An Integrated Architecture For Maintaining Security In Cloud Computing Based On Blockchain

Mrs. Sunitha Surarapu[1]*, Mrs. Srilatha Puli[2], P. Vasavi[3], V. Sravani[4], V. Sreekoumudi[5], E. Laxmi Narasimha[6], B.Shivudu[7]

[1]*Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. sunithasurarapu@sreyas.ac.in
[2]Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. srilatha.puli@sreyas.ac.in
[3]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. vasavivasu092@gmail.com
[4]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. sravaniscorpio@gmail.com
[5]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. vootukurisreekoumudivsk@gmail.com
[6]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. .laxminarasimha2805@gmail.com
[7]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. shivudubolle@gmail.com

***Corresponding Author: -** Mrs. Sunitha Surarapu
[1]*Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India, E-mail:- sunithasurarapu@sreyas.ac.in

Abstract:
Cloud services are vulnerable to assaults because of their widespread availability. Since cloud computing is still a relatively new service, there is a real risk that sensitive information might be altered while in transit. Because of this, bad actors may gain an edge by manipulating data. Clients using the cloud for a wide range of use cases want to know that their data is reliable and secure. Blockchain, on the other hand, is an immutable digital ledger that may be used with cloud computing to provide an immutable cloud-based data storage and processing system. In this work, we present a method that integrates blockchain technology with cloud computing to guarantee the security of data encrypted using any homomorphic encryption method. The suggested technique uses a distributed network of processing CSPs determined by client needs to circumvent the CSP's ultimate jurisdiction over the data. All CSPs work together to calculate a single, unified hash value for use in their shared database. Bitcoin and Ethereum blockchain networks keep track of master hash values to guarantee the production of immutable data.

Keywords – Blockchain, cloud computing, data integrity, homomorphic encryption.

1. INTRODUCTION

Data security risks are a common way to define data security. Cloud computing, like any other industry, is vulnerable to a wide range of dangers. The main cause of this is the fact that cloud computing makes use of a wide variety of technologies. Cloud computing is a not-for-profit organisation whose only mission is to enforce universal security, making risk management a crucial part of the equation. To reduce the risks connected with cloud computing, the Cloud Security Alliance (CSA) has outlined fundamental shared obligations for cloud service providers (CSPs) and the customers. The CSP's duties include documenting, designing, and implementing both the client's security controls and the business's own internal controls. A programme called is used throughout development and rollout to record the identities of those tasked with enforcing certain rules and the procedures they follow. It has also been designed to accommodate the many possible process model changes that would be necessary to complete a cloud-based project. Understanding the capabilities of the underlying cloud platform is essential for determining what is needed, organising the architecture, and filling in any gaps.

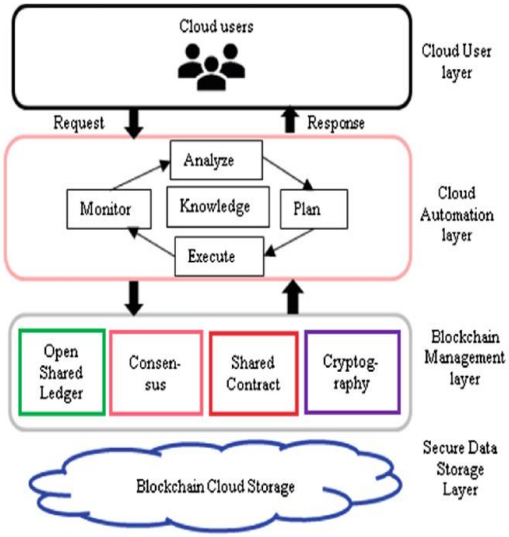

Fig.1: Example figure

Despite the CSP's attempts to establish a strong security base, such arrangements are rarely substantive from the dataowners' perspective, especially when it comes to trusting the CSP itself. This is compounded by the fact that the growth of cloud computing technology leads to new security vulnerabilities and amplifies existing ones. A recent CSA survey [3] compiled the most significant security issues within cloud computing, classifying the top 11 threats into 14 security domains which can be divided into either the governance or operational domains. The governance domain focuses on strategic and policy issues within a cloud computing environment, whereas the operational domain focuses on tactical security concerns.

