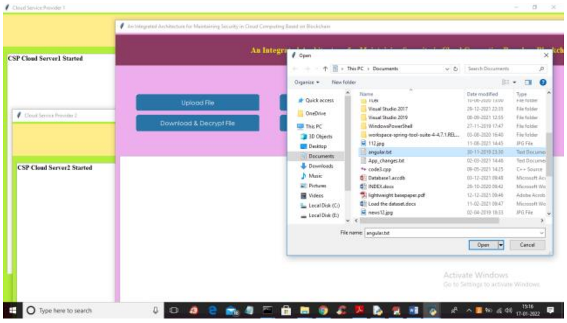


CSP Cloud Server2 Started

In above screen cloud server CSP2 services started and now double click on 'run.bat' file from 'CloudUser' folder to get below screen


An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
Dataset Location:
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification
Type here to search

In above screen click on 'Upload File' button to upload any file



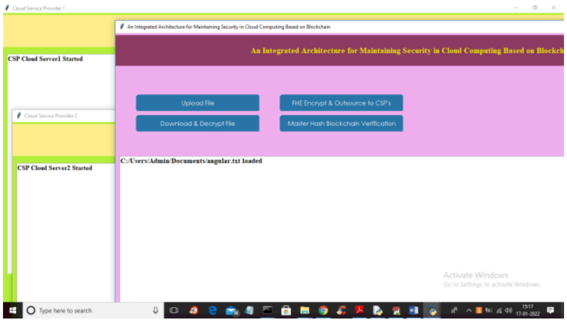
CSP Cloud Server1 Started

CSP Cloud Server2 Started

Name	Date modified	Type
Visual Studio 2017	29-12-2021 22:35	File folder
Visual Studio 2019	08-09-2021 12:55	File folder
WindowsPowerShell	27-11-2019 17:47	File folder
workspace-spring-tool-suite-4-4.7.1.REL...	03-08-2020 16:40	File folder
112.jpg	11-08-2021 14:45	JPG File
angular.txt	30-11-2019 23:30	Text Documen
App_changes.txt	02-03-2021 14:46	Text Documen
code3.cpp	09-05-2021 14:25	C++ Source
Database1.accdb	03-12-2021 09:48	Microsoft Acc
INDEX.docx	29-10-2020 09:42	Microsoft Wo
lightweight basepaper.pdf	12-12-2021 09:46	Adobe Acrob
Load the dataset.docx	11-02-2021 09:47	Microsoft Wo
news12.jpg	02-04-2019 18:33	JPG File

File name: angular.txt

In above screen selecting and uploading file and then click on 'Open' button to upload file and to get below screen

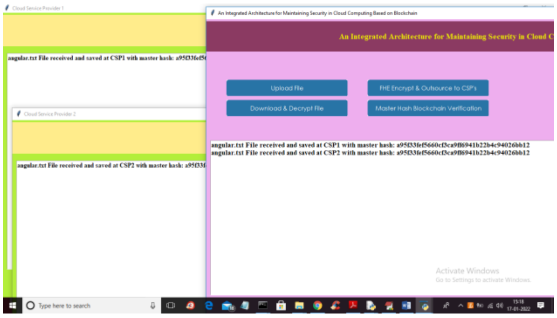

Cloud Service Provider 1
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockch
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification
Cloud Service Provider 2
Activate Windows
Go to Settings to activate Windows.
Type here to search
15:17
17-01-2022

CSP Cloud Server1 Started

CSP Cloud Server2 Started

C:/Users/Admin/Documents/angular.txt loaded

In above screen file is uploaded and now click on 'FHE Encrypt & outsource to CSP's' button to outsource file to cloud

