ISSN:0975-9646



# Decentralize Log File Storage and Integrity Preservation using Blockchain

**Poorvi Jain[1], Ajitabh mahalkari[2]**

*Department of Computer Science and Engoneering, Sushila Devi Bansal College of Technology, Indore(M.P), India*

jainpoorvi301094@gmail.com1,ajitabh.mahalkari@sdbct.ac.in2

***Abstract*— Cloud computing is rapid growing technology as it provides resources to the user's based on their requirements. Users can allocate and de-allocate the services of the cloud. Cloud uses virtual machines to offer assistance. Availably, rapid elasticity and Cost-effectiveness is main key benefits of cloud technology. As today is the digital world, user's uses cloud technology to perform ethical and unethical work. To identify any crime or unethical work in cloud environment forensic team allocated. The Cloud forensic team follows a complete forensic process in a cloud environment to identify any attack and the person behind this attack. Cloud Forensic process completed in four steps that are Identification, Preservation and collection, Examination and presentation. When the user performs single activity in the cloud, it stored in the form of log files. Logs are crucial assets in the legal process. These cloud log files can track all the user's actions. The integrity of log files is essential in cloud computing to reach any attacker. To preserve log file integrity proposed work introduces Decentralize log files storage system to ensure security and integrity of log file—the prototype of the proposed approach based on Ethereum Blockchain and IPFS Peer-to-Peer network protocol. The Proposed prototype is secure, efficient and cost-effective to preserve the integrity of log files with minimum gas value and minimum transaction rate to store log files in Blockchain.**

***Keywords*— Cloud Computing, Cloud Crime, Cloud Forensics, Digital Forensics, Forensics Methods, Incidents, Investigation challenges, logs integrity, Blockchain.**

## I INTRODUCTION

The Cloud computing is a hub for all type of computing services. It is a robust solution to provide software, platform and infrastructure-related services. Cloud works on Pay-as-you-go model; users can access services with minimum cost. Malicious actors take advantage of this feature of cloud computing to perform crime in cloud[11] environments. A specialized team implemented to find these attacks in cloud environment knows as cloud forensics. All the activities performed by a user in the cloud should store in the form of logs. All the users' action can trace with the help of activity logs. In such cases, an investigator depends on the cloud service provider to collect log files.

After the collection of log files into the forensic log directory, it is necessary to prevent these logs from attack. Attackers first try to attack log system as logs are evidential documents. Hence it is mandatory to secure log files. Logs are threatening performed by various parties of the system involved in infrastructure, platform or log access authorities, which can add, remove and changelog data. There are many log tempering situations in different cloud models. If we talk about private cloud, some departments want to make a backup for every Minuit, and at the time the IT team fails to create a backup because of some technical issues in their department. Members of IT departments motivated to temper log files of the system. Sometimes it is also possible that investigator changes log files or remove log data before representing it to the court. Logfile analysis is a specialist in the forensic process to understand system operation, fault analysis and anomaly detection.

Our main objective is to maintain security and reliability in log files, as log files are essential to find attacker's traces. The attacker does first analyse log files and does modifications in it to hide them. In community cloud, all the partners are responsible for their operational task, maintenance task and to control over the cloud for any situation to make it available. In such case, if any party of the community cloud makes a mistake, will motivate to temper log files, in the public cloud, all the services provided by a service provider over the public network.

Users are not able to control over cloud infrastructure because of authentication problem. For example, if he is using any service of cloud and wants to use an auto-scaling [13] feature of cloud to improve performance. In such a case, if he gets any performance issue and asks the service provider to provide a detailed report about service. In such a case, the cloud service provider will temper with logs to prove them right. Because if a client finds any corruption from the provider side, they can file a case at the service provider. In such cases, if anyone will temper logs, the situation becomes a cold case.

We are introducing Blockchain technology to secure log files in a distributed manner [12]. In Blockchain log files integrity can verify by contacting any node in the network. Blockchain requires joint efforts from all the entities in the system. Blockchain is similar to a public account book which maintained by each object of the net. It is trustable technology to store any records with a proper timestamp. It overcomes the problem generated with the centralizing system to store data. In a centralized system, if the server goes fail for some reasons, there is no way to recover data on time, it requires lots of time. [19]With the implementation of Blockchain, data can flow globally without third party verification.

In our system, we are using Public Blockchain such as Ethereum to store log files securely. In Blockchain Blocks sealed cryptographically, this makes it tamper-resistant. Data in Blockchain stored globally in different-different locations, which challenge attackers to break their system. Every small event performed by the user in reflected all the participants of Blockchain; hence no one can moodily log file after storing it to Blockchain. Blockchain is a chain of blocks. Transaction verified first, before storing it to Blockchain. Many organizations over worldwide are adopting Blockchain technology because of its high-level security and availability features.

In Blockchain succeeding block contains the hash value of the preceding block, if an attacker wants to perform the attack, it requires to update each block hash. It is tough to perform any fraudulent activity in Blockchain. To make it little private, we are using an encryption layer before storing our file into Blockchain, so only authorized user can see file content. This encryption layer is using public-key cryptography to encrypt log file. Another issue in Blockchain is it requires several transactions to store the large file.

To overcome this problem and to achieve high throughput, we are using an IPFS protocol. With the addition of this IPFS technology in our Blockchain technology, large files can store in Blockchain with one transaction. First, we store the data in IPFS, IPFS generate a fixed-size hash for the submitted data, and then this hash will be stored in Blockchain. A decentralized system to store log files implemented based on Blockchain and IPFS to ensure availability, security in log files. All the log files distributed globally to preserve the integrity of log files. If an attacker tries to attack one system, then the investigator can access data from uncompromised device globally in a decentralized manner.

## II BACKGROUND

The given section contains detailed overview of the cloud computing, digital forensics and cloud forensics.

### *2.1 Cloud Computing*

Cloud computing is most an appropriate paradigm in today becauseof its benefits. (Marty and Raffael et.al, 2011) .In cloud computing, user's can demand resources as per their requirements. All the resources allocated and de-allocated to the users in sharing way (M. Edington Alexa and R. Kishore b et.al, 2017 ).