Data breaches is at the forefront of threat ranking trend analyses conducted by CSA through 2011, 2016, and 2020 [3], [5], [6]. If such security breaches occur, it would seriously undermine the validity and trust of a cloud-based service. A data breach is an event where an unauthorised entity releases, analyses, steals or uses essential, safe or confidential information. A data breach can either be the primary purpose of a targeted attack or a result of human error, implementation vulnerabilities or inadequate security procedures. The leak of any information not meant for public access is considered a data breach. [7] noted that either encryption and keys vulnerabilities or data storage cryptography vulnerabilities could lead to data breaches. More explicitly, the absence of appropriate encryption algorithms and a poor key management mechanism can contribute to encryption, and key-related failures that directly impact data confidentiality and completeness [8]. Weak key management, defective, insecure, and outdated encryption methods allow data storage to be susceptible to threats [9], [10]. This has been further supported in [11] which highlighted that weak encryption techniques contribute to the most significant risk.

2. LITERATURE REVIEW

A survey on cloud computing security issues and cryptographic techniques:

Today, cloud computing is an emerging way of computing in computer science. Cloud computing is a set of resources and services that are offered by the network or internet. Cloud computing extends various computing techniques like grid computing, distributed computing. Today cloud computing is used in both industrial field and academic field. Cloud facilitates its users by providing virtual resources via internet. As the field of cloud computing is spreading the new techniques are developing. This increase in cloud computing environment also increases security challenges for cloud developers. Users of cloud save their data in the cloud hence the lack of security in cloud can lose the user's trust. In this paper we will discuss some of the cloud security issues in various aspects like multi-tenancy, elasticity, availability etc. the paper also discuss existing security techniques and approaches for a secure cloud. This paper will enable researchers and professionals to know about different security threats and models and tools proposed.

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. Each entry in the glossary points to one or more source NIST publications, and/or CNSSI-4009, and/or supplemental

sources where appropriate. The NIST publications referenced are the most recent versions of those publications (as of the date of this document).

On cloud security requirements, threats, vulnerabilities and countermeasures: A survey:
The world is witnessing a phenomenal growth in the cloud enabled services and is expected to grow further with the improved technological innovations. However, the associated security and privacy challenges inhibit its widespread adoption, and therefore require further exploration. Researchers from academia, industry, and standards organizations have provided potential solutions to these challenges in the previously published studies. The narrative review presented in this survey, however, provides an integrationist end-to-end mapping of cloud security requirements, identified threats, known vulnerabilities, and recommended countermeasures, which seems to be not presented before at one place. Additionally, this study contributes towards identifying a unified taxonomy for security requirements, threats, vulnerabilities and countermeasures to carry out the proposed end-to-end mapping. Further, it highlights security challenges in other related areas like trust based security models, cloud-enabled applications of Big Data, Internet of Things (IoT), Software Defined Network (SDN) and Network Function Virtualization (NFV).

Foundations and technological landscape of cloud computing:
The cloud computing paradigm has brought the benefits of utility computing to a global scale. It has gained paramount attention in recent years. Companies are seriously considering to adopt this new paradigm and expecting to receive significant benefits. In fact, the concept of cloud computing is not a revolution in terms of technology; it has been established based on the solid ground of virtualization, distributed system, and web services. To comprehend cloud computing, its foundations and technological landscape need to be adequately understood. This paper provides a comprehensive review on the building blocks of cloud computing and relevant technological aspects. It focuses on four key areas including architecture, virtualization, data management, and security issues.

Understanding cloud computing vulnerabilities:
The current discourse about cloud computing security issues makes a well-founded assessment of cloud computing's security impact difficult for two primary reasons. First, as is true for many discussions about risk, basic vocabulary such as "risk," "threat," and "vulnerability" are often used as if they were interchangeable, without regard to their respective definitions. Second, not every issue that's raised is really specific to cloud computing. We can achieve an accurate understanding of the security issue "delta" that cloud computing really adds by analyzing how cloud computing influences each risk factor. One important factor concerns vulnerabilities: cloud computing makes certain well-understood vulnerabilities more significant and adds new vulnerabilities. Here, the authors define four indicators of cloud-specific vulnerabilities, introduce a security-specific cloud reference architecture, and provide examples of cloud-specific vulnerabilities for each architectural component.