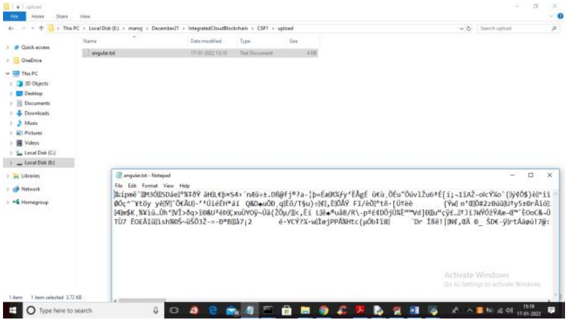

Cloud Service Provider 1
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud C
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification
Cloud Service Provider 2
Activate Windows
Go to Settings to activate Windows.
Type here to search
15:16
17-01-2022

angular.txt File received and saved at CSP1 with master hash: a95f33fef5

angular.txt File received and saved at CSP2 with master hash: a95f33f

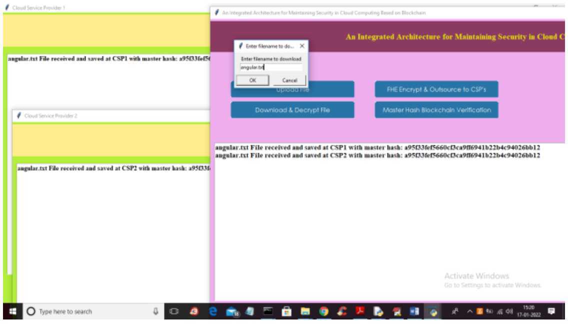
```
angular.txt File received and saved at CSP1 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
angular.txt File received and saved at CSP2 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
```

In above screen we can see file outsource to multiple CSP and we can see its master hash also and in CSP 1 or 2 folder under 'upload' folder you can see file saved in encrypted format



Name	Date modified	Type	Size
angular.txt	17-01-2022 15:16	Text Document	4 KB

In above screen at cloud side we can see file saved in encrypted format and now go back to application and then click on 'Download & Decrypt File' button to download and decrypt file


Cloud Service Provider 1
Cloud Service Provider 2
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud C
Enter filename to do...
OK
Cancel
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification
Activate Windows
Go to Settings to activate Windows.
Type here to search

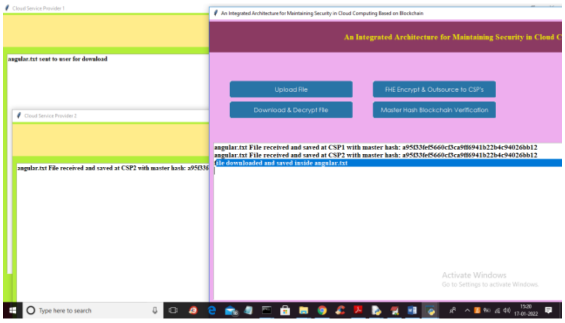
Enter filename to download: angular.txt

```
angular.txt File received and saved at CSP1 with master hash: a95f33fef5
```

```
angular.txt File received and saved at CSP2 with master hash: a95f33f
```

```
angular.txt File received and saved at CSP1 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
angular.txt File received and saved at CSP2 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
```

In above screen enter file name to download and then click ‘OK’ button to download that file and to get below output

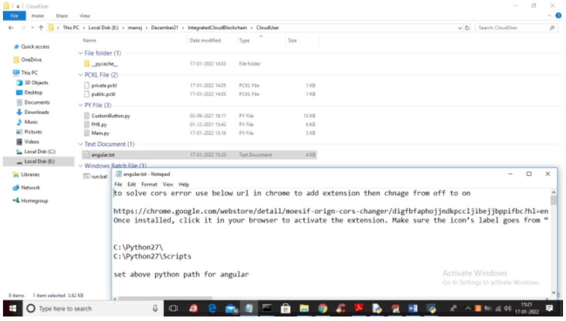

Cloud Service Provider 1
Cloud Service Provider 2
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud C
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification
Activate Windows
Go to Settings to activate Windows.
Type here to search

```
angular.txt sent to user for download
```

```
angular.txt File received and saved at CSP2 with master hash: a95f336
```

```
angular.txt File received and saved at CSP1 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
angular.txt File received and saved at CSP2 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
file downloaded and saved inside angular.txt
```

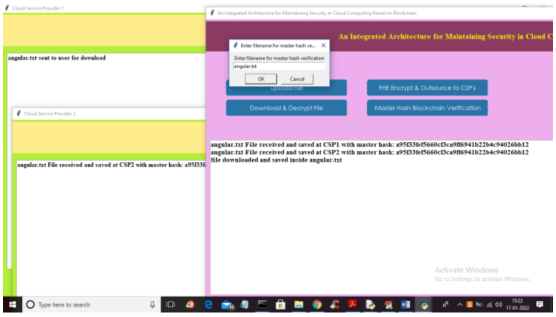
In above screen in blue colour text we can see file downloaded inside ‘CloudUser’ folder and we can see that file downloaded in decrypted format