As per NIST [2] "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

### *2.2 Digital Forensics*

By NIST, 2006 Proposed simple definition “The applications of science to identify, collection, examination and analysis of data while preserving[6] the integrity of the information and maintaining a strict chain of custody for data.”


*Fig 1 Phases in Digital Forensics*

***1) Identification:*** In this phase, malicious activities identified.
***2) Collection:*** Evidence which is related to malicious activity also identify the integrity of the collected evidence maintained
***3) Organization:*** All the conglomerate evidence examined and correlated by the investigator.
***4) Presentation:*** A crucial phase to evidence represented in the form of a report to the jury regarding the case[2].

### *2.3 Cloud Forensics*

National Institute of Standards and Technology (NIST) [2] defines cloud computing as "Cloud computing forensic science is the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events. The judicial process is done through identification, collection, preservation, examination, and interpretation and reporting of digital evidence".

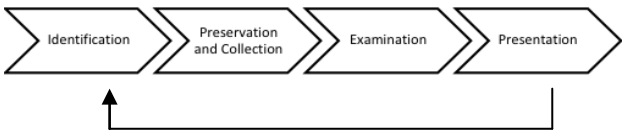


*Fig 2 Cloud forensics Process*

***1) Identification:*** All the evidence related to the investigation process identifies in this step [5]. It is the most important stage in cloud forensics. In identification stage, the explorer collects data and data resources which were used by criminals to commit a crime in the cloud. Clearly, a search warrant issued to access to CSPs infrastructure. All the methods and process to identify evidence in cloud infrastructure should be reported and documented properly.
***2) Preservation and Collection:*** In this stage, all the evidence collected from cloud different cloud locations. All the evidence preserves in isolating way so no one can steal or change evidence information. The integrity of the proof needed in this phase. New tools and technologies required to extract cloud data. These steps require maintenance of chain of custody.
***3) Examination:*** Examination stage involves the extraction of stored data from the previous step and to find evidence from collected data with the help of technician experts needed. A high-level strategy required to make suitable action plans to complete this examination process. Examiners which involves in this process should maintain professionalism—all the steps which followed in the examination phase recorded in files.
***4) Presentation:*** It is a final stage in the judicial process. All the substantiation reported with findings produced with the help of expert testimony. Presentation report should be prepared by experts who can represent evidence in front of the jury. Chain of custody should be maintained and submitted to the court.

#### *2.3.1 Logs in cloud forensics*

Every single process or events performed by cloud entity, Stored in the form of log records[18]. In cloud each process has their separate log file based on executed events and process. These log files provide details about every single step of cloud user. In case if any attacker wants to perform any activity in cloud, all the activities performed by attacker stored in log files and these files stored in server. Attackers find all information before making any attack in cloud. Hence it is necessary to secure maintain integrity of log files to find attackers traces in cloud forensic process.

#### *2.3.2 Provider Driven Cloud Forensics*

There are two types of Provider driven cloud forensics[10]-

- Agent Based Solution
- Log based Solution

***1) Agent-based Solution***

There are various agent-based solutions implemented. To run predefined functions and in given time frame bot and botnets used as a forensic network agent. To exploits vulnerabilities in the network, malware used, Bot is a kind of malware which exploits weaknesses in the system and make a chain of infection by moving from one computer to another device connected over the network. The net creation by infected machines called a botnet.

The technique is helpful to perform proactive measurements in the network. Investigator extracts information from virtual machines, to perform post forensics on this information or data. Forensic centre converts this raw data into a structured format so that it can use in forensic process.

***2) Log-based Solutions***

In the computer system, every process makes an event and the documentation of these events known as logging. The files which contain every log events of hardware and software makes log files. Every log file purpose differs from each other and logs files creation depends on application and software that generate events. These log files are significant assets in the process of forensic investigation; also, these are beneficial in fault tolerance. With the help of logs, investigators can find source and timeline for an event to regenerate events in forensic process.

When a user uses cloud computing services, cloud architecture generates and store different kinds of logs. Named as audit logs, web-server logs, security, network, application logs at various levels know as VM, VMM, cloud and these logs stored in a much secured manner. User can access records based on service model of cloud computing. Cloud logs confidentiality and integrity are very crucial in the forensic process because logs are essential to reach any evidence in cloud forensic process. If logs corrupt, all the investigation process will go in the wrong direction, which can lead the process in the wrong way.

## III LITERATURE REVIEW

This section introduces all the techniques used to maintain log file integrity in forensic process. These methods are helpful to develop and effective mechanism to preserve log files integrity and security.

A scenario [11] discussed by zawoad that collecting and preserving logs is crucial task In cloud computing. Three cases can occur in any cloud attack scenario-

**Case 1:** In first, an attacker and cloud provider can alter logs, in such case investigator, won't be able to detect attacker because he does not know of attacker activity.

**Case 2:** In Second case, the provider is not able to provide any trace of the attack as the attacker rented a machine from a cloud provider and after attack terminated his/ her device.

**Case 3:** In the third case, the attacker claims that investigator and provider are framing him/her for the attack.

A Secure-Logging-as-a-Service (SecLaaS) notion is developed by the author to collect logs from the virtual machines and to store these logs in persistence storage to resolve the volatility issue. Log files sequence maintained in hash-chain format in encrypted form. Because of this proof of past logs can be generated and will be available to users. Now if cloud provider, attacker and investigator will not be able to add/remove/modify log files. A RESTful API exposed by SecLaaS to process of log collection required in the forensic procedure. A Bloom tree scheme used to increase the security and performance of the system—the Performance of the system measure by security terms, execution time and storage space. The limitation of this system logs alteration is possible by CSP before publishing PPL.

Metadata which collects information about every object and operation performed on these objects is known as cloud data provenance. The security of cloud data provenance is essential to complete any forensic task, accountability to get information about cloud activities. An architecture called ProvChain [16] is implemented for cloud data provenance with Blockchain technology to operate on data in a cloud system. The complete history of data operations hashed and stored in Merkle tree nodes.

