JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 26 Issue 01, 2023 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

AN INTEGRATED ARCHITECTURE FOR MAINTAINING SECURITY IN CLOUD COMPUTING USING LIGHT COMPUTATION CHA - CHA ALGORITHM IN BLOCKCHAIN

K. Ramesh[1], Dr. A.P. Siva Kumar[2]

[1]PG-Scholar, Department of CSE (AI), JNTUACEA, Ananthapuramu, Andhra Pradesh, India

[2]Associate Professor, Department of CSE, JNTUACEA, Ananthapuramu, Andhra Pradesh, India

kattelaramesh762@gmail.com[1], sivakumar.cse@jntua.ac.in[2]

Abstract

In this paper, widespread availability, cloud services are an easy target for actors with malicious intentions. Cloud computing is a relatively new technology that falls under the umbrella of cloud services. Cloud computing presents a significant risk to the integrity of data if improper actions are taken with the data, as cloud services are an umbrella term for cloud computing. As a consequence of this, bad actors might gain an advantage by manipulating data. Customers of cloud computing services in a diverse array of industries are becoming increasingly concerned about the veracity of the information they store in the cloud. On the other hand, blockchain is a digital ledger that cannot be altered, and it has the potential to be utilized with cloud computing to produce a cloud service that cannot be hacked. The authors of this study propose a solution that combines blockchain technology with cloud computing as a means of assuring the confidentiality of all homomorphic encryption procedures. The proposed plan calls for the utilization of the Byzantine Fault Tolerance consensus in order to build a decentralized network of cloud service providers (CSPs) that are capable of processing data based on the requirements of individual customers. This will result in the elimination of the monopoly that the CSP has on the storage and management of data. Every CSP collaborates in order to arrive at a single, standardized hash value that can be stored in the shared database they all use. Blockchain networks, such as Bitcoin's and Ethereum's, keep a record of the values of their master hashes to ensure the production of data that is incorruptible. Keeping track of the address of the block header is the first step; next, obtain the master hash values for use in auditing functions. An in-depth theoretical analysis of the costs that have already been incurred in producing new master hash values for each cryptocurrency is presented here. Bitcoin's online performance is slower and more expensive than Ethereum's, whereas Ethereum leads to reduced client financial expenses due to its lower transaction fees. In addition, we detail the application of the suggested methodology, discuss the criteria for data security that it satisfies, and offer potential directions for further development. The suggested verification method uses a publicly available cryptocurrency as a backend service. It also does not require any special configuration from the user, other than the installation of a wallet for the desired cryptocurrency. Computing in the cloud, companies that provide cloud services (also known as CSPs), and blockchain are all examples of terms that can be used to describe this rapidly expanding industry.

Submitted: 13/01/2023 **Accepted**: 30/01/2023

Keywords: Cloud service providers (CSPs), Blockchain networks, Cloud computing, Concrete Hash Algorithm (CHA), Cloud Security Alliance (CSA).

I. INTRODUCTION

When attempting to define data security [1-2], it is common practise to focus on the potential threats to data safety. Computing in the cloud, like any other area of the technology industry, is susceptible to a wide variety of potential dangers [3]. The primary contributor is the fact that cloud computing makes use of a diverse set of technologies, [4-7] all of which collaborate with one another to achieve the desired results. When conducting a pros and cons analysis of cloud computing security issues, risk management is one of the most important components to include [5]. The Cloud Security Alliance, also referred to as CSA, is an organization that does not operate for the purpose of making a profit. Instead, it is committed to ensuring that the cloud computing industry as a whole is secure. [4-5] The Cloud Security Alliance (CSA) has outlined critical responsibilities that cloud service providers (CSPs) and the end users of cloud computing are expected to fulfil in order to mitigate the inherent risks that are associated with cloud computing. It is the responsibility of the CSP to document, design, and implement both the client's security controls as well as the organization's own internal controls. [6] This is all part of the CSP's job description. During both the phase of planning and the phase of actually carrying out the project, the Consensus Assessments Initiative Questionnaire is utilised (CAIQ) [6-8]. Cloud Control Matrix, or CCM for short, is a tool that users of cloud computing services can employ to keep track of the roles and responsibilities of the individuals responsible for the enforcement of various security measures. CCM is an abbreviation for the Cloud Control Matrix [8]. A high-level process model for cloud security management has also been established in order to accommodate the substantial variations in the process model that are anticipated to arise during the process of developing a cloud project. [9] This model was created in order to accommodate substantial variations in the process model that are anticipated to arise during the process of developing a cloud project. These differences are anticipated to be quite significant [10]. In order to determine what is required, organise the architecture, and fill in any gaps, it is absolutely necessary to have a solid understanding of the capabilities offered by the underlying cloud platform.

II. LITERATURE REVIEW

[1] V. Agarwal, A. K. Kaushal, and L. Chouhan, (2020), ‘‘A survey on cloud computing security issues and cryptographic techniques,’’. Cloud computing is an Internet-based computing model, having various resources used by distinct users in a concurrent manner. Apart from all of its advantages, it faces a major setback due to various data security issues. To overcome these issues, various security mechanisms have been proposed, such as cryptography and authentication. Cryptography can be used to provide data integrity, authorization for data manipulation, and also making the data unreadable to an interceptor through encryption. There are various classifications of models in cloud computing. The service models are classified as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). There are several deployment models mainly distinguished by ownership which

consists of public cloud, private cloud, and hybrid cloud. This survey mainly focuses on security issues in cloud service models and cloud deployment models along with various cryptographic mechanisms of data protection, such as symmetric key cryptography, asymmetric key cryptography, and their encryption algorithms.