Name	Date modified	Type	Size
File folder (1)			
__pycache__	17-01-2022 14:03	File folder	
PCKL File (2)			
private.pckl	17-01-2022 14:05	PCKL File	1 KB
public.pckl	17-01-2022 14:05	PCKL File	1 KB
PY File (3)			
CustomButton.py	03-09-2021 18:11	PY File	13 KB
FHE.py	01-12-2021 15:42	PY File	6 KB
Main.py	17-01-2022 15:16	PY File	5 KB
Text Document (1)			
angular.txt	17-01-2022 15:20	Text Document	4 KB
Windows Batch File (1)			
run.bat			

```
to solve cors error use below url in chrome to add extension then chnage from off to on

https://chrome.google.com/webstore/detail/moesif-orign-cors-changer/digfbfaphojjndkpccljibejjbppifbc?hl=en
Once installed, click it in your browser to activate the extension. Make sure the icon's label goes from "


C:\Python27\
C:\Python27\Scripts

set above python path for angular
```

In above screen we can see file decrypted and now go back to application and then click on ‘Master Hash Blockchain Verification’ button to enter file and then get master has verification from Blockchain


Cloud Service Provider 1
Cloud Service Provider 2
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud C
Enter filename for master hash ve...
OK
Cancel
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification
Activate Windows
Go to Settings to activate Windows.
Type here to search

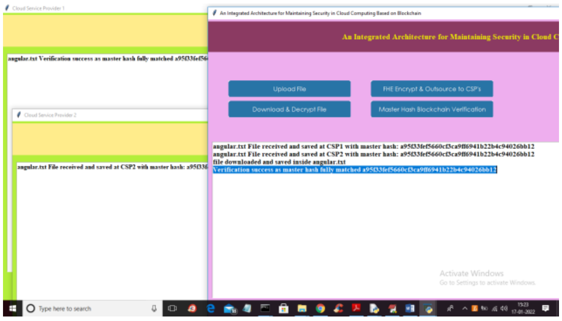
Enter filename for master hash verification: angular.txt

```
angular.txt sent to user for download
```

```
angular.txt File received and saved at CSP2 with master hash: a95f336
```

```
angular.txt File received and saved at CSP1 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
angular.txt File received and saved at CSP2 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
file downloaded and saved inside angular.txt
```

In above screen enter filename for which verification has to done and then click on ‘OK’ button to get below output


Cloud Service Provider 1
Cloud Service Provider 2
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud C
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification
Activate Windows
Go to Settings to activate Windows.
Type here to search

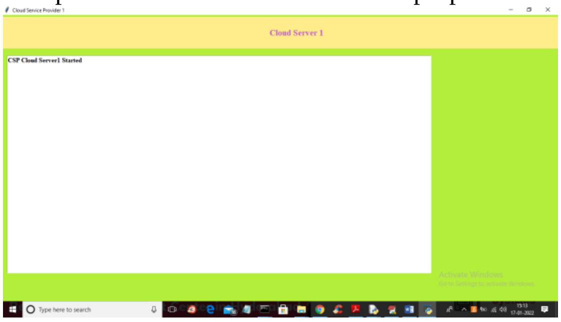
angular.txt Verification success as master hash fully matched a95f33fef56

angular.txt File received and saved at CSP2 with master hash: a95f33f

```
angular.txt File received and saved at CSP1 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
angular.txt File received and saved at CSP2 with master hash: a95f33fef5660cf3ca9ff6941b22b4c94026bb12
file downloaded and saved inside angular.txt
Verification success as master hash fully matched a95f33fef5660cf3ca9ff6941b22b4c94026bb12
```

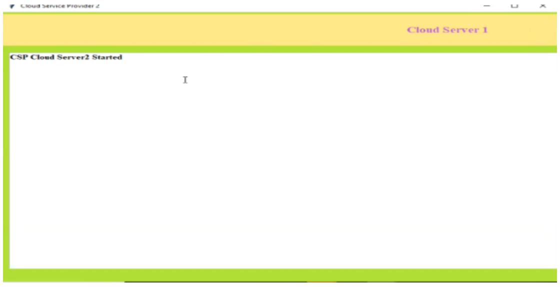
In above screen in blue colour text we can see master hash verification successful and similarly you can upload and download any number of files and for each file you can perform verification.