3.METHODOLOGY

Method, HE by alone is insufficient to meet the anti-tampering security requirements of IND-CCA2. As a result, there is the possibility of data loss or unreported changes to the database due to administrative errors. Blockchain (BC) technology is now the only viable option for using decentralisation and improving the transparency of manipulation of homomorphically encrypted data. BC has been used by a number of studies to reorganise the cloud in order to address a variety of security concerns. However, they have a difficult configuration setup and the embedding is expensive and time-consuming.

The flaws in the current system:

- First, it has the potential to lead to database corruption or loss of information.
- They have a difficult time getting set up and embedded, which takes a lot of time and money.

To address these issues, this study proposes a verification system built on the concepts of Client data will be stored and processed by many CSPs. Databases like Bitcoin and Ethereum will need regular computation from each CSP. There is no need for coordination or dialogue between these CSPs. Clients may check for evidence of data manipulation by comparing the original and new master hash values. Due to the ability to compare master hash values maintained on the blockchain, this distributed verification method satisfies the criteria of.

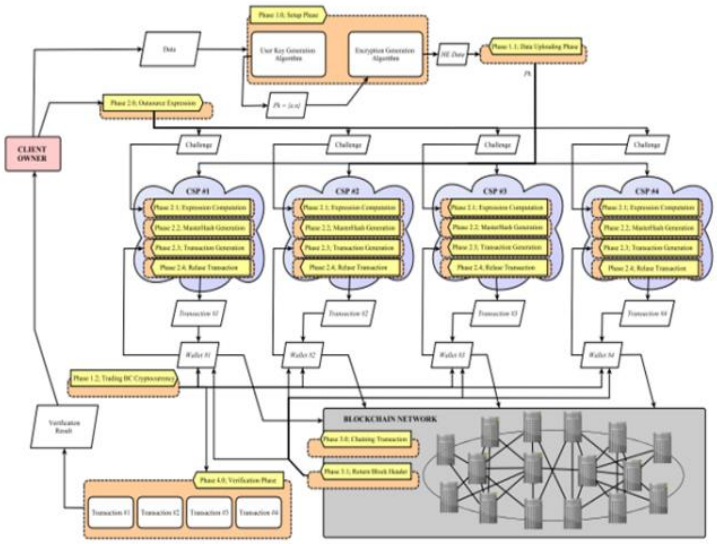

Fig.5.1.1 System architecture

Fig.2: System architecture

Specifically, we have developed the following modules for this project's implementation:
CSP1 is a fake cloud server that stores encrypted data in cloud storage and sends the Master Hash to the Blockchain.
Second, CSP2 is a fictitious cloud server that stores encrypted files in the cloud and sends their master hashes and filenames to the blockchain.

Thirdly, we have the Cloud User, who can upload any file to the cloud, have it encrypted using FHE, have the Master Hash produced, have the encrypted file outsourced to many CSPs, and then get the file and verify it whenever they want. However, Blockchain does cost money, thus the author is also analysing the costs associated with storing and accessing master hashes on the cloud. Below is an example of a screen demonstrating the default GAS values offered by ethereum for educational purposes and how they may be used to store a file's hash code.

4. IMPLEMENTATION

In order to save money and take advantage of more computing power and storage capacity, businesses of all sizes are turning to cloud services. However, this shift has created a new set of security concerns, as cloud users' data is now housed on servers outside of their control. To solve this issue, encryption was introduced, which would encrypt data before it was sent to the cloud; however, cloud internal employees or attackers could gain access to decryption keys by monitoring them, and there is no way to notify the user that his data had been modified on the cloud server.

To address the aforementioned issue, the author has implemented or integrated CLOUD and BLOCKCHAIN technologies to either safeguard data from being tampered with or alert the user to any such changes. In the proposed article, the author uses a number of different CSPs (cloud service providers) from which the user may choose to employ any or all of the available services. Fully holomorphic encryption (FHE) is an encryption method that does not need decryption in order to perform computations on encrypted data. Files are encrypted using FHE, and the author generates a MASTER HASH on each one before storing it in the cloud to ensure that it hasn't been tampered with in any way.

Requesting verification of data in the cloud activates the Blockchain Ethereum tool, which logs the MASTER HASH code for all files. If the master hash calculated by the cloud corresponds to the one sent by the blockchain, then the user may rest certain that his data is safe.

Multiple nodes in the Blockchain will store each master hash as a transactional block by connecting the blocks with code (decentralized). The data is safe if and only if the hashcode for each block is verified by each node throughout the verification process.