[2] Cloud Security Alliance. (2017). "Security Guidance V4.0". Cloud computing offers tremendous potential benefits in agility, resiliency, economy as well as security. However, the security benefits only appear if you understand and adopt cloud-native models and adjust your architectures and controls to align with the features and capabilities of cloud platforms. The cloud security best practices outlined in the Security Guidance for Critical Areas of Focus in Cloud Computing 4.0 were crowd-sourced by Cloud Security Alliance's community of security experts and can help you implement and adopt a cloud-native approach. While the implementation details vary greatly depending on the specific cloud project, there is a relatively straightforward, high-level process for managing cloud security.

[3] CSA. (2020). "Top Threats to Cloud Computing: Egregious Eleven". The Cloud Security Alliance (CSA) Egregious 11 is similar to the OWASP Top Ten for Web Applications. Regularly, the organization releases a detailed "Top Threats to Cloud Computing" report to raise awareness of the most critical cloud security issues and promote strong security practices. An interesting trend in this fourth edition is that traditional cloud security issues directly under the control of the cloud service provider (CSP), e.g., denial of service and shared technology vulnerabilities, are absent. This reflects a trend where security concerns are higher up the tech stack, more toward those business applications deployed on CSP infrastructure and the services and APIs that power them.

[4] R. Kissel, (2019). ''Glossary of key information security terms,''. The National Institute of Standards and Technology (NIST) has received numerous requests to provide a summary glossary for our publications and other relevant sources, and to make the glossary available to practitioners. As a result of these requests, this glossary of common security terms has been extracted from NIST Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, NIST Interagency Reports (NISTIRs), and from the Committee for National Security Systems Instruction 4009 (CNSSI-4009). This glossary includes most of the terms in the NIST publications. It also contains nearly all of the terms and definitions from CNSSI-4009. This glossary provides a central resource of terms and definitions most commonly used in NIST information security publications and in CNSS information assurance publications. For a given term, we do not include all definitions in NIST documents – especially not from the older NIST publications. Since draft documents are not stable, we do not refer to terms/definitions in them.

III. METHODOLOGY

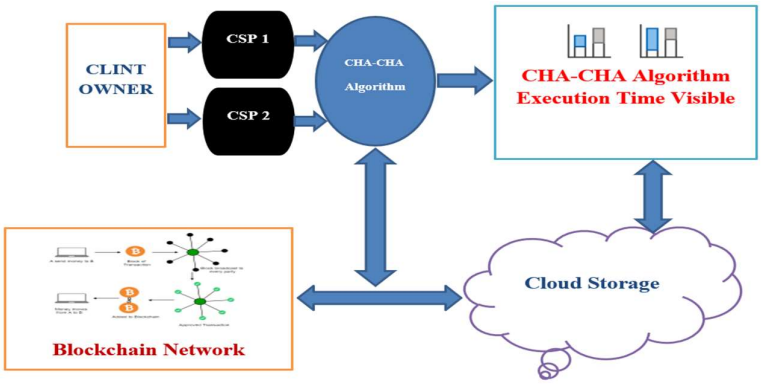

Figure 1: Proposed System Architecture

Blockchain

Definition: Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An *asset* can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

- **Importance:**

Business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

- **Benefits of blockchain:**

Operations often waste effort on duplicate record keeping and third-party validations. Record-keeping systems can be vulnerable to fraud and cyberattacks. Limited transparency can slow data verification. And with the arrival of IoT, transaction volumes have exploded. All of this slows business, drains the bottom line — and means we need a better way. Enter blockchain.

- **Greater trust:**

With blockchain, as a member of a members-only network, you can rest assured that you are receiving accurate and timely data, and that your confidential blockchain records will be shared only with network members to whom you have specifically granted access.

- **Greater security:**

Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.

- **More efficiencies:**

With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated. And to speed transactions, a set of rules called a smart contract can be stored on the blockchain and executed automatically.

Cloud Computing Security Architecture:

Security in cloud computing is a major concern. Proxy and brokerage services should be employed to restrict a client from accessing the shared data directly. Data in the cloud should be stored in encrypted form.

Security Planning

Before deploying a particular resource to the cloud, one should need to analyze several aspects of the resource, such as:

- ✓ A select resource needs to move to the cloud and analyze its sensitivity to risk.
- ✓ Consider cloud service models such as IaaS, PaaS,and These models require the customer to be responsible for Security at different service levels.
- ✓ Consider the cloud type, such as public, private, community, or
- ✓ Understand the cloud service provider's system regarding data storage and its transfer into and out of the cloud.
- ✓ The risk in cloud deployment mainly depends upon the service models and cloud types.

Understanding Security of Cloud

Security Boundaries:

The Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate. A particular service model defines the boundary between the service provider's responsibilities and the customer. The following diagram shows the CSA stack model:

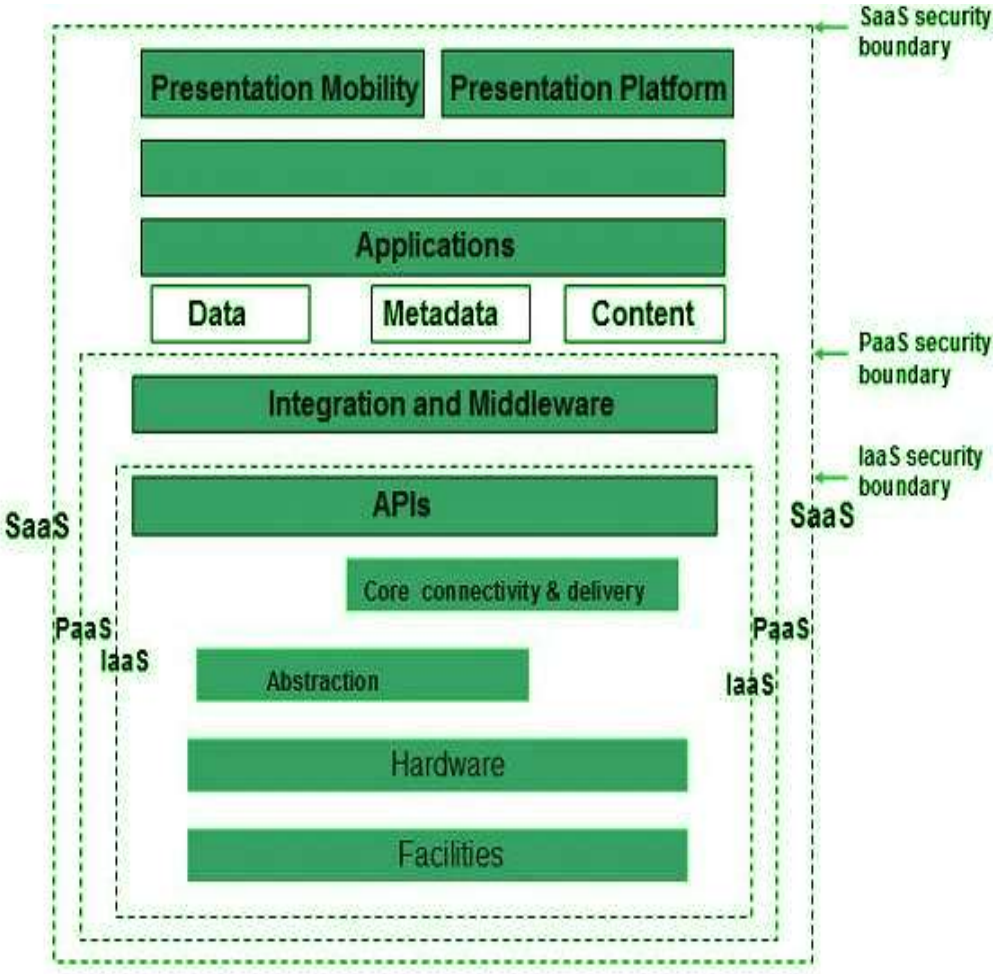

Figure 2: CSA stack model

Key Points to CSA Model:

- ✓ IaaS is the most basic level of service, with PaaS and SaaS next two above levels of services.
- ✓ Moving upwards, each service inherits the capabilities and security concerns of the model beneath.
- ✓ IaaS provides the infrastructure, PaaS provides the platform development environment, and SaaS provides the operating environment.
- ✓ IaaS has the lowest integrated functionality and security level, while SaaS has the highest.
- ✓ This model describes the security boundaries at which cloud service providers' responsibilities end and customers' responsibilities begin.
- ✓ Any protection mechanism below the security limit must be built into the system and maintained by the customer.

Although each service model has a security mechanism, security requirements also depend on where these services are located, private, public, hybrid, or community cloud.

Understanding data security:

Since all data is transferred using the Internet, data security in the cloud is a major concern. Here are the key mechanisms to protect the data.

- access control
- audit trail
- certification
- authority

The service model should include security mechanisms working in all of the above areas.

Principles of Cloud Security Architecture

A well-designed cloud security architecture should be based on the following key principles:

- ✓ **Identification**: Knowledge of the users, assets, business environment, policies, vulnerabilities and threats, and risk management strategies (business and supply chain) that exist within your cloud environment.
- ✓ **Security Controls**: Defines parameters and policies implemented across users, data, and infrastructure to help manage the overall security posture.
- ✓ **Security by Design**: Defines the control responsibilities, security configurations, and security baseline automations. Usually standardized and repeatable for deployment across common use cases, with security standards, and in audit requirements.
- ✓ **Compliance**: Integrates industry standards and regulatory components into the architecture and ensures standards and regulatory responsibilities are met.
- ✓ **Perimeter Security**: Protects and secures traffic in and out of organization's cloud-based resources, including connection points between corporate network and public internet.
- ✓ **Segmentation**: Partitions the architecture into isolated component sections to prevent lateral movement in the case of a breach. Often includes principles of 'least privilege'.
- ✓ **User Identity and Access Management**: Ensures understanding, visibility, and control into all users (people, devices, and systems) that access corporate assets. Enables enforcement of access, permissions, and protocols.
- ✓ **Data encryption**: Ensures data at rest and traveling between internal and external cloud connection points is encrypted to minimize breach impact.
- ✓ **Automation**: Facilitates rapid security and configuration provisioning and updates as well as quick threat detection.
- ✓ **Logging and Monitoring**: Captures activities and constant observation (often automated) of all activity on connected systems and cloud-based services to ensure compliance, visibility into operations, and awareness of threats.
- ✓ **Visibility**: Incorporates tools and processes to maintain visibility across an organization's multiple cloud deployments.
- ✓ **Flexible Design**: Ensuring architecture design is sufficiently agile to develop and incorporate new components and solutions without sacrificing inherent security.