In below screen we can see the computation time difference between propose FHE and extension CHA-CHA



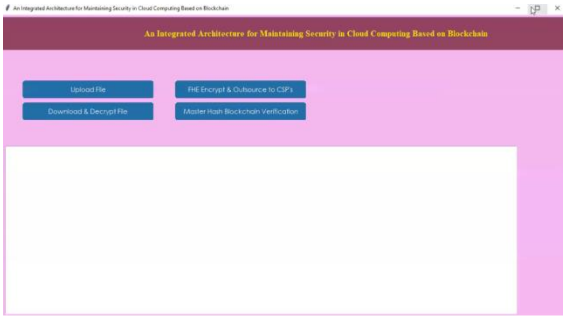
CSP Cloud Server1 Started

In above screen CSP1 server started and now double click on 'run.bat' file from 'CSP2' folder to get below screen

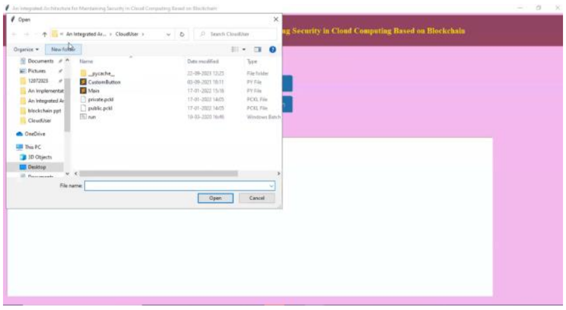


CSP Cloud Server2 Started

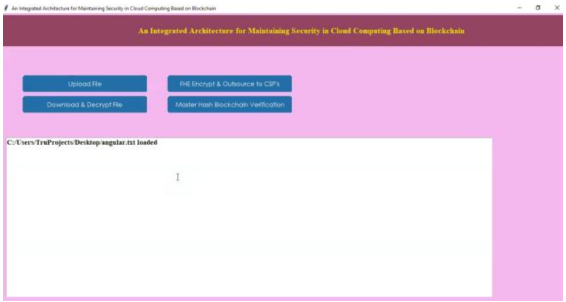
In above screen cloud server CSP2 services started and now double click on 'run.bat' file from 'CloudUser' folder to get below screen


An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification

In above screen click on 'Upload File' button to upload any file

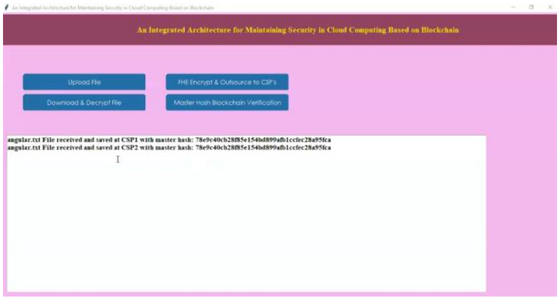


In above screen selecting and uploading file and then click on ‘Open’ button to upload file and to get below screen

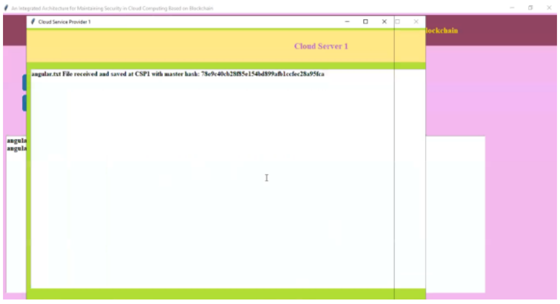

An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification

```
C:/Users/TruProjects/Desktop/angular.txt loaded
```

In above screen file is uploaded and now click on ‘FHE Encrypt & outsource to CSP’s’ button to outsource file to cloud

