National College of Ireland

Enhancing Authorization and Authentication in Cloud Services using Blockchain

MSc Research Project
MSc in Cyber Security

Prateek Pulastya
X21112541

School of Computing
National College of Ireland

Supervisor: Dr Vanessa Ayala-Rivera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Prateek Pulastya		
Student ID:	x21112541		
Programme:	MSc in Cyber Security	**Year:**	2022-2023
Module:	MSc Research Project		
Supervisor:	Dr Vanessa Ayala-Rivera		
Submission Due Date:	15/12/2022		
Project Title:	Enhancing Authorization and Authentication in Cloud Services using Blockchain		
Word Count:	6921	**Page Count:**	21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Prateek Pulastya

Date: 15/12/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Authorization and Authentication in Cloud Services using Blockchain

Prateek Pulastya
x21112541

Abstract

Cloud computing environments have been growing in popularity, and many organizations are completely shifting to cloud computing for storing important data and accessing the cloud's high computing capabilities. But one main problem associated with the cloud is security. Cyber-attacks on the cloud can result in the loss of critical data, and many organizations and individuals are storing the data in an environment provided by a third party. So, a system that can provide efficient security to the cloud is proposed in this approach. Blockchain technology will be used to provide security to the cloud environment. The blockchain will use the private and public keys generated during the creation of the blockchain to improve the authentication, authorization, and access control of the cloud environment. The system will be implemented in the form of a web application that can be used by the users to save data to the cloud. Amazon Web Services (AWS) will be used as cloud storage. The results of the study reveal that blockchain technology can enhance the authentication, authorization, and access control of the cloud environment.

1 Introduction

Cloud computing deals with accessing the processing and the data storage power of a system online. Cloud computing is flexible and cost effective and is an effective solution for several internet services (Nepal et al., 2011). Without investing in new infrastructure, hiring new IT staff, or buying new licensed software that are necessary for the automation of numerous operations, cloud computing helps enterprises increase their capacity dynamically. Cloud computing has grown from being a promising business idea, in its initial years of conception, to one of the most used technologies in the IT industry. Several organizations have turned to cloud computing as it helps them reduce the cost of infrastructure and provides them quick access to applications. By using cloud computing an organization can sell and rent its computing prowess (Mell and Grance, 2011). Six out of ten organizations have moved their workload to the cloud in 2022 and as the cloud computing market grows this number is likely to increase (Bulao, 2020). Cloud is most suited for organizations whose customers demand a growing or fluctuating bandwidth as cloud services can be scaled up or down based on demand. This flexibility associated with cloud services allows organizations to work efficiently by using the resources provided by the cloud. Even with all these advantages organizations adopting cloud services remain cautious and some organizations are still hesitant to move to cloud services.

The main reason for this is security concerns over storing data in the cloud storage as the data that an organization may store in the cloud may be sensitive and important to the working of the company. So, any cyber-attack on the cloud will result in the organization losing its important data which may even threaten the existence of the organization. The instances of cyber-attacks are increasing daily and the underlying technologies in cloud computing have made the security concerns complex. An organization or person may also have a concern

about confidentiality as they might feel that they have lost control of their data when it is stored in a storage space provided by a cloud service provider. A wide range of cyber-attacks is likely to occur in a cloud infrastructure. These attacks range from simple attacks due to the ignorance or negligence of a user to complex attacks like APT's (Vance, 2014). Virtualization, a defining characteristic of cloud computing will also be under threat as the cyber-attacks on virtual machines in the cloud might be more complicated than attacks on physical data storage infrastructure. So, it is important to ensure that the data provided by an organization or a user to a cloud service provider is confidential and can only be accessed by the legitimate users or organizations who are the owners of the data. It is also important to ensure that the data is stored in a safe environment in which an instance of cyber-attack can be identified.

Block chain technology is a decentralized framework having a distributed computing paradigm. It is based on the decentralization P2P architecture. In this architecture all nodes are equal and no center for control exists. Blockchain technology has a number of benefits associated with it. The first one being that a third-party service provider no longer needs to be trusted as damages to a few nodes will not affect the robustness of the entire system. Another benefit of the block chain technology is that the data record and rules are open, transparent, and traceable. Also, the data structure in the form of a chain and the consensus mechanism ensures security and integrity (Li et al., 2021).