CHA-CHA ALGORITHM:

Daniel J. Bernstein is responsible for the development of the stream cyphers Salsa20 and Cha-cha, which are closely related to one another. Bernstein initially proposed the Salsa20 cypher in 2005, and then in later years he sent it to be validated cryptographically through the

eSTREAM process that was used by the European Union. Salsa20, which was first released in 2008, has been modified to become Cha-cha. It makes use of a new round function that improves diffusion while simultaneously boosting performance on certain architectures. [4] Both cyphers are constructed using a pseudorandom function that is based on add-rotate-XOR (ARX) operations. These are operations that involve bitwise addition (XOR), 32-bit addition, and rotation. A 256-bit key, a 64-bit nonce, and a 64-bit counter are mapped by the core function to a 512-bit block of the key stream (a Salsa version with a 128-bit key also exists). This provides Salsa20 and Cha-cha with an unusual advantage in that the user is able to seek to any position in the key stream efficiently and in the same amount of time as the original key stream. On contemporary x86 processors, the software performance of Salsa20 is between 4 and 14 cycles per byte, and the hardware performance is satisfactory. [5] It is not protected by a patent, and Bernstein has written several implementations that are available in the public domain and are optimized for typical architectures.

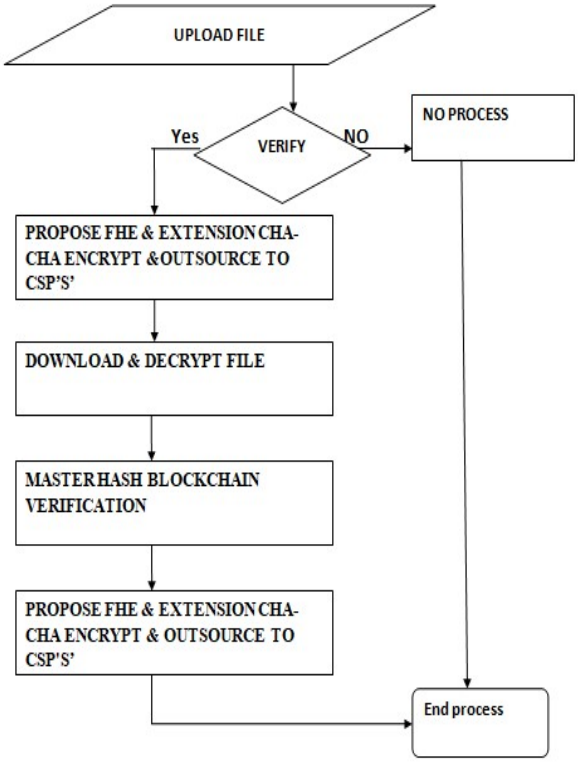

Figure 3: Flowchart

IV. RESULTS AND DISCUSSIONS

Using the ideas of BFT and blockchain technology, this paper proposes a verification scheme to address these issues. Data for multiple clients will be stored and processed by using multiple CSPs. It is required that every CSP periodically calculate a master hash value of their database to be recorded on a public blockchain like Bitcoin or Ethereum. There is no requirement for coordination or dialogue between these CSPs. When a client wants to know if data has been

altered, they can check for it by comparing the master hash values. Both confidentiality (HE will be used for encryption) and integrity (data modifications by the CSPs can be detected by comparing master hash values stored on the blockchain) requirements are met by this distributed verification system.

Advantages of proposed system:

- These CSPs do not need to collaborate or communicate with one another.
- CSPs can be detected by comparing master hash values stored on the blockchain.

Requirements:

- SOFTWARE REQUIREMENTS
- The functional requirements or the overall description documents include the product perspective and features, operating system and operating environment, graphics requirements, design constraints and user documentation.
- The appropriation of requirements and implementation constraints gives the general overview of the project in regard to what the areas of strength and deficit are and how to tackle them.
- Python idel 3.7 version (or)
- Anaconda 3.7 (or)
- Jupiter (or) Google colab

HARDWARE REQUIREMENTS

- Minimum hardware requirements are very dependent on the particular software being developed by a given Enthought Python / Canopy / VS Code user. Applications that need to store large arrays/objects in memory will require more RAM, whereas applications that need to perform numerous calculations or tasks more quickly will require a faster processor.
- **Operating system : windows, linux**
- **Processor : minimum intel i3**
- **Ram : minimum 4 gb**
- **Hard disk : minimum 250gb**