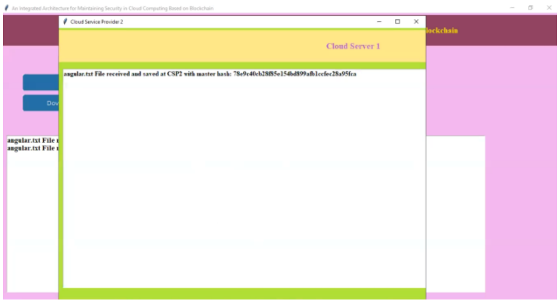

An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification

```
angular.txt File received and saved at CSP1 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
angular.txt File received and saved at CSP2 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
```


An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
Cloud Service Provider 1
Cloud Server 1
lockchain

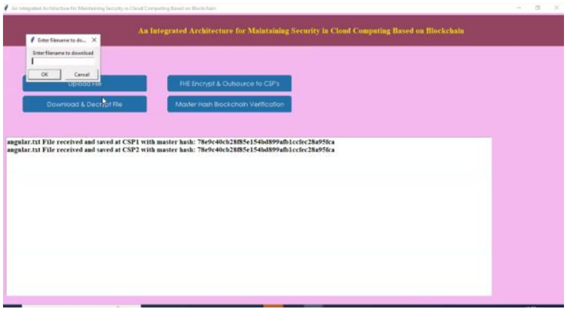
```
angular.txt File received and saved at CSP1 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
```

In above screen we can see file outsource to multiple CSP and we can see its master hash also and in CSP 1 or 2 folder under ‘upload’ folder you can see file saved in encrypted format


An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
Cloud Service Provider 2
Cloud Server 1
lockchain
Dov

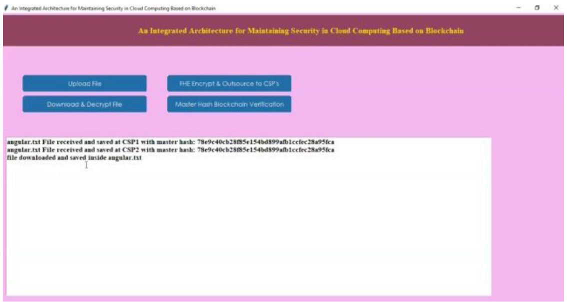
```
angular.txt File received and saved at CSP2 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
```

In above screen at cloud side we can see file saved in encrypted format and now go back to application and then click on ‘Download & Decrypt File’ button to download and decrypt file


An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
Enter filename to do...
Enter filename to download
OK
Cancel
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification

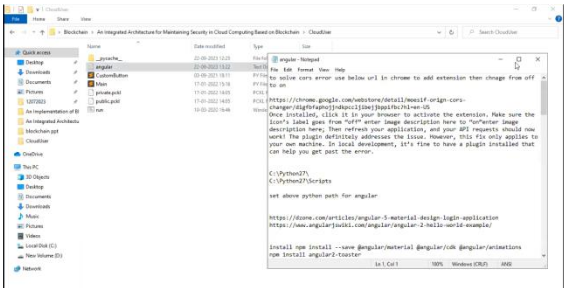
```
angular.txt File received and saved at CSP1 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
angular.txt File received and saved at CSP2 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
```

In above screen enter file name to download and then click ‘OK’ button to download that file and to get below output


An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification

```
angular.txt File received and saved at CSP1 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
angular.txt File received and saved at CSP2 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
file downloaded and saved inside angular.txt
```

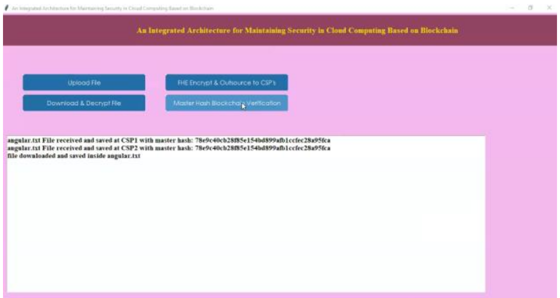
In above screen in blue colour text we can see file downloaded inside ‘CloudUser’ folder and we can see that file downloaded in decrypted format