The decentralized model of the block chain can be used in the creation of a trust enabled cloud environment were a user or organization will be able to provide a cloud service provider their data without having to fully trust the service provider as the cloud environment will be a based on a decentralized block chain model (Yin et al., 2021). So, it is important to study the effectiveness of the block chain technology in making the cloud storage more secure and such a study will be performed here. For finding out the security offered by a block chain model a web application will be created here.

This web application will allow the users to store their data in a cloud storage service offered by a third-party service provider and the data stored in the cloud will only be accessible to the person storing or uploading the data to the cloud. The legitimacy of the user will also be determined before they can create an account in the web application. The implementation of this web application will help in understanding the effectiveness of the block chain technology in securing data and ensuring confidentiality.

1.1 Research questions

- To what extend are the processes of authentication, authorization and access control enhanced in cloud services when blockchain is used?

1.2 Contribution

- A web application using Blockchain that can be used for uploading a file to a cloud storage in a secure manner.

The contents of the report will be arranged in the following sections after Section 1.

Section 2 discusses the existing literature related to the methods used for securing cloud infrastructures. Section 3 explains the methods followed for implementing the web application and the block chain technology on the web application will be discussed in this

section. Section 4 explains the underlying framework used for creating the web application and implementing the block chain technology will be discussed here along with the final implementation and form of the web application. Section 5 discusses the main findings from the study. Section 6 provides an overview of the study and the results obtained from the study will be defined in this section along with the enhancements that can be made to the study in the future.

2 Related Work

2.1 Authentication

Authentication issues and authentication mechanisms in cloud were studied in approaches like (Najib EL KAMOUN, 2017). The details about several authentication techniques were studied in this approach. Several encryption techniques like CAPTCHA based, encryption based, password based etc., were studied in this approach. The importance of authentication in a cloud environment was highlighted in this approach. Another survey-based approach studied the authentication techniques based on biometrics (Alsultan et al., 2019). This approach also focused on providing security to the cloud. The main limitation of these approaches is that these were merely a survey of different authentication techniques.

Cryptography based methods were used for user authentication in several approaches. Cryptographic techniques like Advanced Encryption Standard (AES) and elliptic curve cryptography (ECC) were used in these approaches. Two factor authentication, AES encryption for securing the data stored in cloud, admin verification of users, distributed database storage was performed in (Kumar et al., 2020). The weakness in security and functionality of authentication techniques in cloud computing was discussed in (Lee et al., 2021). The ECC based three factor authentication was also proposed in this approach for overcoming the security problems associated with authentication. The results from these studies reveal that the use of encryption for securing data and user authentication is highly effective in providing security to the cloud environment. But these cryptographic approaches can be studied by attackers for finding out a way to bypass the security provided by these techniques and if the attackers are able to figure out the key generation mechanism of these techniques, these techniques will become ineffective.

2.2 Authorization

Existing authorization techniques in cloud environment and the effectiveness of these techniques were studied in (Masood et al., 2015). The survey method for studying authorization techniques were also studied in (Mohammad, 2022). Both survey-based approaches studied several authorization frameworks and access control models. Some limitations are associated with these approaches. One main limitation is that these two approaches are just surveys on existing authorization techniques and none of the techniques discussed in the surveys are implemented in both approaches. Another limitation is that some of the requirements and basics of access control in clouds have not been considered in these approaches.

An identity management mechanism was proposed as a solution for cloud security in (Dr. Chandra Jadala, 2019). The approach proposed here was based on protocols for performing authorization and allowing communication across applications using tokens instead of the

credentials of a person. The Microsoft Azure active directory will be used for the authentication in this approach. The use of authentication of a user is shown to be effective for providing security to a cloud environment. Also, the using an administrator to monitor security is shown to be effective. The main limitation of this approach is the use of Azure AD which has disadvantages like the complexity, complicated pricing and the lack of efficient support provided by Microsoft.

