Secure Deployment of Decentralized Cloud in Blockchain Environment using Inter-Planetary File System

Mruthyunjaya Mendu, Dr. B Krishna, Sallauddin Mohmmad, Y Sharvani, Ch Vinay Kumar Reddy

1,4 Sumathi Reddy Institute of Technology for Women, Warangal, India.
2 Vaagdevi College of Engineering, Warangal, India.
3,5 SR Engineering College, Warangal, India.

1 mruthyunjay.m@gmail.com

Abstract: Nowadays, the entire globe with enormous resources is connected using web-based technologies. These integrations are implemented using an advanced network environment and need a higher degree of security and integrity. Most of the people are now using smart gadgets to access the corporate, social, and government services. The smart gadgets are having high performance operating systems including Android, iOS, Windows, Blackberry, Tizen, Lune OS, Kai OS, and many others. With the increase of such platforms, the need for security and integrity arises and because of this, the term "Blockchain" is getting huge prominence for multiple secured services. Blockchain was invented as the decentralised transaction chief of the Bitcoin crypto currency Satoshi Nakamoto was called in 2008 by an individual (or group of people). Satoshi Nakamoto's name appears to date uncertain. The blockchain inventor for Bitcoin made it the first digital currency to address the double dilemma without the need for a trustworthy regulator or a central server. This manuscript underlines the assorted features of the Inter-Planetary File System (IPFS) as the advanced implementation for a secured blockchain environment.

Keywords: Blockchain, Secured Blockchain, Decentralized Cloud

1. Introduction
A blockchain is a time-bound collection of unchanging data records which is operated by a network of computers that are not owned by any particular organisation. A data node (i.e. node) is protected by means of cryptographic principles (i.e., chain) [1, 2] and connected to one another.

In classical web applications, there is the deployment of a Centralized Web Server. These centralized web apps having a single server, cloud, or datacenter are deployed for many services including E-Governance, Medical Records Management, Academic Institutes, Corporate Sector, or any other services. In these traditional web-based applications deployed on centralized web servers, there are huge vulnerabilities.

In these scenarios, all other users or remote systems access the web services using their web client application. These web client applications include assorted web browsers. The major problem in this type of environment is the centralization in which if the server fails or hacked then the entire network environment gets compromised.
In deployments where only one server or few more replicated servers are deployed, if that is hacked then all data can be leaked out or can be copied or destroyed and this is the major issue with centralized servers. To avoid the issues with Centralized Servers, there is a specific implementation using the Decentralized Web. In a decentralized web, there is no central repository of data or applications. In Blockchain Technology, only a decentralized web is there. The data and applications are stored in multiple places and regions using blockchain technology to ensure security and privacy [4].

In the case of Blockchain Technology, is directly associated with the decentralization in which there are associations of Decentralized Apps or dApp. Decentralized Web, the data is stored on every node or system using that network. In the blockchain environment, there is no threat of data because the chain of nodes (blockchain) is immutable (unbreakable) and all blocks are interconnected with a dynamic hash (encrypted text). The chain block in the blockchain system is designed with high-performance protocols in such a way that it is unchangeable and cannot be compromised or changed by intruders or sniffers from third parties[5].

2. Decentralized Platforms for Blockchain Implementations
There are hundreds of distributed cloud platforms that can be used for blockchains. Following is the table of decentralized platforms for blockchain-based cloud integrations with the official URL.

| Decentralized Cloud | Official URL                  |
|---------------------|-------------------------------|
| IPFS                | ipfs.io                       |
| Sia                 | sia.tech                      |
| Storj               | storj.io                      |
| Iagon               | iagon.com                     |
| Cubbit              | cubbit.io                     |
| IExec               | iex.ec                        |
| PPIO                | pp.io                         |
| Opacity             | opacity.io                    |
| BTFS                | bittorrent.com/token/bittorrent-file-system |
| NeoFS               | fs.neo.org                    |
| Dfinity             | dfinity.org                   |
| Solana              | solana.com                    |
| Blockstack          | blockstack.org                |
| SafeNetwork         | safenetwork.tech              |