5. EXPERIMENTAL RESULTS

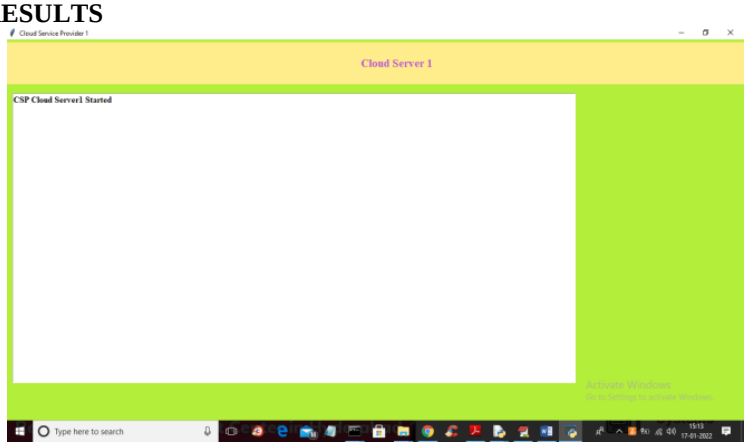

Fig.3: Output

Fig.4: Output

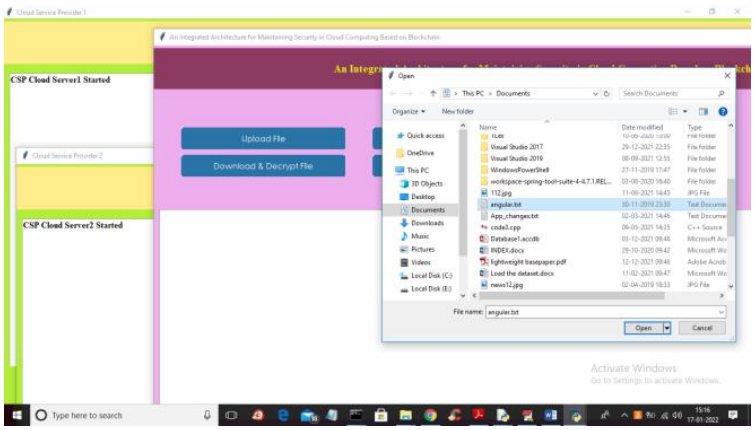

Fig.5: Output

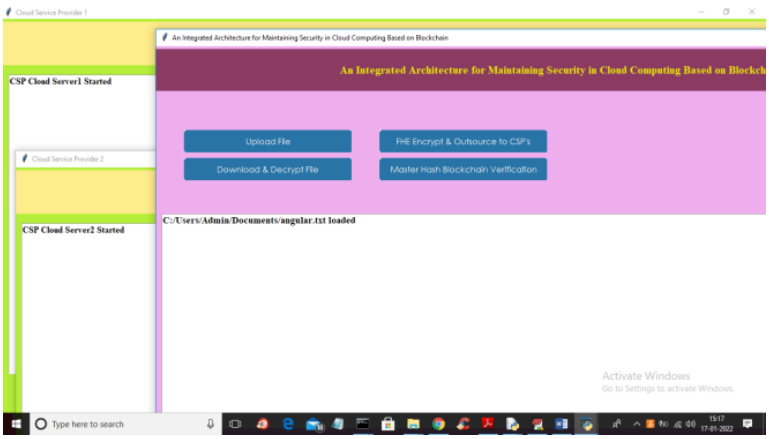

Fig.6: Output

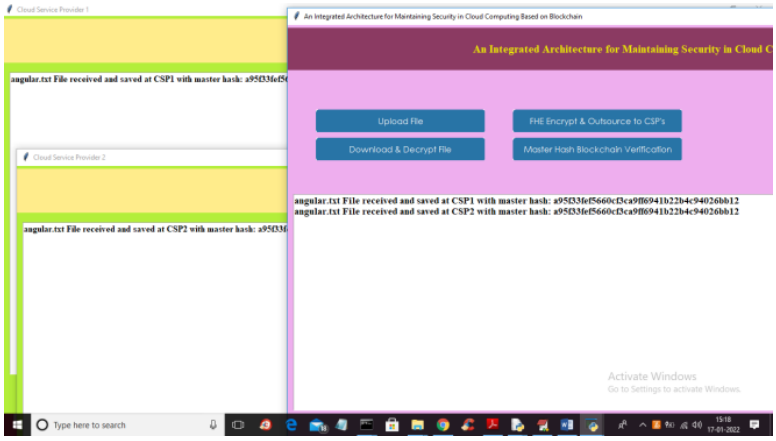

Fig.7: Output

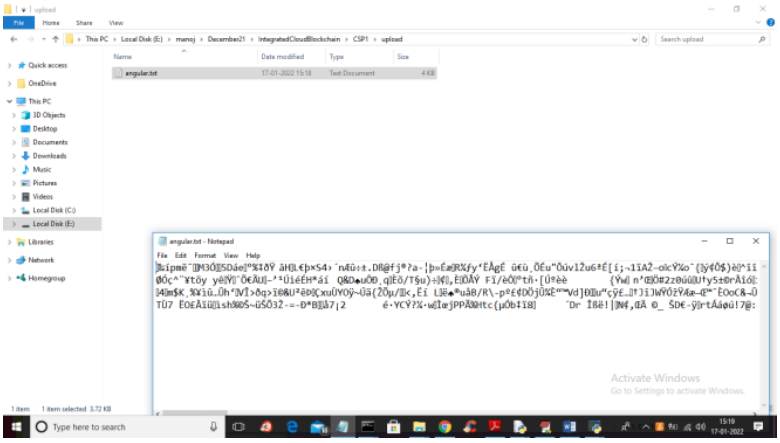