A list of transactions will make a block. When block implemented, it requires confirmation from all nodes of the tree. In such a case, if the user wants to modify any provenance data value, the user needs to check transactions and blocks. This process of modification in Blockchain is hard and time-consuming work; hence no one can harm provenance data in Blockchain-based system. Data integrity and trustworthiness achieved by using Blockchain. The current system is validated for only one cloud service provider.

A solution to store log files in such a way that no one can temper log files implemented by William Pourmajidi and Andriy Miranskyy in [13] named as Logchain. This Log chain system using Blockchain technology to store logs from different providers. An immutable log system developed to prevent log tempering by log cryptography and then storage of logs in the hierarchical ledger. This system stores hash or log files and stores them in a hierarchical ledger. In this prototype, they divided Blockchain to make a hierarchy of Blockchain. The primary purpose of this system is to make this system scalable for storing a large number of log files. The integrity of the log file checked on a higher level by reducing operations, which already performed on lower blocks.

The prototype requires making a hierarchical ledger for which application needs to sit on primary Blockchain first. In this prototype first, the log file will be loaded and converted into blocks, and after that, this will mine the blocks to store files in Blockchain. To send, retrieve or verify these log data clients need to interact with this system via API. A verify tb function introduced in this API to improve the scalability of the system. This function assures that no one tempered the block sequence in the order. A search function also introduced in this system to improve the accessibility of log files. User can search for data based on block index.

A review paper about cloud forensics challenges, solutions published (Poorvi Jain and Ajitabh Mahalkari, 2018) with a comparative study about forensics techniques with their benefits and limitations. Some problems are marked by author in cloud forensics that when we collected data for the forensic process, then there is no particular method to secure pre-forensic and post forensic data. To make cloud services to cloud forensics enabled services, a method described with the summation of cloud computing and the process of investigation in the cloud. Nowadays, crimes are increasing; hence this model implemented (Simou et al., 2018) cloud forensics enabled services to make forensics process easier.

New network monitoring system has a short time window to detect an attack in the network. This timeframe [17] to make a network connection with security monitoring devices is too short; attackers collect all the information of the network before making any theft in the network. They know very well about this weakness of network monitoring system; hence they perform attack actions over the net for an extended period to remove their traces from the network.

An analysis of log files to uncover the attacker's traces is an essential process in forensic investigation [12]. First, Bitcoin implemented in the form of the Bitcoin protocol. It is a collection of blocks to store transactions. This transaction stored in the form of the hash in a very secure way so no one can overwrite any transaction. First Blockchain used only for cryptocurrency, but nowadays users are aware of its advantages very well, so it is using in different areas to make systems better. Integrity and confidentiality of the log files is a tremendous task in cloud legal process.

In this system, they used the engrave chain to provide integrity in log files. To protect log files from attacks logs are stored in a distributed system to avail redundant copies of log files, a complete system implemented over-hyper ledger fabric to provide security and confidentiality in log files. To enable and create private and permission Blockchain hyper ledger used. File ID required to access log file data in the system. This method is suitable for integrity, but there are some issues related to scalability and performance.

The only technical team in cloud computing is responsible for providing attention on logs to ensure the performance of the system. Logs are needed when customers issue complains about the performance of the platform or accessibility of the system services. Any party who wants to generate fault in order can temper logs in the cloud. In such case to resolve customer issue management team, customer care, customer support depends on these log files.

Any computational crime can be detected by using analysis of log files; Log files contain a complete track of operations executed in a cloud system. In this paper [14] author

proposed a method to provide integrity in log files using third party auditor in such a way so that CSPs and attacker not able to modify it after-the-fact. A Merkle hash tree used to convert his concept in reality. In this data structure, log files block aggregated and generate root node, The value of root node stored in Blockchain to make it secure to prevent it from the threat. To reduce computational complexity overhead, this model implemented for a security audit of log files.

The protocol designed to support only public verification of log files. This concept comes in author mind to provide security and performance of log data in cloud; it allows any trusted third party to verify the log's integrity. Auditing correctness ensured by this model. It is a weighted light system; Minimum computation cost required to audit logs. The author used Homomorphic hash function to generate tag of log blocks. Sometimes CSP is not trustable to provide an actual tag of log files. After the generation of tag these log blocks aggregated and root node value stored in Blockchain to reduce cost and to maintain integrity.

Existing solutions to maintain log integrity are cost-effective and takes time to implement. A new approach proposed (Benedikt Putz, Florian Menges, Günther Pernul,2019) to prevent log integrity. This system reduces dependency on a trusted third party or any specialised hardware. A secure and reliable system implemented based on Blockchain to store log files in a non-repudiable way to preserve the integrity of log files. In this system, no CSPs and trusted third party can modify logging source.

They modified a prototype name as Dingfest project. The aim was to implement this prototype is to create an opensource infrastructure to provide help in data acquisition, data analysis and incident reporting to make the forensic process easier. To ensure forensic audit ability in this system fourth component was developed in [15]. This module invented to fulfil the needs of the legal department to prevent relevant evidence so that they used in court without any trusted third-party verification.

Data sharing in a secured way can be done quickly with this system because they used permissioned Blockchain to implement their system to provide integrity, security and audit ability of log files. An exonum framework used to design Blockchain-based system to store log files. Various vital features of exonum framework used to make it secure. The only limitation of this system is that it is using Blockchain auditing layer, which effects transaction throughput of the system.

To overcome the problem as mentioned above of a real-time system, researchers took advantage of archived log analysis. In this process logs preservation for a long time is essential, this is a very critical challenge because system logs are small in size, but when we talk about network logs, they are plentiful as the network is a cluster of nodes or systems. It is cost-effective to store such records for an extended period. Scalability of the system is the main objective in this research—Blockchain and cloud platform used to provide scalability and security in this system. Blockchain used to provide security in the system as it contains complete log data of network and subnetwork.