3. InterPlanetary File System (IPFS): Blockchain-Based Hypermedia Protocol with Peer-to-Peer Communication
URL: https://ipfs.io/
To work with the blockchain environment, there are separate file systems and protocols which are highly secured. One of the prominent Protocol and File System for Decentralized / Distributed Web / Distributed Cloud is IPFS - InterPlanetary File System. IPFS is a dedicated protocol for decentralized applications [6].
Figure 1: Advantages of IPFS over HTTP
(Source: Official Portal of IPFS https://ipfs.io)

In a traditional web-based environment, the web application or web service is accessed using HyperText Transfer Protocol (HTTP) like following

http://www.rediff.com
http://www.google.com
http://www.du.ac.in
or any other

In the case of Blockchain-based file system, the protocol of IPFS is used with a dynamic hash key with secured encryption as follows

ipfs://QmUDT1jRPuaiZYky1kfvoMWoWdFLqrJiuNDRvMvYc8ohW2
ipfs://QmUDT1jRPuaiZYky1kfvoMWoWdFLqrJiuNDRvMaYc8ohW2
or any other

By this method of using IPFS, the entire communication becomes secured and anonymous. The sender and receivers can communicate and share the documents in secured channels of blockchain [7, 8].
IPFS can be installed and implemented with following
IPFS Desktop
Command-line install
IPFS Companion for Browser
IPFS Cluster for Big Data and Server Deployments

In the variants of Go Language and JS-based Implementation the software versions of IPFS are available. These software updates have been used to build and run for corporate and large data applications in a private blockchain environment[9, 10]. Many blockchain based implementations use Go Language, which is high performance in several aspects including fast compile time, dynamic error testing, scalability.
IPFS encourages the creation of multifunctionally stable networks that enable sustained availability — with or without the Internet backbone. In developed countries, during natural disasters or just when you're in the wireless coffee shop, that means better connectivity.

IPFS uses the object itself to represent the client instead of a location key. This is achieved by using an encryption hash on a file and used as the password. The hash is a root object, and in its direction other objects can be identified. You get access to this "start point" of data instead of talking to a computer. This increases the physical closeness of the system. If someone close to me has what I want, instead of linking to a central computer, I can get it directly from them. The classroom students will take the data from each other in the lecture example from before without anyone needing to make a contact with the server. HTTP allows you to wonder where is a certain file, while IPFS wonders where a particular file is stored. IPFS puts together a few popular innovations from other peer-to-peer networks [11] to do this.

For many operating systems, the IPFS server edition is available and can be used for blockchain-based deployment. You can download it from https://github.com/ipfs-shipyard/ipfs-desktop to run IPFS on Windows Operating System.

![IPFS Dashboard and Status](image)

**Figure 4: Dashboard and Status of IPFS**

Following are the commands to install IPFS using prominent package managers

- **Chocolatey**: choco install ipfs-desktop
- **Homebrew**: brew cask install ipfs
- **Snap**: snap install ipfs-desktop

4. **Cloud Integration for Blockchain Scenarios**

The cloud integration of IPFS can be implemented using the Ethereum blockchain platform and to have a higher degree of security in overall communication networks [12-14]. Once IPFS is integrated, then the dashboard is displayed and is used to share the files on the blockchain network as follows
Using this approach, the entire communication in IPFS based blockchain environment shall be fully secured and all the addresses shall be encrypted[15-18]. As in Figure, the address of file ss.txt is having a unique encrypted hash address with the prefix Qm. The remaining part of the address denotes the assorted properties of the file. This way of communication in the blockchain using IPFS shall be encrypted and with a base of peer-to-peer communication with higher integrity and security.