Fig.8: Output

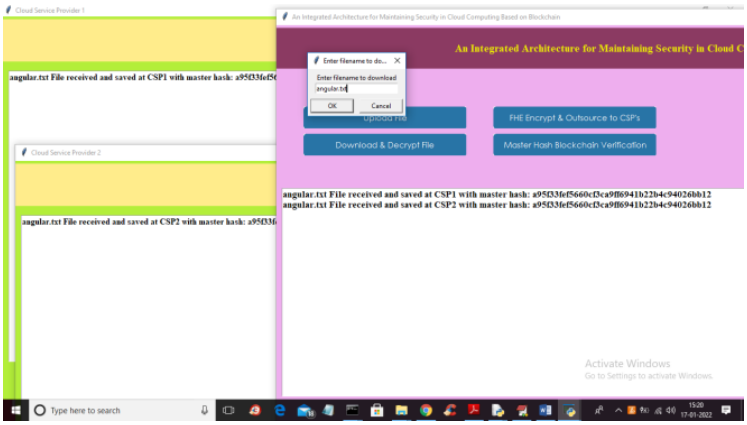

Fig.9: Output

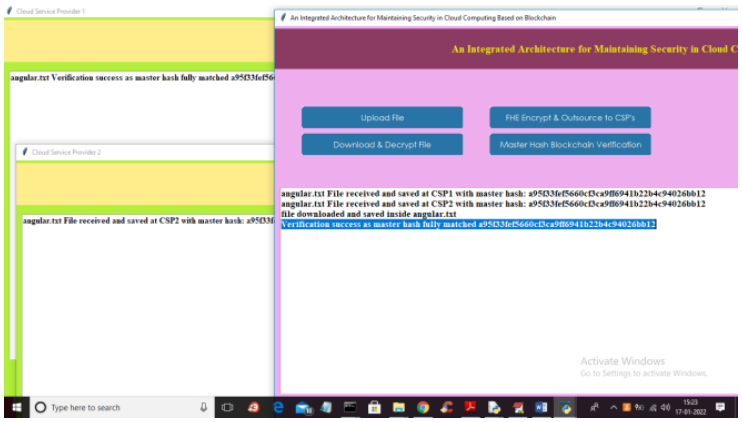

Fig.10: Output

As an addition, we've included the CHA-CHA method, which is more secure than the one proposed in the original study but uses far less computing power than Fully Homomorphic encryption.