It is beneficial to make system tamper-proof. Blockchain is a secured data storage technology; no one can tamper or forge data which resides in Blockchain. It ensures the availability of the data to make analysis and auditing process easy. This architecture provides log storage for a long period to make in-depth analysis easily to understand attack patterns easily.

## IV PROBLEM DOMAIN

To analyze the problems in recent system many research papers has been studied. Following are some problems extracted from previous research.

- In the previous system, there was no storage system to store pre-forensic data or securely log files.
- Auditing of log files was very tedious and cost-effective in a centralized system. The trusted third party required to audit cloud logs.
- To store complete log files over Block chain requires huge transaction amount and Gas.
- There was problem of availability and security of log files in centralizes system.

## V OBJECTIVE OF WORK

The main objective of this research is to convert centralize log file storage into decentralize log file storage system and integrity preservation of log files. Following steps needed to make this research beneficial in forensic process.

- *To study different Blockchain based solutions for log integrity:* We will study different Blockchain based technique to make our prototype feasible.
- *To design and implement new optimal solution to achieve log integrity in cloud forensics process:* After analysis from previous phase, we will implement new optimal solution to preserve integrity of log files using Blockchain.
- *To develop a de-centralize storage system for forensic log files:* Need to build a decentralized app to store log files to remove the dependency on a centralized server.
- *To remove the dependency on the third party for an audit of log files:* In centralize, system trusted the third party required to audit log files, which was costly. We are trying to build a system to avail log files in a de-centralize manner over peer to peer network.
- *To build an optimized Blockchain-based system to minimize transaction fee and gas value for log file storage:* A method to store a large number of log files with a minimum transaction fee and gas value.
- *Performance evaluation of proposed system:* In this phase we will evaluate performance of the proposed system to make it adaptable in forensic process.

## VI SOLUTION DOMAIN

The proposed work is about to solve the problem of log files integrity in cloud forensics process. Any activity performed by the user in the cloud, recorded in the form of logs. When an illegal action taken by an attacker shown in cloud computing, it stored in the form of logs. Every log files in cloud shows different process and logs make easier to find details about attack and also to make system resist from that attack. Security is main concern in very system to make it beneficial for all users. Logs preservation is an excellent challenge in cloud computing. After log preservation, it is necessary to maintain integrity in log files to make it tamper-proof.

In [17] centralize system used to preserve log files, but there are some limitations of the centralizing system. All the data in concentrate system stores centrally with the benefits of Blockchain and cloud computing technology, if in any condition server goes down, or server attacked by an attacker then there is no chance to retrieve log files on time. To overcome these issues of centralize system, we are proposing a methodology to convert centralize system into decentralize log files storage system to makes file availability. we are using Blockchain technology to store log files to preserve integrity.

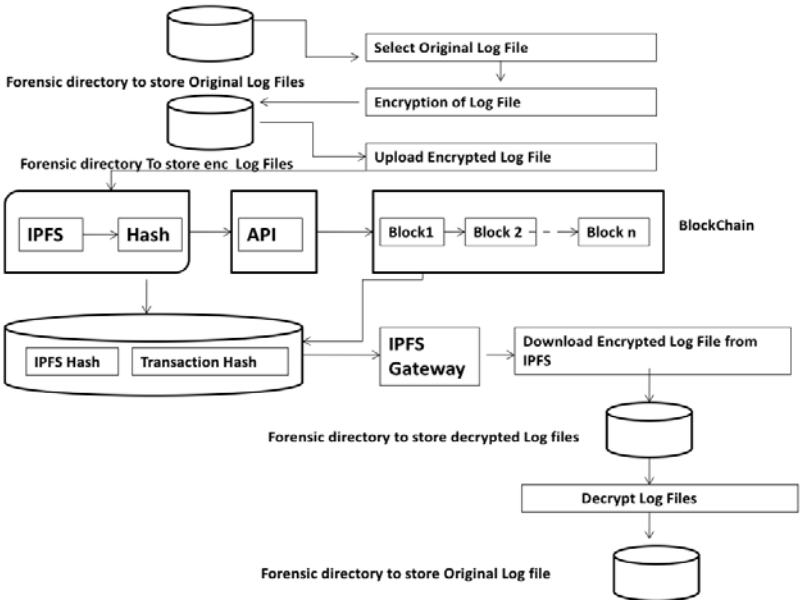


Fig 3 Flowchart for Proposed Prototype

As our researches used Blockchain technology to preserve integrity of log files, but their research bounded with one disadvantage of Blockchain. Theoretically it is proven that Blockchain has limited storage to store any data but practically to store high amount or data in Blockchain requires high transaction amount or high gas required to pay for miners. To store large number of files in Blockchain with minimum transaction fee and minimum gas value, we are developing a prototype based on Ethereum Blockchain and IPFS. Ethereum Blockchain and IPFS has great benefits to make our prototype feasible in cloud forensics. Our prototype serves both intentions in log file storage system by converting centralize log file storage system to decentralize system and to preserve integrity.

In our methodology, we are using Blockchain technology for storing log files. We are using the IPFS protocol to store log files. First, we store log files in IPFS, IPFS generate a hash value for the submitted file. IPFS is a de-centralize system to store data. It's a connected network of peer-to-peer nodes, which makes it a de-centralize network. Data availability is high when we saved any data in IPFS, it uses a Distributed hash table data structure for data storage. In some cases, if one system will fail to provide stored data to the user, other nodes in the network are ready to provide data to users based on their interest. IPFS uses content addressing to search file in global file space. It follows a public cryptography method to secure data.

In our system, we are using Blockchain technology to provide integrity in log files. Blockchain is the chain of blocks. Blocks in Blockchain contain digital data and chain is a public database. Every block in Blockchain contains transaction details, this transaction verified by Blockchain before including it to the block. Blockchain uses Public-key cryptography to secure data. High level of security achieved in Blockchain because of its de-centralize nature, and no one allows to do modification in Blockchain data. Blockchain provides data in a readable format only.