Executed Outputs

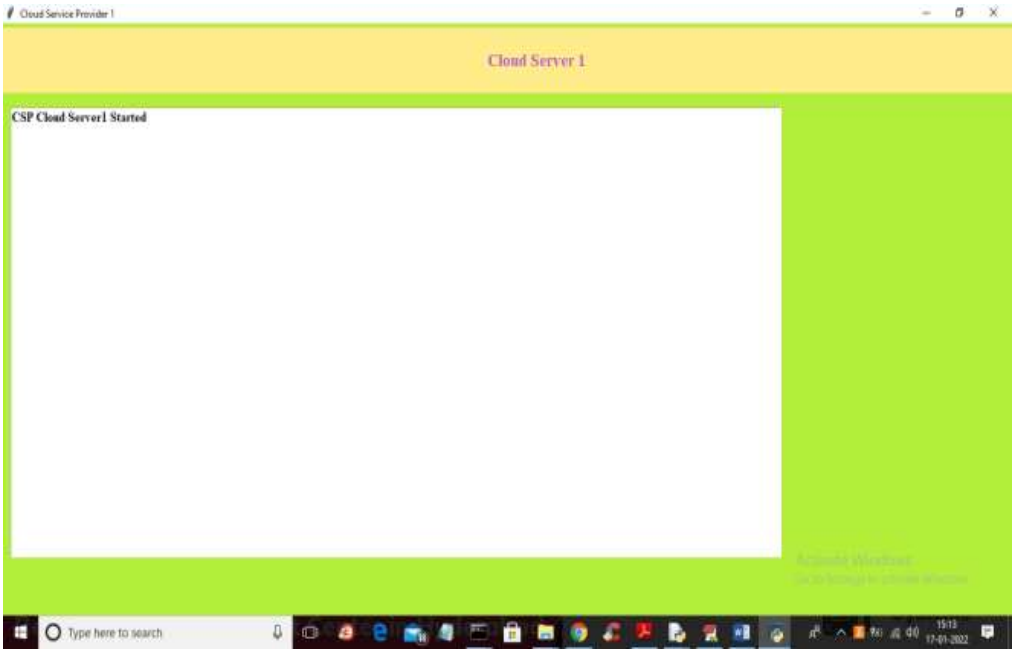

Figure 4: CSP1

CSP cloud server1 started software dashboard opened.

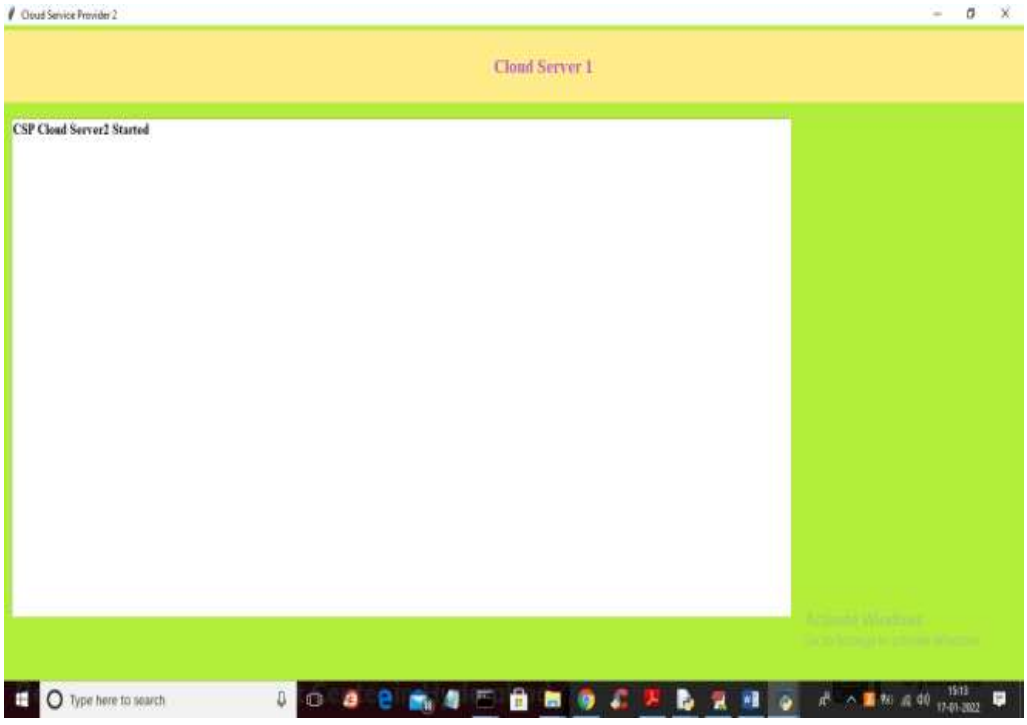

Figure 5: CSP2

CSP cloud server2 started software dashboard opened.

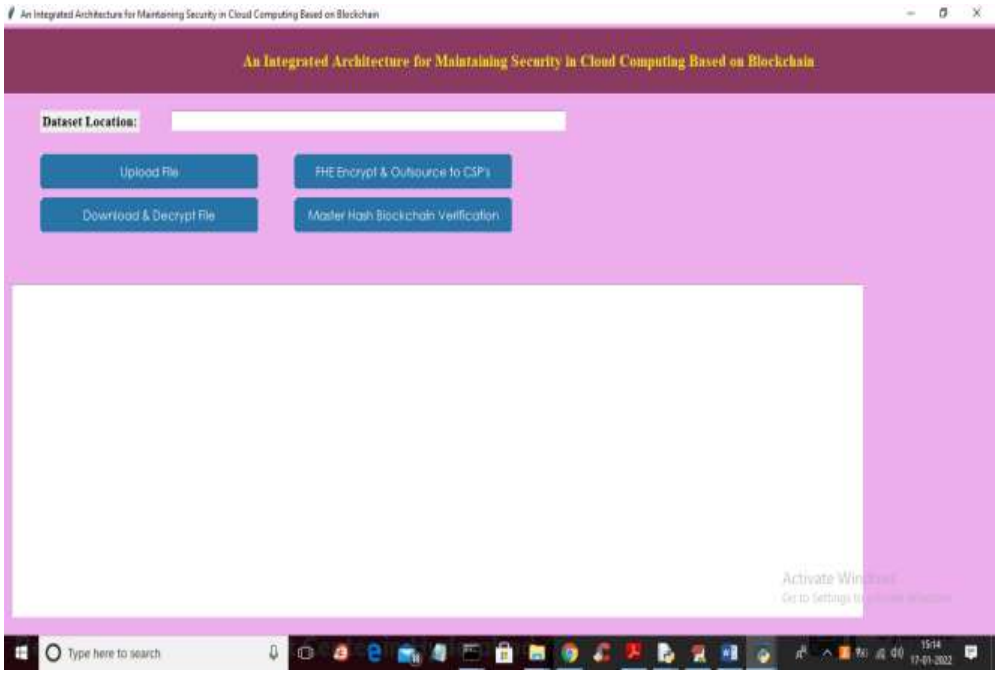

Figure 6: Home screen

An integrated architecture for maintaining security in cloud computing based on black chain in put dashboard open.