Name	Date modified	Type
__pycache__	22-09-2023 12:23	File fol
angular	22-09-2023 13:22	Text Do
CustomButton	03-09-2021 18:11	PY File
Main	17-01-2022 15:18	PY File
private.pckl	17-01-2022 14:05	PCKL F
public.pckl	17-01-2022 14:05	PCKL F
run	10-03-2022 15:46	Windo

```
to solve cors error use below url in chrome to add extension then chnage from off
to on

https://chrome.google.com/webstore/detail/moesif-orign-cors-
changer/digfbfaphojjndkpccljibejjbppifbc?hl=en-US
Once installed, click it in your browser to activate the extension. Make sure the
icon's label goes from "off" enter image description here to "on"enter image
description here; Then refresh your application, and your API requests should now
work! The plugin definitely addresses the issue. However, this fix only applies to
your own machine. In local development, it's fine to have a plugin installed that
can help you get past the error.


C:\Python27\
C:\Python27\Scripts

set above python path for angular


https://dzone.com/articles/angular-5-material-design-login-application
https://www.angularjswiki.com/angular/angular-2-hello-world-example/


install npm install --save @angular/material @angular/cdk @angular/animations
npm install angular2-toaster
```

In above screen we can see file decrypted and now go back to application and then click on ‘Master Hash Blockchain Verification’ button to enter file and then get master has verification from Blockchain


An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain
Upload File
FHE Encrypt & Outsource to CSP's
Download & Decrypt File
Master Hash Blockchain Verification

```
angular.txt File received and saved at CSP1 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
angular.txt File received and saved at CSP2 with master hash: 78e9c40cb28f85e154bd899afb1ccfec28a95fca
file downloaded and saved inside angular.txt
```

In above screen enter filename for which verification has to done and then click on ‘OK’ button to get below output

V. CONCLUSION

This project revolutionizes data security in cloud computing through the integration of blockchain technology, fortifying data protection measures. It introduces an additional layer of defense to safeguard data integrity, ensuring that user information remains secure and unaltered. Immediate alerts notify users of any suspicious activities or alterations, instilling confidence in the system's vigilance and protection mechanisms.

Utilizing multiple cloud service providers (CSPs) enhances user flexibility, offering a diverse range of cloud services while maintaining robust data security protocols. Fully Homomorphic Encryption (FHE) enables computations on encrypted data without decryption[19], enhancing privacy and security. Each file is assigned a Master Hash, serving as a digital fingerprint for tamper-proof storage on the Blockchain, a decentralized and highly secure platform.

Integration with Ethereum[32] smart contracts ensures secure storage of file hash[33-37] codes, further bolstering data protection measures. Cost analysis of storing and accessing Master Hashes, considering Ethereum's GAS prices, ensures transparency and enables users to manage expenses efficiently. This project exemplifies the potential of blockchain[23-25] to reinforce cloud data security, laying the foundation for a future where cloud computing is safer and more reliable, addressing concerns surrounding data security and integrity comprehensively.

VI. FUTURE SCOPE

In the future, integrating blockchain technology with emerging technologies like artificial intelligence, machine learning, Internet of Things (IoT), and edge computing holds immense potential for advancing cloud computing capabilities. This synergy can unlock new avenues for delivering intelligent, responsive, and personalized services, revolutionizing the way data is processed, analyzed, and utilized. By harnessing the combined power of these technologies, cloud computing can evolve to meet the growing demands of a digitalized world, paving the way for innovative solutions and enhanced user experiences.

REFERENCES

[1]. V. Agarwal, A. K. Kaushal, and L. Chouhan, ‘‘A survey on cloud computing security issues and cryptographic techniques,’’ in Social Networking and Computational Intelligence. Singapore: Springer, 2020, pp. 119–134, doi: 10.1007/978-981-15-2071-6_10.