We are using Ethereum Blockchain in our proposed system because Ethereum provides a great platform to develop a de-centralize application in Blockchain. To perform any action in Ethereum Blockchain, smart contracts build. It is beneficial technology to achieve higher-level security and availability in log files. Ether currency required to make any transaction in Ethereum. Every operation in Blockchain charges a token value; another token used to provide miners fees in Blockchain called gas value.

To connect web application and Blockchain an API introduced in our system known as Infura. It does not perform any transaction in Blockchain to maintain security. But a wallet is introduced by Infura team to manage the transaction in Blockchain called Metamask. It uses the private key and public key to perform any operation in Blockchain. After executed verified transaction in Blockchain, data can be stored in blocks of Blockchain. It contains cryptographic data.

In our Prototype we are using an extra encryption layer at the receiver and sender side to achieve confidentiality and more security. Public key encryption used in our system to make it more secure.

A flowchart implemented in the proposed method to show the process of our model. A Public key encryption layer is used before making any transaction in Blockchain. IPFS used to store a large number of log files to ensure security and availability of log files. Only log files hash submitted to Blockchain for log file integrity. The sender needs to store IPFS hash of the log file, so whomever sender wants to share log files, can share IPFS hash to the receiver. The receiver will receive the file and will decrypt it to get file data.

## VII RESULT ANALYSIS

The suggested approach fulfills its objective of storing log files into Ethereum Blockchain with minimum transaction cost and minimum gas value. For measuring of system performance certain parameters are selected. This chapter shows certain aspect of measurements with predefined measurements parameters. The result is represented in tabular and graphical form. Where row representing single experiments record, column showing parameters on which experiments result is measured. Here some parameters to analyze our prototype result that are File size, Gas used, Transaction cost, file submission time. On the basis of these initial parameters system performance can be measured. The later result analysis factors are (i) Availability(ii) Execution Time (iii) Transaction cost .

| S.No | LOG File | File Size (Byte) before enc | File Size (Byte) After enc | Exe time in sec | Nonce | Tranx Fee(Ether) | Gas Used(units) By transaction | GAS Price (GWEI) | File H.S. (BYTE) | Block No. | File Size (Bytes) Before dec | File Size (Bytes) after dec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | LF 1 | 8452 | 1502 | 12.27 | 28 | 0.000034837 | 34837 | 1 | 32 | 7529782 | 1502 | 8452 |
| 2 | LF 2 | 16904 | 1628 | 16.49 | 18 | 0.000034837 | 34837 | 1 | 32 | 7529536 | 1628 | 16904 |
| 3 | LF 3 | 23296 | 4222 | 33.63 | 9 | 1.7E-13 | 34837 | 1 | 32 | 7461045 | 4222 | 23296 |
| 4 | LF 4 | 33808 | 1831 | 15.2 | 19 | 0.000034837 | 34837 | 1 | 32 | 7529550 | 1831 | 33808 |
| 5 | LF 5 | 44675 | 3848 | 42.83 | 11 | 1.7E-13 | 34837 | 1 | 32 | 7461319 | 3848 | 44675 |
| 6 | LF 6 | 50712 | 2012 | 18.51 | 21 | 0.000034837 | 34837 | 1 | 32 | 7529581 | 2012 | 50712 |
| 7 | LF 7 | 67712 | 2196 | 13.73 | 23 | 0.000034837 | 34837 | 1 | 32 | 7529572 | 2196 | 67712 |
| 8 | LF 8 | 84520 | 2391 | 16.71 | 22 | 0.000034837 | 34837 | 1 | 32 | 7529593 | 2391 | 84520 |
| 9 | LF 9 | 99271 | 14114 | 40.54 | 7,8 | 1.3E-13 | 26437 | 1 | 32 | 7457875 | 14114 | 99271 |
| 10 | LF 10 | 118328 | 2739 | 38.73 | 20 | 0.000034837 | 34837 | 1 | 32 | 7529609 | 2739 | 118328 |
| 11 | LF 11 | 135232 | 2921 | 10.64 | 25 | 0.000034837 | 34837 | 1 | 32 | 7529622 | 2921 | 135232 |
| 12 | LF 12 | 152136 | 3102 | 16.74 | 24 | 0.000034837 | 34837 | 1 | 32 | 7529613 | 3102 | 152136 |
| 13 | LF 13 | 169040 | 3282 | 34 | 28 | 0.000034837 | 34837 | 1 | 32 | 7529622 | 3282 | 169040 |
| 14 | LF 14 | 185944 | 3459 | 10.64 | 26 | 0.000034837 | 34837 | 1 | 32 | 7529622 | 3459 | 185944 |
| 15 | LF 15 | 202848 | 3183 | 13.18 | 12 | 0.000034837 | 34837 | 1 | 32 | 7529634 | 3183 | 202848 |
| 16 | LF 16 | 219752 | 3787 | 17.14 | 27 | 0.000034837 | 34837 | 1 | 32 | 7529644 | 3787 | 219752 |

Table 1 Experiments Result

*To store large amount of the data in Ethereum requires high amount. Generally to store 1 word(8 bytes) requires 20,000 gas. Gas price is 4gwei/gas. So if 1 word requires 20000 gas price then 20000*4gwei/gas= 80000 gwei requires to store one word in Blockchain.80,000 gwei for 8 bytes. x 1000bytes/8 = 10,000,000 gwei/kB = .01 Ether .01 Ether/kB x 1000kB = 10 Ether to store a 1Mb at $860/ether = $8600.00*

Above table with 16 experiments to analyze out prototype results. Rows in table shows result analysis parameters and column shows all the experiments result for the mentioned parameters.

Our system made to store large amount of file into Ethereum with low gas price as shown in above graph. We used IPFS to store log files and to generate hash value of files. In our system after generating hash value, IPFS automatically submit hash into Blockchain. This hash size is equal for different size of log files.