Fig.11: Output

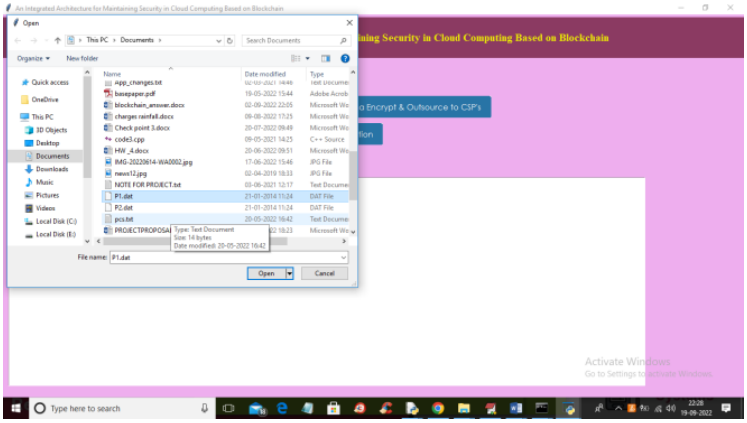

Fig.12: Output

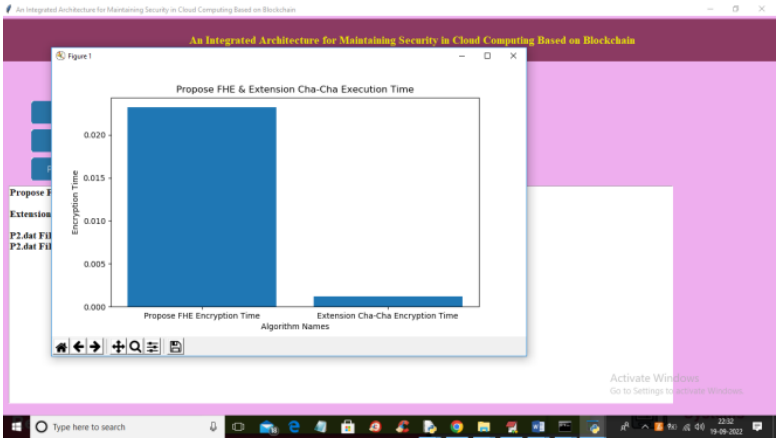

Fig.13: Output

6. CONCLUSION

In this article, we will discuss the issues of cloud computing data breaches and the all-encompassing jurisdiction of cloud service providers over client data operations. The method we provide enhances the client's existing capacity for data security. For outsourced computations to be private and secure, the suggested technique uses homomorphic encryption. A unique solution is provided based on a distributed network of cloud service providers and Byzantine Fault Tolerance consensus to guarantee data integrity and detect data tampering from the cloud service provider itself. No information is shared directly between the various cloud providers in the proposed approach. Cloud providers are obligated to offer clients with immutable verification data by computing master hash values of their databases and storing them in blockchain networks like Bitcoin's or Ethereum's. In order to meet the needs of our varied clientele, we provide a quantitative breakdown of overhead expenses per time frame. It turns out that the cheapest way to reliably generate master hash verification values every 30 minutes is to embed the master hash value as a log event in the Ethereum network (about $88 USD per year). However, the paradigm where the master hash values are incorporated as a variable in an Ethereum

transaction offers the best online performance. Additionally, we analysed the security needs and outlined how the suggested technique may be easily implemented.

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.

[11]. Srilatha Puli, A Machine Learning Model For Air Quality Prediction For Smart Cities, Design Engineering || Issn: 0011-9342 | Year 2021 - Issue: 9 | Pages: 18090 – 18104

[12]. Srilatha Puli, Quality Risk Analysis For Sustainable Smart Water Supply Using Data Perception, International Journal Of Health Sciences Issn 2550-6978 E-Issn 2550-696x © 2022, Https://Doi.Org/10.53730/Ijhs.V6ns5.9826, 18 June 2022

[13]. Srilatha Puli, Urban Street Cleanliness, Journal Of Algebraic Statistics Volume 13, No. 3, 2022, P. 547-552, Https://Publishoa.Com, Issn: 1309-3452

[14]. Srilatha Puli, Self-Annihilation Ideation Detection, Neuroquantology | June 2022 | Volume 20 | Issue 6 | Page 7229-7239 | Doi: 10.14704/Nq.2022.20.6.Nq22727

[15]. Srilatha Puli, Crime Analysis Using Machine Learning, Ymer|| Issn: 0044-0477, April 2022

[16]. srilatha puli, a machine learning model for air quality prediction for smart cities, design engineering || issn: 0011-9342 | year 2021 - issue: 9 | pages: 18090 – 18104

[17]. srilatha puli, quality risk analysis for sustainable smart water supply using data perception, international journal of health sciences issn 2550-6978 e-issn 2550-696x © 2022, https://doi.org/10.53730/ijhs.v6ns5.9826, 18 june 2022