[2]. Cloud Security Alliance. (2017). Security Guidance V4.0. [Online]. Available: https://cloudsecurityalliance.org/download/security-guidance-v4/

[3]. CSA. (2020). Top Threats to Cloud Computing: Egregious Eleven. [Online]. Available: https://cloudsecurityalliance.org/artifacts/topthreatsto-cloud-computing-egregious-eleven/

[4]. R. Kissel, ‘‘Glossary of key information security terms,’’ Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 7298, 2013, Revision 2. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[5]. CSA. (2013). Practices for Secure Development of Cloud Applications. [Online]. Available: https://safecode.org/practices-for-securedevelopment-of-cloud-applications/

[6]. Cloud Security Alliance. (2016). Top Threats Research. [Online]. Available: https://cloudsecurityalliance.org/group/top-threats/

[7]. R. Kumar and R. Goyal, ‘‘On cloud security requirements, threats, vulnerabilities and countermeasures: A survey,’’ Comput. Sci. Rev., vol. 33, pp. 1–48, Aug. 2019.

[8]. N. Phaphoom, X. Wang, and P. Abrahamsson, ‘‘Foundations and technological landscape of cloud computing,’’ ISRN Softw. Eng., vol. 2013, pp. 1–31, Feb. 2013, doi: 10.1155/2013/782174.

[9]. B. Grobauer, T. Walloschek, and E. Stocker, ‘‘Understanding cloud computing vulnerabilities,’’ IEEE Secur. Privacy Mag., vol. 9, no. 2, pp. 50–57, Mar. 2011, doi: 10.1109/MSP.2010.115.

[10]. D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, ‘‘Security issues in cloud environments: A survey,’’ Int. J. Inf. Secur., vol. 13, no. 2, pp. 113–170, Apr. 2014, doi: 10.1007/s10207- 013-0208-7.

[11]. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, ‘‘A survey on security issues and solutions at different layers of cloud computing,’’ J. Supercomput., vol. 63, no. 2, pp. 561–592, Feb. 2013, doi: 10.1007/s11227-012-0831-5.

[12]. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, ‘‘NIST cloud computing reference architecture,’’ Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 500-292, 2011. [Online]. Available: https://ws680.nist.gov/publication/get_pdf.cfm_pub_id=909505

[13]. R. P. Madhubala, ‘‘Survey on security concerns in cloud computing,’’ in Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT), Oct. 2015, pp. 1458–1462.

[14]. L. Martin, ‘‘XTS: A mode of AES for encrypting hard disks,’’ IEEE Security Privacy Mag., vol. 8, no. 3, pp. 68–69, May 2010, doi: 10.1109/MSP. 2010.111.

[15]. H.-Y. Lin and W.-G. Tzeng, ‘‘A secure erasure code-based cloud storage system with secure data forwarding,’’ IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 995–1003, Jun. 2012, doi: 10.1109/TPDS.2011.252.

[16]. M. Ahmed, Q. H. Vu, R. Asal, H. Al Muhairi, and C. Y. Yeun, ‘‘Lightweight secure storage model with fault-tolerance in cloud environment,’’ Electron. Commerce Res., vol. 14, no. 3, pp. 271–291, Nov. 2014, doi: 10.1007/s10660-014-9140-9.

[17]. M. van Dijk, A. Juels, A. Oprea, R. L. Rivest, E. Stefanov, and N. Triandopoulos, ‘‘Hourglass schemes: How to prove that cloud files are encrypted,’’ in Proc. ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2012, pp. 265–280, doi: 10.1145/2382196.2382227.

[18]. S. Eletriby, E. M. Mohamed, and H. S. Abdelkader, ‘‘Modern encryption techniques for cloud computing randomness and performance testing,’’ in Proc. 3rd Int. Conf. Commun. Inf. Technol. (ICCIT), 2012, pp. 800–805.

[19]. S. Zaineldeen and A. Ate, ‘‘Review of cryptography in cloud computing,’’ Int. J. Comput. Sci. Mobile Comput., vol. 9, no. 3, pp. 211–220, Mar. 2020.

[20]. I. Mouhib, D. Ouadghiri, and N. Hassan, ‘‘Homomorphic encryption as a service for outsourced images in mobile cloud computing environment,’’ in Cryptography: Breakthroughs in Research and Practice. Hershey, PA, USA: IGI Global, 2020, pp. 316–330, doi: 10.4018/978-1-7998-1763- 5.ch019.

[21]. P. Awasthi, S. Mittal, S. Mukherjee, and T. Limbasiya, ‘‘A protected cloud computation algorithm using homomorphic encryption for preserving data integrity,’’ in Recent Findings in Intelligent Computing Techniques (Advances in Intelligent Systems and Computing). Singapore: Springer, 2019, p. 707, doi: 10.1007/978-981-10-8639-7_53.