**A. Log File Sizes before submitting it to Blockchain**

Below table shows the results for log file sizes before encryption and after encryption. Row of the table contains all the parameters and column shows respected values for all the parameters required to perform log files size analysis.

| S.No. | Log Files | Log File Size(Bytes) before dec | Log File Size (Bytes) After dec |
|---|---|---|---|
| 1 | LF 1 | 8452 | 1502 |
| 2 | LF 2 | 16904 | 1628 |
| 3 | LF 3 | 23296 | 4222 |
| 4 | LF 4 | 33808 | 1831 |
| 5 | LF 5 | 44675 | 3848 |
| 6 | LF 6 | 50712 | 2012 |
| 7 | LF 7 | 67712 | 2196 |
| 8 | LF 8 | 84520 | 2391 |
| 9 | LF 9 | 99271 | 14114 |
| 10 | LF 10 | 118328 | 2739 |
| 11 | LF 11 | 135232 | 2921 |
| 12 | LF 12 | 152136 | 3102 |
| 13 | LF 13 | 169040 | 3282 |
| 14 | LF 14 | 185944 | 3459 |
| 15 | LF 15 | 202848 | 3183 |
| 16 | LF 16 | 219752 | 3787 |

Table 2 Table for Log File Size before submitting it to Blockchain

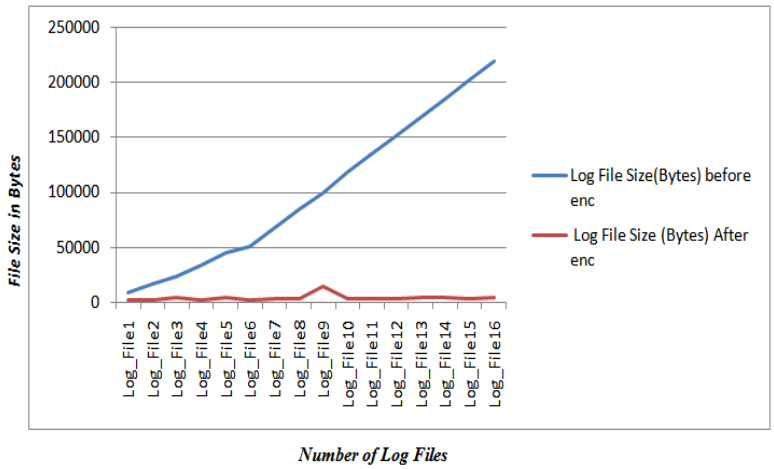


Fig 4 Log File Size before submitting it to Blockchain

Above Graph shows file size before submitting it to Blockchain for our prototype. X-axis of the graph shows no of log files used to collect results for our prototype. Y-axis shows log file size in Bytes.

**A. Log File Size after receiving it from Blockchain**

Below table shows the results for log file sizes before decryption and after decryption . Row of the table contains all the parameters and column shows respected values for all the parameters required to perform log files size analysis.

| S.N. | Log Files | Log File Size(Bytes) before dec | Log File Size (Bytes) After dec |
|---|---|---|---|
| 1 | LF 1 | 1502 | 8452 |
| 2 | LF 2 | 1628 | 16904 |
| 3 | LF 3 | 4222 | 23296 |
| 4 | LF 4 | 1831 | 33808 |
| 5 | LF 5 | 3848 | 44675 |
| 6 | LF 6 | 2012 | 50712 |
| 7 | LF 7 | 2196 | 67712 |
| 8 | LF 8 | 2391 | 84520 |
| 9 | LF 9 | 14114 | 99271 |
| 10 | LF 10 | 2739 | 118328 |
| 11 | LF 11 | 2921 | 135232 |
| 12 | LF 12 | 3102 | 152136 |
| 13 | LF 13 | 3282 | 169040 |
| 14 | LF 14 | 3459 | 185944 |
| 15 | LF 15 | 3183 | 202848 |
| 16 | LF 16 | 3787 | 219752 |

Table 3 Table for Log File Sizes after receiving it to Blockchain

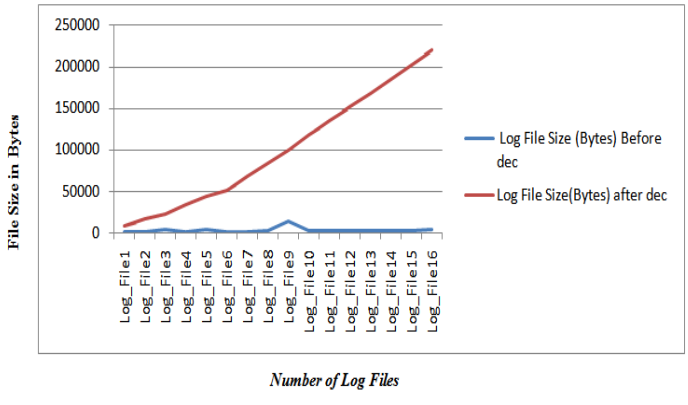


fig 5 Log File Size after receiving it from Blockchain

Above Graph shows file size after receiving it from Blockchain for our prototype. X-axis of the graph shows no of log files used to collect results for our prototype. Y-axis shows log file size in Bytes.

### C. Transaction Time analysis

| *S.N.* | *Log Files* | *Exe. time in sec* |
|---|---|---|
| 1 | LF 1 | 12.27 |
| 2 | LF 2 | 16.49 |
| 3 | LF 3 | 33.63 |
| 4 | LF 4 | 15.2 |
| 5 | LF 5 | 42.83 |
| 6 | LF 6 | 18.51 |
| 7 | LF 7 | 13.73 |
| 8 | LF 8 | 16.71 |
| 9 | LF 9 | 40.54 |
| 10 | LF 10 | 38.73 |
| 11 | LF 11 | 10.64 |
| 12 | LF 12 | 16.74 |
| 13 | LF 13 | 34 |
| 14 | LF 14 | 10.64 |
| 15 | LF 15 | 13.18 |
| 16 | LF 16 | 17.14 |