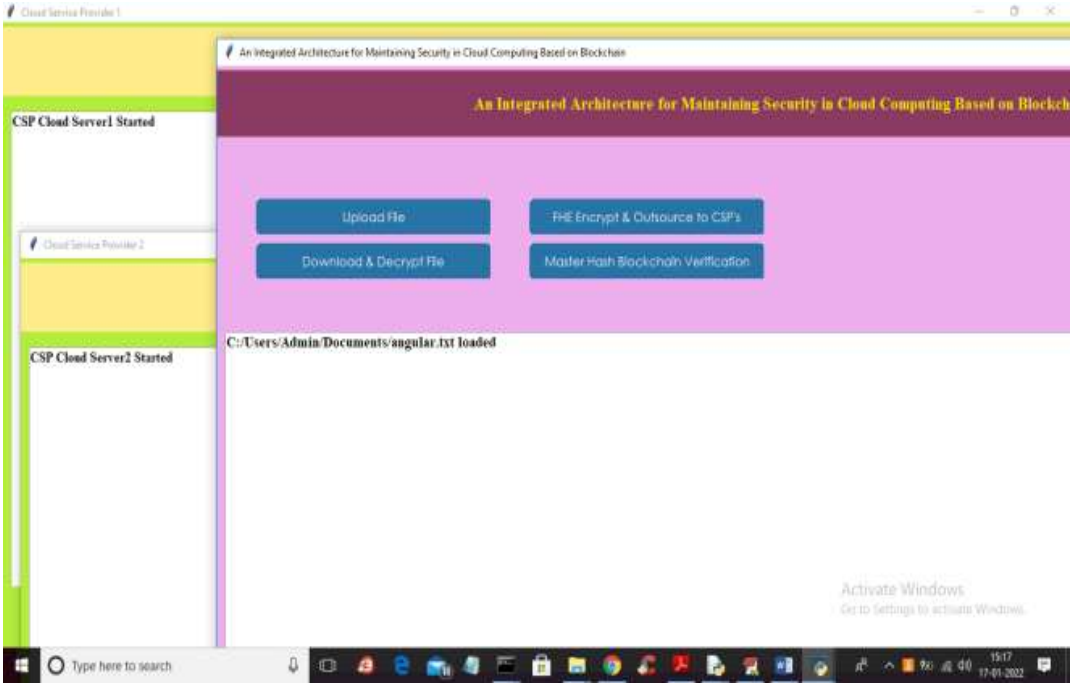

Figure 7: Upload file

An integrated architecture for maintaining security in cloud computing based on black chain in put dashboard open and upload a new input file.

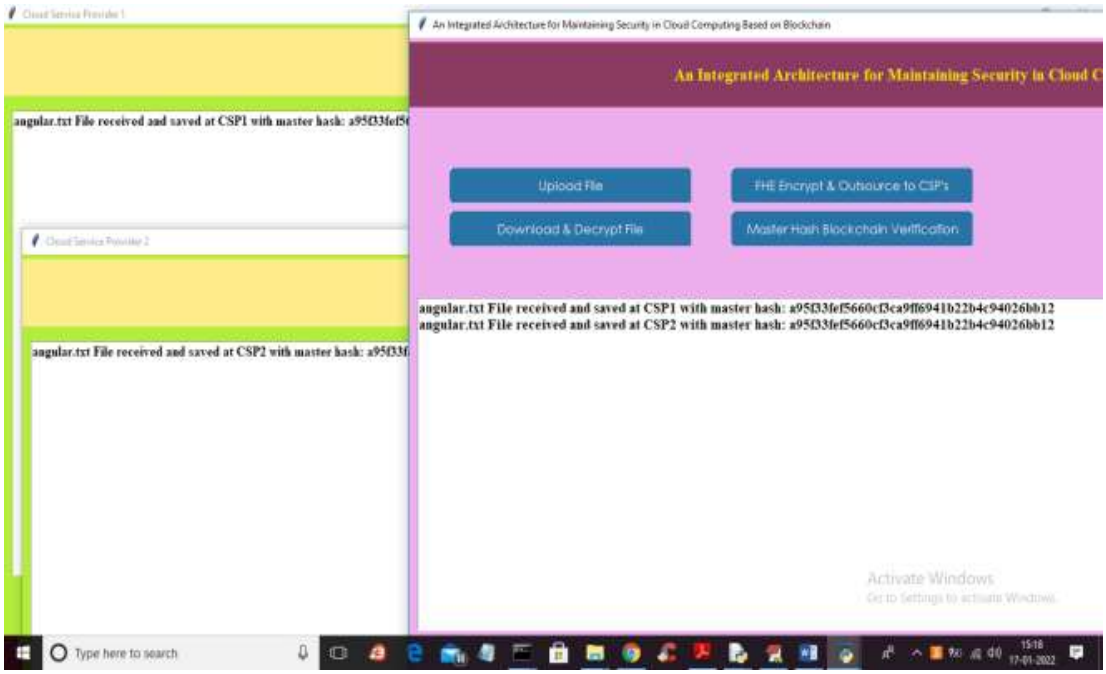

Figure 8: FHE encrypt & outsource to CSPs

An integrated architecture for maintaining security in cloud computing based on black chain in put dashboard open and upload a new input file and file share in securely in CSP1 & CSP2 as shown in figure 8.