5. Conclusion

There is a huge scope of research in blockchain technologies for the research scholars, professors, and practitioners. As E-Governance is one of the very common services that are in the targets of hackers, crackers, and sniffers, these platforms can be secured using advanced decentralized cloud integrations. On the deployment of these services on decentralized clouds, the performance evaluation and comparison with the traditional web environment can be done. Besides, this type of implementation shall avoid the scope of corruption in web-based services because there will be no single administrator and all the communications will be transparent without any scope of manual or accidental modifications in the records.

6. References

[1] Sharma, P K, Chen, M Y, & Park, J H (2017) A software defined fog node based distributed blockchain cloud architecture for IoT Ieee Access, 6 115-124
[2] Li, Z, Barenji, A V, & Huang, G Q (2018) Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform Robotics and Computer-Integrated Manufacturing, 54 133-144
[3] Tosh, D K, Shetty, S, Liang, X, Kamhoua, C A, Kwiat, K A, & Njilla, L (2017, May) Security implications of blockchain cloud with analysis of block withholding attack In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID) (pp 458-467) IEEE
[4] Esposito, C, De Santis, A, Tortora, G, Chang, H, & Choo, K K R (2018) Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31-37
[5] Xia, Q, Sifah, E B, Smahi, A, Amofa, S, & Zhang, X (2017) BBDS: Blockchain-based data sharing for electronic medical records in cloud environments Information, 8(2) 44
[6] Samaniego, M, Jamsrandorj, U, & Deters, R (2016, December) Blockchain as a Service for IoT In 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) (pp 433-436) IEEE
[7] Liu, H, Zhang, Y, & Yang, T (2018) Blockchain-enabled security in electric vehicles cloud and edge computing IEEE Network, 32(3) 78-83
[8] Zhang, Y, Deng, R H, Liu, X, & Zheng, D (2018) Blockchain based efficient and robust fair payment for outsourcing services in cloud computing Information Sciences, 462 262-277
[9] Wang, H, & Song, Y (2018) Secure cloud-based EHR system using attribute-based cryptosystem and blockchain Journal of medical systems, 42(8) 152
[10] Zheng, Q, Li, Y, Chen, P, & Dong, X (2018, December) An innovative IPFS-based storage model for blockchain In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI) (pp 704-708) IEEE
[11] Ali, M S, Dolui, K, & Antonelli, F (2017, October) IoT data privacy via blockchains and IPFS In Proceedings of the seventh international conference on the internet of things (pp 1-7)
[12] Nizamuddin, N, Hasan, H R, & Salah, K (2018, June) IPFS-blockchain-based authenticity of online publications In International Conference on Blockchain (pp 199-212) Springer, Cham
[13] Mounika, S & Sampath Kumar, T 2019, "Client –requirement fulfil QOS in multi server for max beneficial in cloud computing", International Journal of Advanced Science and Technology, vol 28 no 7 pp 44-49
[14] Mahender K, Kumar TA and Ramesh KS 2019 Simple transmit diversity techniques for wireless communications Advances in Intelligent Systems and Computing 669 329-342 10.1007/978-981-10-8968-8_28
[15] Rajasri I, Guptha AVSSKS and Rao YVD 2013 A Comparative Study of a Few Tests for Isomorphism in Planetary gear trains International Journal of Engineering and Technology Innovation 3(2) 95-103
[16] Monelli, A &Sriramoju, SB 2019, "An overview of the challenges and applications towards web mining", Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018 pp 127
[17] Sudarshan E, Naik K.S, Kumar P.P 2020 Parallel approach for backward coding of wavelet trees with CUDA. ARPN Journal of Engineering and Applied Sciences 15(9), pp.1094-1100
[18] Mohmmad S, Ramesh D, Pasha SN, Shabana and Shankar K 2019 Research on new network architecture through SD-WAN International Journal of Innovative Technology and Exploring Engineering 8(6 Special Issue 4) 483-490 10.35940/ijitee.f1101.0486s419
Secure Deployment of Decentralized Cloud in Blockchain Environment using Inter-Planetary File System

Mruthyunjaya Mendu¹, Dr.B Krishna², Sallauddin Mohmmad³, Y Sharvani⁴, Ch Vinay Kumar Reddy⁵

¹,⁴Sumathi Reddy Institute of Technology for Women, Warangal, India.
²Vaagdevi College of Engineering, Warangal, India.
³,⁵SR Engineering College, Warangal, India.