Table 4 Table for Transaction Time Analysis

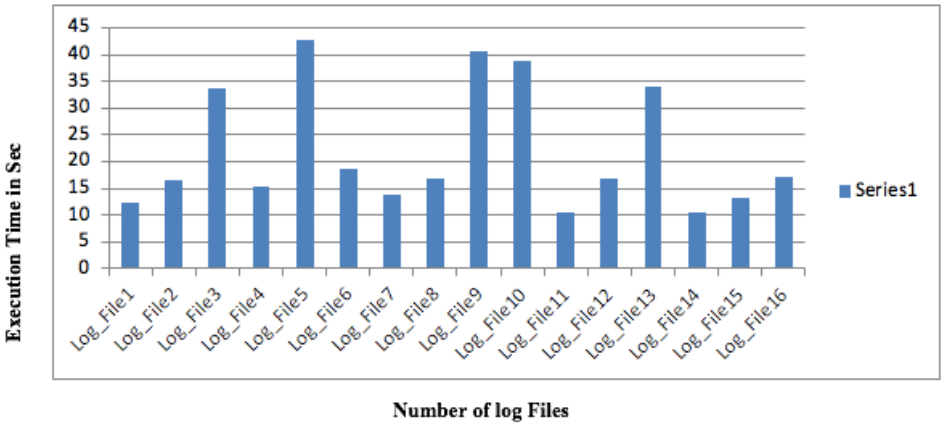


Fig 6 Transaction Time analysis graph

Above table shows the results for execution time. Row of the table contains all the parameters and column shows respected values for all the parameters required to perform log files size analysis.

Above Graph shows execution time analysis for our project. X-axis of the graph shows number of log files used in experiment and Y- axis shows execution time to perform experiment.

### D. Transaction Cost analysis

Below table shows the results for transaction cost analysis. Row of the table contains all the parameters and column shows respected values for all the parameters required to perform Transaction cost analysis.

| *S.N.* | *Log Files* | *Tranx Fee(Ether)* |
|---|---|---|
| 1 | LF 1 | 0.000034837 |
| 2 | LF 2 | 0.000034837 |
| 3 | LF 3 | 1.7E-13 |
| 4 | LF 4 | 0.000034837 |
| 5 | LF 5 | 1.7E-13 |
| 6 | LF 6 | 0.000034837 |
| 7 | LF 7 | 0.000034837 |
| 8 | LF 8 | 0.000034837 |
| 9 | LF 9 | 1.3E-13 |
| 10 | LF 10 | 0.000034837 |
| 11 | LF 11 | 0.000034837 |
| 12 | LF 12 | 0.000034837 |
| 13 | LF 13 | 0.000034837 |
| 14 | LF 14 | 0.000034837 |
| 15 | LF 15 | 0.000034837 |
| 16 | LF 16 | 0.000034837 |

Table *5* Table for Transaction Cost Analysis

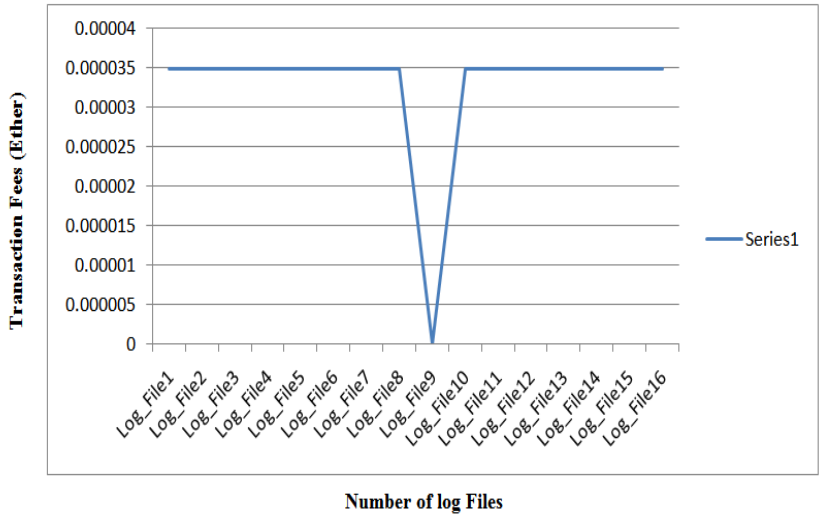


Fig 7 Transaction Cost analysis graph

## VII CONCLUSION AND FUTURE WORK

In our Prototype we used Blockchain technology to preserve log files integrity. We integrate IPFS with Blockchain technology into our system to convert centralize storage system into decentralize storage system. Also with our prototype we can preserve log files integrity as we are storing log files into Blockchain. Blockchain is a chain of hashed blocks. In Blockchain each contains hash of previous block and original data and then generate hash for the next block. We proposed a system to store large number of log Files with minimum transaction cost and gas value.Our system is secure, scalable and assures high performance.Current system depends on CSP to collect log files. In future we can increase the trust on CSPs by decreasing dependency on CSPs.

## REFERENCES

[1] Marty, Raffael, "Cloud application logging for forensics. Proceedings of the ACM Symposium on Applied Computing", 178-184. 10.1145/1982185.1982226, 2011.

[2] M.E. Alex, R. Kishore, "Forensics framework for cloud computing", Computers and Electrical Engineering.http://dx.doi.org/10.1016/j.compeleceng.201 7.02.006, 2017.

[3] https://www.fingent.com/blog/cloud-service-models-saas-iaas-paas-choose-the-right-one-for-your-business

[4] https://www.sciencedirect.com/topics/computer-science/cloud-deployment-model

[5] Simou, Stavros & Kalloniatis, Christos & Gritzalis, Stefanos & Mouratidis, Haris, "A survey on cloud forensics challenges and solutions". Security and Communication Networks. 10.1002/sec.1688,2016.

[6] Du, Xiaoyu & Le-Khac, Nhien-An & Scanlon, Mark, "Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service",2017.

[7] Ruan, Keyun & Carthy, Joe & Kechadi, Tahar & Crosbie, Mark,"Cloud Forensics. Advances in Digital Forensics VII. 35-46. 10.1007/978-3-642-24212-0_3,2011.

[8] Poorvi Jain, Ajitabh Mahalkari, "Review of Cloud Forensics: Challenges, Solutions and Comparative Analysis",2018.