[18]. srilatha puli, urban street cleanliness, journal of algebraic statistics volume 13, no. 3, 2022, p. 547-552, https://publishoa.com, and issn: 1309-3452

[19]. srilatha puli, self-annihilation ideation detection, and neuroquantology | june 2022 | volume 20 | issue 6 | page 7229-7239 | doi: 10.14704/nq.2022.20.6.nq22727

[20]. srilatha puli, crime analysis using machine learning, ymer|| issn: 0044-0477, april 2022

[21]. srilatha puli, n-grams assisted youtube spam comment detection, ymer || issn: 0044-0477, april 2022

[22]. srilatha puli, analysis of brand popularity using big data and twitter, ymer|| issn: 0044-0477, april 2022

[23]. srilatha puli, cyber threat detection based on artificial neural networks using event profiles, the international journal of analytical and experimental modal analysis, issn no: 0886-9367

[24]. srilatha puli, face mask monitoring system, the international journal of analytical and experimental modal analysis, issn no: 0886-9367

[25]. srilatha puli, iot based smart door lock surveillance system using security sensors, advanced science letters e-issn: 1936-7317

[26]. srilatha puli, safety alerting system for drowsy driver, 9th international conference on innovations in electronics & communication engineering (iciece-2021), page – 40

[27]. n. swapna suhasini, srilatha puli, big data analytics for malware detection in a virtualized framework, journal of critical reviews, issn:2394-5125 vol.7, issue 14, july – 2020

[28]. srilatha puli, block chain based certificate validation, international journal of science and research (ijsr), and issn: 2319-7064 sjif (2022): 7.942, volume 11 issue 12, december 2022, paper id: sr221219113003, doi: 10.21275/sr221219113003, www.ijsr.net

[29]. mrs. srilatha puli, energy efficient teaching-learning-based optimization for the discrete routing problem in wireless sensor network, international journal of early childhood special education (int-jecs) doi: 10.48047/intjecse/v14i7.296 issn: 1308-5581 vol 14, issue 07 2022.
[30]. mrs. srilatha puli, a hybrid block chain-based identity authentication scheme for multi- wsn, international journal of early childhood special education (int-jecs) doi: 10.48047/intjecse/v14i7.296 issn: 1308-5581 vol 14, issue 07 2022
[31]. mrs. srilatha puli, implementation of a secured watermarking mechanism based on cryptography and bit pairs matching, international journal of early childhood special education (int-jecs) doi: 10.48047/intjecse/v14i7.296 issn: 1308-5581 vol 14, issue 07 2022
[32]. mrs. s.sunitha, mrs. srilatha puli, multilevel data concealing technique using steganography and visual cryptography, international journal of early childhood special education (int-jecse) doi:10.48047/intjecse/v15i1.1 issn: 1308-5581 vol 15, issue 01 2023
[33]. mrs. srilatha puli, blood bank management donation and automation, specialusis ugdymas / special education 2022 1 (43), https://www.sumc.lt/index.php/se/article/view/1995
[34]. n. s. suhasini and s. puli, "big data analytics in cloud computing," 2021 sixth international conference on image information processing (iciip), shimla, india, 2021, pp. 320-325, doi: 10.1109/iciip53038.2021.9702705.
[35]. surarapu sunitha, blockchain-based access control system for cloud storage, ymer || issn: 0044-0477, april 2022
[36]. surarapu sunitha, artificial intelligence support for cloud computing intrusion, deep-cloud issues, solid stage technology, volume:63, issue:2s, publication-2020
[37]. surarapu sunitha, cryptocurrency price analysis using artificial intelligence, journal of algebraic statistics volume 13, no. 3, 2022, p. 486-493 https://publishoa.com issn: 1309-3452
[38]. surarapu sunitha, an empirical study on security issues and mitigation techniques in opportunities networks, think india journal, issn:0971-1260, vol-22, issue-41, december-2019
[39]. surarapu sunitha, a hybrid block chain-based identity authentication scheme for multi-wsn, international journal of early childhood special education, issn: 1308-5581, vol 14, issue july-2022
[40]. sunithasurarapu, cryptocurrency price prediction using neural networks, deep learning and machine learning , international journal for innovative engineering and management research, issn:2456-5083, volume 12, issue 05 may 2023, pages:408-417
[41]. sunitha surarapu, multilevel data concealing technique using steganography and visual cryptography, international journal of early childhood special education, volume 15, issn:1308-5581, iisue january 2023