¹mruthyunjay.m@gmail.com

Abstract: Nowadays, the entire globe with enormous resources is connected using web-based technologies. These integrations are implemented using an advanced network environment and need a higher degree of security and integrity. Most of the people are now using smart gadgets to access the corporate, social, and government services. The smart gadgets are having high performance operating systems including Android, iOS, Windows, Blackberry, Tizen, Lune OS, Kai OS, and many others. With the increase of such platforms, the need for security and integrity arises and because of this, the term "Blockchain" is getting huge prominence for multiple secured services. Blockchain was invented as the decentralised transaction chief of the Bitcoin crypto currency Satoshi Nakamoto was called in 2008 by a individual (or group of people). Satoshi Nakamoto's name appears to date uncertain. The blockchain inventor for Bitcoin made it the first digital currency to address the double dilemma without the need for a trustworthy regulator or a central server. This manuscript underlines the assorted features of the Inter-Planetary File System (IPFS) as the advanced implementation for a secured blockchain environment.

Keywords: Blockchain, Secured Blockchain, Decentralized Cloud

1. Introduction
A blockchain is a time-bound collection of unchanging data records which is operated by a network of computers that are not owned by any particular organisation. A data node (i.e. node) is protected by means of cryptographic principles (i.e., chain) [¹, ²] and connected to one another.

In classical web applications, there is the deployment of a Centralized Web Server. These centralized web apps having a single server, cloud, or datacenter are deployed for many services including E-Governance, Medical Records Management, Academic Institutes, Corporate Sector, or any other services. In these traditional web-based applications deployed on centralized web servers, there are huge vulnerabilities.

In these scenarios, all other users or remote systems access the web services using their web client application. These web client applications include assorted web browsers. The major problem in this type of environment is the centralization in which if the server fails or hacked then the entire network environment gets compromised.
In deployments where only one server or few more replicated servers are deployed, if that is hacked then all data can be leaked out or can be copied or destroyed and this is the major issue with centralized servers. To avoid the issues with Centralized Servers, there is a specific implementation using the Decentralized Web. In a decentralized web, there is no central repository of data or applications. In Blockchain Technology, only a decentralized web is there. The data and applications are stored in multiple places and regions using blockchain technology to ensure security and privacy [4].

In the case of Blockchain Technology, is directly associated with the decentralization in which there are associations of Decentralized Apps or dApp. Decentralized Web, the data is stored on every node or system using that network. In the blockchain environment, there is no threat of data because the chain of nodes (blockchain) is immutable (unbreakable) and all blocks are interconnected with a dynamic hash (encrypted text). The chain block in the blockchain system is designed with high-performance protocols in such a way that it is unchangeable and cannot be compromised or changed by intruders or sniffers from third parties[5].

2. Decentralized Platforms for Blockchain Implementations
There are hundreds of distributed cloud platforms that can be used for blockchains. Following is the table of decentralized platforms for blockchain-based cloud integrations with the official URL.

| Decentralized Cloud | Official URL                      |
|---------------------|----------------------------------|
| IPFS                | ipfs.io                          |
| Sia                 | sia.tech                         |
| Storj               | storj.io                         |
| Iagon               | iagon.com                        |
| Cubbit              | cubbit.io                        |
| IExec               | iex.ec                           |
| PPIO                | pp.io                            |
| Opacity             | opacity.io                       |
| BTFS                | bittorrent.com/token/bittorrent-file-system |
| NeoFS               | fs.neo.org                       |
| Dfinity             | dfinity.org                      |
| Solana              | solana.com                       |
| Blockstack          | blockstack.org                   |
| SafeNetwork         | safenetwork.tech                 |