[9] Stavros Simou,Christos Kalloniatis,Stefanos Gritzalis,Va silios Katos, "A framework for designing cloud forensic-enabled services (CFeS)", 2018.

[10] Manral, Bharat & Somani, Gaurav & Choo, Kim-Kwang Raymond & Conti, Mauro & Gaur, Manoj "A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions", ACM Computing Surveys. 52. 1-38. 10.1145/3361216,2019.

[11] Zawoad, Shams & Dutta, Amit & Hasan, Ragib, "Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service", IEEE Transactions on Dependable and Secure Computing. 13. 1-1. 10.1109/TDSC.2015.2482484,2015.

[12] Shekhtman, Louis & Waisbard, Erez, "EngraveChain: Tamper-proof distributed log system", 8-14. 10.1145/3362744.3363346,2019.

[13] Pourmajidi, William & Miranskyy, Andriy, "Logchain: Blockchain-Assisted Log Storage", 978-982. 10.1109/CLOUD.2018.00150,2018.

[14] Wang, Jia & Peng, Fang & Tian, Hui & Chen, Wenqi & Lu, Jing, "Public Auditing of Log Integrity for Cloud Storage Systems via Blockchain" , 10.1007/978-3-030-21373-2_29,2019.

[15] Putz, Benedikt & Menges, Florian & Pernul, Günther "A secure and auditable logging infrastructure based on a permissioned Blockchain", Computers & Security. 87. 101602. 10.1016/j.cose.2019.101602,2019.

[16] Liang, Xueping & Shetty, Sachin & Tosh, Deepak & Kamhoua, Charles & Kwiat, Kevin & Njilla, Laurent, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability", 10.1109/CCGRID.2017.8,2017.

[17] Kumar, Manish & Singh, Ashish Kumar & Skumar, tv, Secure Log Storage Using Blockchain and Cloud Infrastructure, 1-4. 10.1109/ICCCNT.2018.8494085,2018

[18] Santra, Palash & Roy, Asmita & Midya, Sadip & Majumder, Koushik & Phadikar, Santanu, "Log-Based Cloud Forensic Techniques: A Comparative Study", 10.1007/978-981-10-4600-1_5,2018.

[19] Wei, PengCheng & Wang, Dahu & Zhao, Yu & Tyagi, Sumarga & Kumar, Neeraj, "Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems" 102. 10.1016/j.future.2019.09.028,2019.

[20] Ethereum: article about Ethereum "What is Ethereum?" , By Ameer Rosic, URL: https://blockgeeks.com/guides/Ethereum.

[21] Metamask: A crypto wallet & gateway to blockchain apps, URL: https://Metamask.io

[22] IPFS: article about IPFS"A Beginner's Guide to IPFS" URL: https://hackernoon.com/a-beginners-guide-to-ipfs-20673fedd3f

[23] INFURA: article about infura "Introducing Infura: Connecting DApps With Ethereum Without Setting up Ethereum Nodes" By Manish Misra
URL: https://dzone.com/articles/introducing-Infura-connecting-dapps-with-Ethereum

[24] GPG4win: a secure solution for file and email encryption
URL:https://www.gpg4win.org/

[25] Almulla, Sameera; Iraqi, Youssef; and Jones, Andrew, "A State-Of-The-Art Review of Cloud Forensics", Journal of Digital Forensics, Security and Law: Vol. 9:No. 4, Article 2, DOI: https://doi.org/10.15394/jdfsl.2014.1190,2014.

[26] A. Castiglione, G. Cattaneo, G. De Maio, A. De Santis and G. Roscigno, "A Novel Methodology to Acquire Live Big Data

Evidence from the Cloud", in IEEE Transactions on Big Data, doi: 10.1109/TBDATA.2017.2683521,2017.

[27] Bennett, Juan-Carlos & H. Diallo, Mamadou, "A Forensic Pattern-Based Approach for Investigations in Cloud System Environments", 1-8. 10.1109/CSNET.2018.8602908,2018.

[28] Santra P., Roy A., Majumder K, "A Comparative Analysis of Cloud Forensic Techniques in IaaS", In: Bhatia S., Mishra K., Tiwari S., Singh V. (eds) Advances in Computer and Computational Sciences. Advances in Intelligent Systems and Computing, vol 554. Springer, Singapore, 2018.

[29] Bhatia, Sugandh & Malhotra, Jyoteesh, "CSPCR: Cloud Security, Privacy and Compliance Readiness - A Trustworthy Framework." International Journal of Electrical and Computer Engineering. 8. 10.11591/ijece.v8i5.pp3756-3766, 2018.

[30] Hemdan E.ED., Manjaiah D.H., " Digital Forensic Approach for Investigation of Cybercrimes in Private Cloud Environment." In: Sa P., Bakshi S., Hatzilygeroudis I., Sahoo M. (eds) Recent Findings in Intelligent Computing Techniques. Advances in Intelligent Systems and Computing, vol 707. Springer, Singapore, 2019.

[31] Moussa, A.N., Ithnin, N. & Zainal,CFaaS: bilaterally agreed evidence collection", A. J Cloud Comp 7: 1. https://doi.org/10.1186/s13677-017-0102-3,2018

[32] Pichan, Ameer & Lazarescu, Mihai & Teng Soh, Sie, "Cloud forensics: Technical challenges, solutions and comparative analysis",Digital Investigatio. 13. 10.1016/j.diin.2015.03.002,2015.

[33] DykNetwork Forensicsstra, Josiah & Sherman, A.T, "Understanding Issues in cloud forensics: Two hypothetical case studies", Journal of . 3. 19-31,2011.

[34] Dykstra, Josiah & T. Sherman, Alan, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform" Digital Investigation. 10. S87–S95. 10.1016/j.diin.2013.06.010,2013.

[35] K. R. Choo, C. Esposito and A. Castiglione, "Evidence and Forensics in the Cloud: Challenges and Future Research Directions", In IEEE Cloud Computing, vol. 4, no. 3, pp. 14-19, 2017.