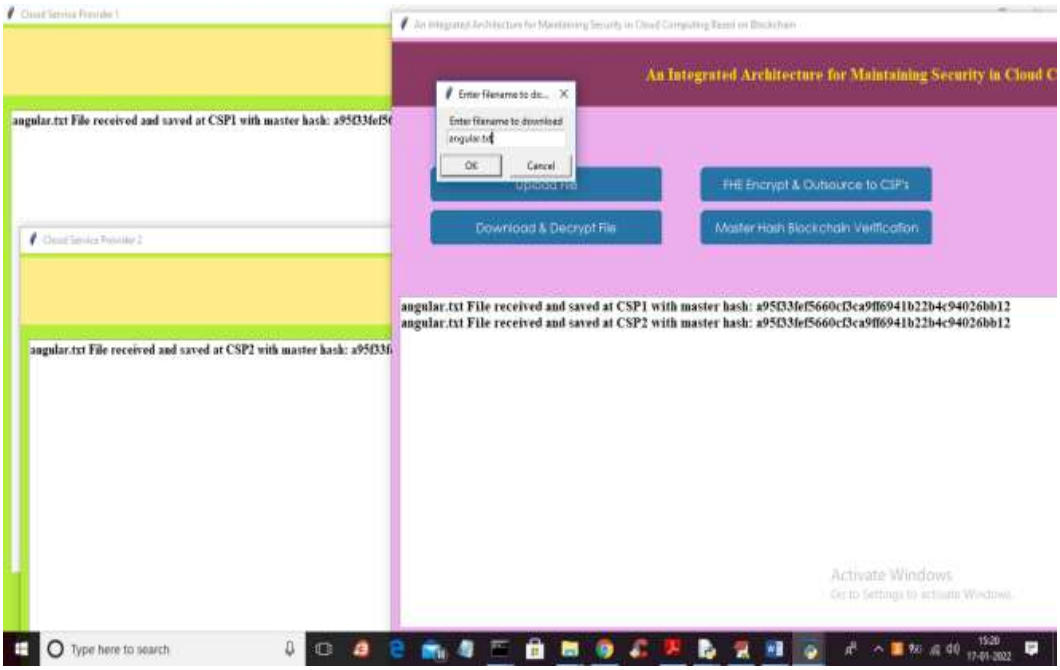

Figure 9: Download & decrypt file

An integrated architecture for maintaining security in cloud computing based on black chain in put dashboard open and upload a new input file and file share in securely in CSP1 & CSP2 and saved as shown in figure 9.

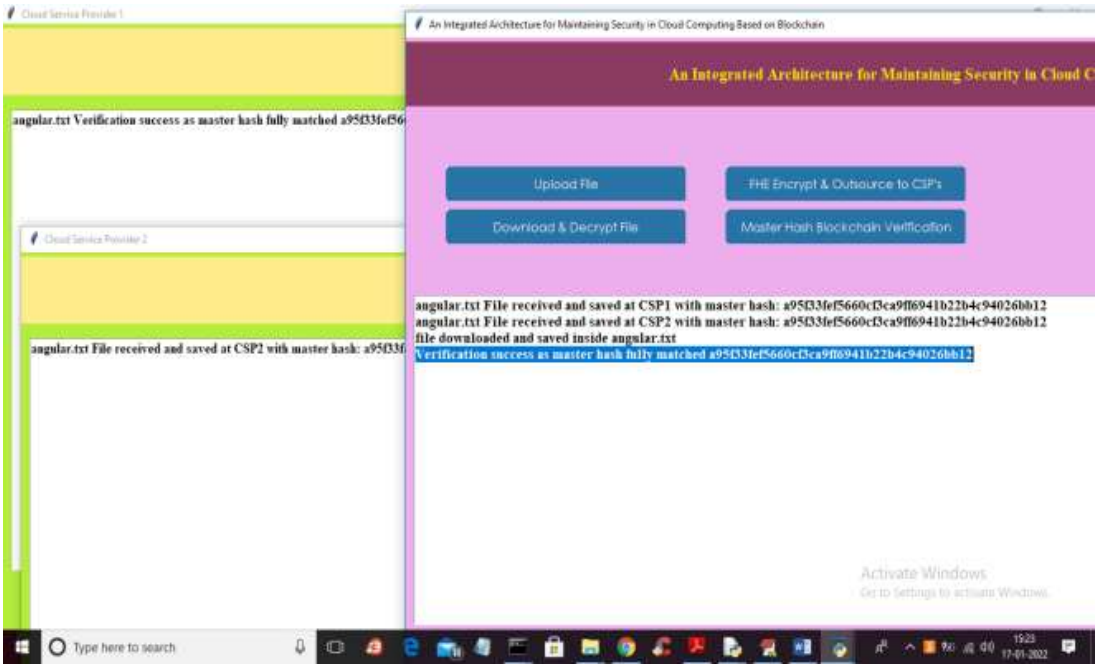

Figure 10: Master Hash Blockchain Verification

An integrated architecture for maintaining security in cloud computing based on black chain in put dashboard open and upload a new input file and file share in securely in CSP1 & CSP2 and saved and run as shown in figure 10.