3. InterPlanetary File System (IPFS): Blockchain-Based Hypermedia Protocol with Peer-to-Peer Communication
URL: https://ipfs.io/
To work with the blockchain environment, there are separate file systems and protocols which are highly secured. One of the prominent Protocol and File System for Decentralized / Distributed Web / Distributed Cloud is IPFS - InterPlanetary File System. IPFS is a dedicated protocol for decentralized applications [6].
In a traditional web-based environment, the web application or web service is accessed using HyperText Transfer Protocol (HTTP) like following:
- http://www.rediff.com
- http://www.google.com
- http://www.du.ac.in
or any other

In the case of Blockchain-based file system, the protocol of IPFS is used with a dynamic hash key with secured encryption as follows:
- ipfs://QmUDT1jRPuaiZYky1kfvoMWOwDFlqRjJuNDRvMyYeYc8ohW2
- ipfs://QmUDT1jRPuaiZYky1kfvoMWOwDFlqRjJuNDRvMaYc8ohW2
or any other

By this method of using IPFS, the entire communication becomes secured and anonymous. The sender and receivers can communicate and share the documents in secured channels of blockchain [7, 8].
IPFS can be installed and implemented with following
IPFS Desktop
Command-line install
IPFS Companion for Browser
IPFS Cluster for Big Data and Server Deployments

In the variants of Go Language and JS-based Implementation the software versions of IPFS are available. These software updates have been used to build and run for corporate and large data applications in a private blockchain environment[9, 10]. Many blockchain based implementations use Go Language, which is high performance in several aspects including fast compile time, dynamic error testing, scalability.
IPFS encourages the creation of multifunctionally stable networks that enable sustained availability — with or without the Internet backbone. In developed countries, during natural disasters or just when you're in the wireless coffee shop, that means better connectivity.

IPFS uses the object itself to represent the client instead of a location key. This is achieved by using an encryption hash on a file and used as the password. The hash is a root object, and in its direction other objects can be identified. You get access to this “start point” of data instead of talking to a computer. This increases the physical closeness of the system. If someone close to me has what I want, instead of linking to a central computer, I can get it directly from them. The classroom students will take the data from each other in the lecture example from before without anyone needing to make a contact with the server. HTTP allows you to wonder where is a certain file, while IPFS wonders where a particular file is stored. IPFS puts together a few popular innovations from other peer-to-peer networks [11] to do this.

For many operating systems, the IPFS server edition is available and can be used for blockchain-based deployment. You can download it from https://github.com/ipfs-shipyards/ipfs-desktop to run IPFS on Windows Operating System.

![Figure 4: Dashboard and Status of IPFS](image)

Following are the commands to install IPFS using prominent package managers:

- **Chocolatey**: `choco install ipfs-desktop`
- **Homebrew**: `brew cask install ipfs`
- **Snap**: `snap install ipfs-desktop`

4. **Cloud Integration for Blockchain Scenarios**
   The cloud integration of IPFS can be implemented using the Ethereum blockchain platform and to have a higher degree of security in overall communication networks [12-14]. Once IPFS is integrated, then the dashboard is displayed and is used to share the files on the blockchain network as follows.
Using this approach, the entire communication in IPFS based blockchain environment shall be fully secured and all the addresses shall be encrypted [15-18]. As in Figure, the address of file ss.txt is having a unique encrypted hash address with the prefix Qm. The remaining part of the address denotes the assorted properties of the file. This way of communication in the blockchain using IPFS shall be encrypted and with a base of peer-to-peer communication with higher integrity and security.