[22]. A. Alanwar, Y. Shoukry, S. Chakraborty, P. Martin, P. Tabuada, and M. Srivastava, ‘‘PrOLoc: Resilient localization with private observers using partial homomorphic encryption,’’ in Proc. 16th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN), Apr. 2017, pp. 41–52, doi: 10.1145/3055031.3055080.

[23]. P. K. Sharma, M.-Y. Chen, and J. H. Park, ‘‘A software defined fog node based distributed blockchain cloud architecture for IoT,’’ IEEE Access, vol. 6, pp. 115–124, 2018, doi: 10.1109/ACCESS.2017.2757955.

[24]. K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, ‘‘Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 7992–8004, Oct. 2019, doi: 10.1109/JIOT.2019.2904303.

[25]. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, ‘‘ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,’’ in Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID), May 2017, pp. 468–477, doi: 10.1109/CCGRID.2017.8.

[26]. R. L. Rivest, L. Adleman, and M. L. Dertouzos, ‘‘On data banks and privacy homomorphisms,’’ Found. Secure Comput., vol. 4, no. 11, pp. 169–180, 1978.

[27]. S. Goldwasser and S. Micali, ‘‘Probabilistic encryption & amp; how to play mental poker keeping secret all partial information,’’ in Proc. 14th Annu. ACM Symp. Theory Comput., 1982, pp. 365–377.

[28]. P. Paillier, ‘‘Public-key cryptosystems based on composite degree residuosity classes,’’ in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 1999, pp. 223–238.

[29]. D. Boneh, E. Goh, and K. Nissim, ‘‘Evaluating 2-DNF formulas on ciphertexts,’’ in Theory Cryptography. Berlin, Germany: Springer, 2005, pp. 325–341, doi: 10.1007/978-3-540-30576-7_18.

[30]. C. Gentry, ‘‘A fully homomorphic encryption scheme,’’ Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009.

[31]. R. McLelland, G. Hurey, Y. Hackett, and D. Collins, ‘‘Agreements between cloud service providers and their clients: A review of contract terms,’’ in Proc. Arxius i Industries Culturals, Girona, Spain, 2014, p. 11.

[32]. W. W. Hargrove, F. M. Hoffman, and T. Sterling, ‘‘The do-it-yourself supercomputer,’’ Sci. Amer., vol. 285, no. 2, pp. 72–79, Aug. 2001.

[33]. E. Orsini, N. P. Smart, and F. Vercauteren, ‘‘Overdrive2k: Efficient secure MPC over Z k 2 from somewhat homomorphic encryption,’’ in Proc. Cryptographers’ Track RSA Conf. Cham, Switzerland: Springer, 2019, pp. 254–283.

[34]. A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, ‘‘A survey on homomorphic encryption schemes: Theory and implementation,’’ ACM Comput. Surv., vol. 51, no. 4, pp. 1–35, Sep. 2018.

[35]. T. S. Fun and A. Samsudin, ‘‘A survey of homomorphic encryption for outsourced big data computation,’’ KSII Trans. Internet Inf. Syst., vol. 10, no. 8, pp. 3826–3851, 2016.

[36]. N. Döttling, J. Müller-Quade, and A. C. Nascimento, ‘‘IND-CCA secure cryptography based on a variant of the LPN problem,’’ in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. Berlin, Germany: Springer, 2012, pp. 485–503.

[37]. M. Kandeeban and T. Nivetha, ‘‘Blockchain: A tool for a secure, safe and transparent way of food and agricultural supply chain,’’ Int. J. Farm Sci., vol. 9, no. 1, pp. 97–100, 2019.

[38]. K. Gai, K.-K. R. Choo, and L. Zhu, ‘‘Blockchain-enabled reengineering of cloud datacenters,’’ IEEE Cloud Comput., vol. 5, no. 6, pp. 21–25, Nov./Dec. 2018.

[39]. D. Yaga, P. Mell, N. Roby, and K. Scarfone, ‘‘Blockchain technology overview,’’ 2019, arXiv:1906.11078. [Online]. Available: http://arxiv. org/abs/1906.11078