EXTENSION RESULTS:

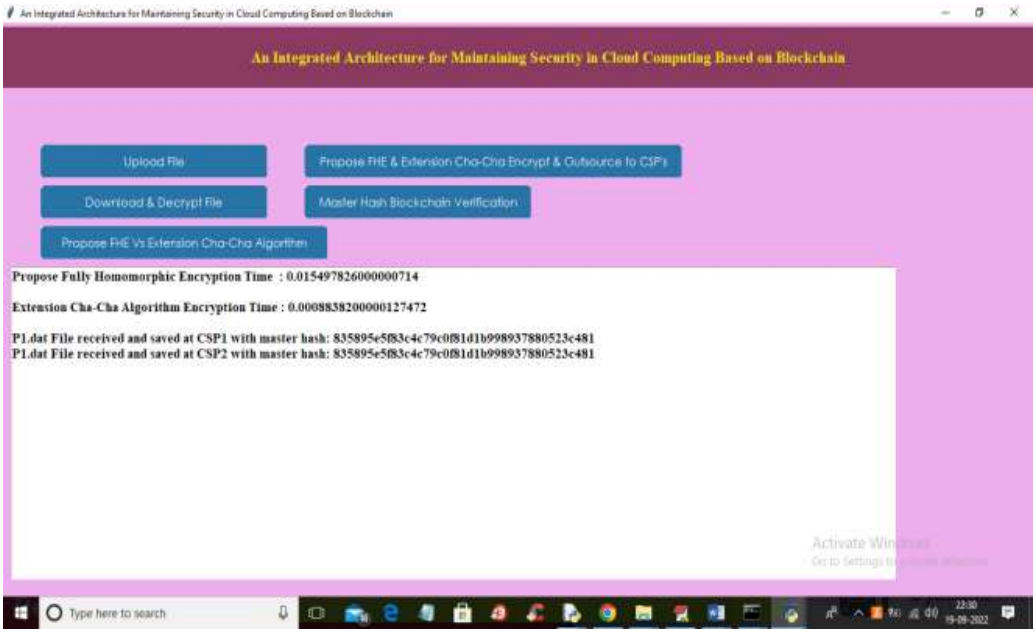

Figure 11: Propose FHE & Extension Cha-Cha Encrypt & Outsource to CSP's'

An integrated architecture for maintaining security in cloud computing based on black chain in put dashboard open and upload a new input file and file share in securely in CSP1 & CSP2 and saved and run and finally send data from one cloud to another cloud as shown in figure 11.

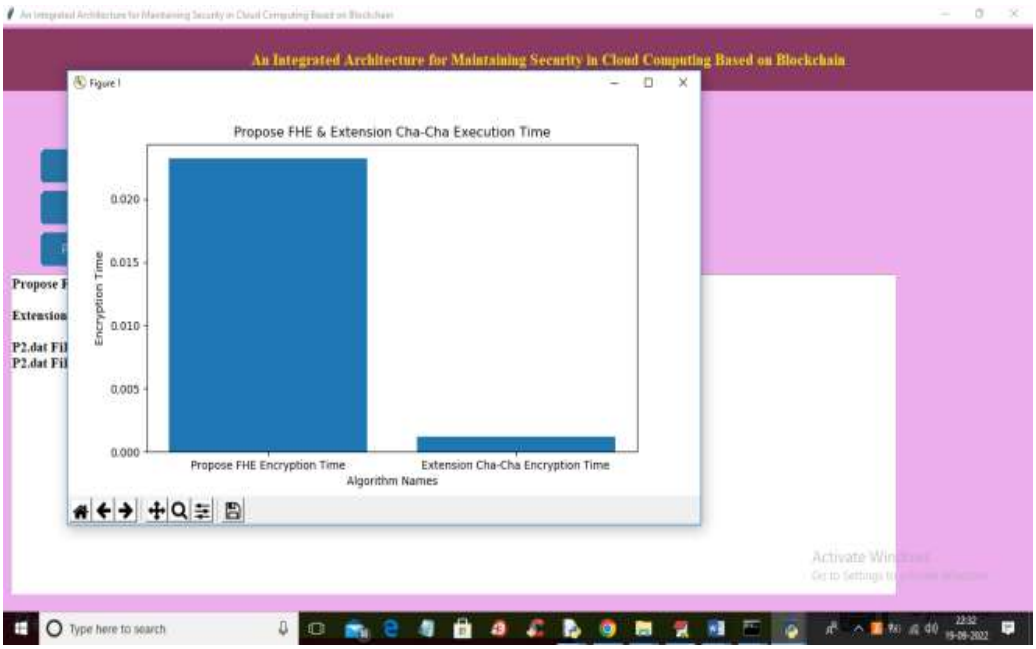

Figure 12: Propose FHE Vs Extension Cha-Cha Algorithm

An integrated architecture for maintaining security in cloud computing based on black chain in put dashboard open and upload a new input file and file share in securely in CSP1 & CSP2 and saved and run & finally send data from one cloud to another cloud propose FHE Vs Extension Cha-Cha Algorithm execution time visible,
as shown in figure 12.

V. CONCLUSIONS

This article addresses the problem of data breaches in cloud computing as well as the all-encompassing authority that cloud service providers have over the data operations of their customers. We recommend an approach that will improve the client's capability to keep their data secure. Keeping data private and secure during computations that are outsourced is the goal of the scheme that has been proposed, which makes use of homomorphic encryption. A novel approach that is based on a distributed network of cloud service providers and Byzantine Fault Tolerance consensus has been introduced in order to ensure the integrity of the data and detect any data tampering that may have been performed by the cloud service provider themselves. Under the plan that has been proposed, there is no requirement for direct communication to take place between the various cloud service providers. Cloud service providers are required to calculate the master hash values of their databases and store them in blockchain networks, such as Bitcoin or Ethereum, in order to provide their customers with immutable verification data. This is done to ensure that the customer receives accurate information. We provided a quantitative analysis of overhead costs based on a number of different time options to accommodate the varied needs of our customers.

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/top-threatsto-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.