5. Conclusion
There is a huge scope of research in blockchain technologies for the research scholars, professors, and practitioners. As E-Governance is one of the very common services that are in the targets of hackers, crackers, and sniffers, these platforms can be secured using advanced decentralized cloud integrations. On the deployment of these services on decentralized clouds, the performance evaluation and comparison with the traditional web environment can be done. Besides, this type of implementation shall avoid the scope of corruption in web-based services because there will be no single administrator and all the communications will be transparent without any scope of manual or accidental modifications in the records.

6. References
[1] Sharma, P K, Chen, M Y, & Park, J H (2017) A software defined fog node based distributed blockchain cloud architecture for IoT Ieee Access, 6 115-124
[2] Li, Z, Barenji, A V, & Huang, G Q (2018) Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform Robotics and Computer-Integrated Manufacturing, 54 133-144
[3] Tosh, D K, Shetty, S, Liang, X, Kamhoua, C A, Kwiat, K A, & Njilla, L (2017, May) Security implications of blockchain cloud with analysis of block withholding attack In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID) (pp 458-467) IEEE
[4] Esposito, C, De Santis, A, Tortora, G, Chang, H, & Choo, K K R (2018) Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31-37
[5] Xia, Q, Sifah, E B, Smahi, A, Amofa, S, & Zhang, X (2017) BBDS: Blockchain-based data sharing for electronic medical records in cloud environments Information, 8(2) 44
[6] Samaniego, M, Jamsrandorj, U, & Deters, R (2016, December) Blockchain as a Service for IoT In 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSSCom) and IEEE smart data (SmartData) (pp 433-436) IEEE
[7] Liu, H, Zhang, Y, & Yang, T (2018) Blockchain-enabled security in electric vehicles cloud and edge computing IEEE Network, 32(3) 78-83
[8] Zhang, Y, Deng, R H, Liu, X, & Zheng, D (2018) Blockchain based efficient and robust fair payment for outsourcing services in cloud computing Information Sciences, 462 262-277
[9] Wang, H, & Song, Y (2018) Secure cloud-based EHR system using attribute-based cryptosystem and blockchain Journal of medical systems, 42(8) 152
[10] Zheng, Q, Li, Y, Chen, P, & Dong, X (2018, December) An innovative IPFS-based storage model for blockchain In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI) (pp 704-708) IEEE
[11] Ali, M S, Dolui, K, & Antonelli, F (2017, October) IoT data privacy via blockchains and IPFS In Proceedings of the seventh international conference on the internet of things (pp 1-7)
[12] Nizamuddin, N, Hasan, H R, & Salah, K (2018, June) IPFS-blockchain-based authenticity of online publications In International Conference on Blockchain (pp 199-212) Springer, Cham
[13] Mounika, S & Sampath Kumar, T 2019, "Client –requirement fulfil QOS in multi server for max beneficial in cloud computing", International Journal of Advanced Science and Technology, vol 28 no 7 pp 44-49
[14] Mahender K, Kumar TA and Ramesh KS 2019 Simple transmit diversity techniques for wireless communications Advances in Intelligent Systems and Computing 669 329-342 10.1007/978-981-10-8968-8_28
[15] Rajasri I, Gupta AVSSKS and Rao YVD 2013 A Comparative Study of a Few Tests for Isomorphism in Planetary gear trains International Journal of Engineering and Technology Innovation 3(2) 95-103
[16] Monelli, A &Sriramoju, SB 2019, "An overview of the challenges and applications towards web mining", Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018 pp 127
[17] Sudarshan E, Naik K.S, Kumar P.P 2020 Parallel approach for backward coding of wavelet trees with CUDA. ARPN Journal of Engineering and Applied Sciences 15(9), pp.1094-1100
[18] Mohmmad S, Ramesh D, Pasha SN, Shabana and Shankar K 2019 Research on new network architecture through SD-WAN International Journal of Innovative Technology and Exploring Engineering 8(6 Special Issue 4) 483-490 10.35940/ijitee.f1101.0486s419