2.3 Blockchain

The application of Block chain for security in cloud computing is studied in (Ashok Gupta et al, 2019). The characteristics of block chain and the security requirements of cloud are discussed in this approach. This ability of the block chain technology is also studied in (Sanghi et al., 2018). The methodologies used in block chain like the private key cryptography, protocol and distributed network is discussed and the use of these methods for providing security to cloud environments is also discussed in (Sanghi et al., 2018). For providing security to the cloud the generation of a private key for the authentication of a user in an application has been shown to be effective from the observations in (Mendki, 2021). This approach of studying the capabilities of the block chain technology was again performed in several approaches (Pavithra, Ramya, and Prathibha, 2019; Rouhani and Deters, 2019; Dar et al., 2020). The observations from all these approaches showed that the block chain technology was highly effective providing security to the cloud. The abilities of the blockchain technology to provide identity management, access control to the cloud services were highlighted in these approaches. The main limitation of all these studies is that none of these studies implemented the security frameworks based on blockchain for studying about its effectiveness or proposed any techniques as most of these approaches were surveys that studied the security that the blockchain technology provided in the cloud environment.

Block chain was observed to perform authentication effectively in cloud services based on the observations from (Ghaffari et al., 2020; Khieu and Moh, 2019). It was observed from these approaches that blockchain was better than traditional methods for providing security to the cloud. The approach by Khieu and Moh, (2019) showed that the use of public key in a decentralized increased the security. The blockchain was implemented in Khieu and Moh, (2019) while it was not implanted in Ghaffari et al., (2020).

Many approaches implemented the blockchain frameworks for studying the ability of the blockchain to provide security to the cloud environment or proposed new techniques based on blockchain. A block chain-based method for securing the cloud using verifiable data access control is proposed in (LI, 2022). The block chain components in this approach are used for identifying the suspicious behavior in a cloud environment. The effectiveness of the policy used in this approach is analyzed by exposing it to the scenario of an attack like Eclipse attack. A novel identity and access management system that belongs to FaaS is proposed in (Alansari et al., 2017). The system proposed in this approach can be used by federated organizations for enforcing access control policies based on attributes for preserving the privacy of their data. Blockchain is used along with the Intel SGX hardware platform for guaranteeing the integrity associated with the policy evaluation in this approach. A multi-blockchain access control architecture was used for access control in (Ajay et al., 2022). The access control architecture used a lightweight privacy protection named Authorization-Privacy. The account address belonging to a node in the blockchain was

chosen as the unique id and admission permission is also defined at the same time of the creation of the id and stored in the blockchain. Although the approaches mentioned here implemented several security frameworks none of these approaches were completely effective and the results or observations from these approaches were not studied in an advanced manner.

Problems related to security like authorization and access control in IoT networks have been tackled using the blockchain framework in (Chinnasamy et al., 2021), just like this approach blockchain technology was used for providing security in a number of approaches like (Algarni et al., 2021; Tapas, Merlino and Longo, 2018). Observations from these approaches reveal that the block chain technology was remarkably effective in providing security to the data in IoT environments. Tapas found it, Merlino and Longo, (2018) that the Ganache performs better than other techniques like TestRPC for adding delegation and access validation. The main limitation of these approaches was that that these approaches focused on the security in IoT environments while the effectiveness of blockchain in other environments were not studied in these approaches.

The ciphertext-policy attribute-based encryption (CP-ABE) was used along with the blockchain for providing security to cloud environments in (Sukhodolskiy and Zapechnikov, 2018; Son et al., 2020). The CP-ABE was also used for adding a temporal dimension to file sharing in an approach involving block chain technology (Jemel and Serhrouchni, 2017). The effectiveness of the block chain technology in providing security was again observed from these approaches. The main limitation of these approaches was the use of the complex CP-ABE algorithm for performing encryption.

2.4 Summary

The study of the existing literature focused on the ability of the block chain technology to implement access control, authorization, and authentication. Several approaches have studied the effectiveness of the block chain technology in implementing access control, authentication, authorization, and the use of blockchain in a cloud environment but all these approaches have not implemented the blockchain technology in any form or with the cloud environment. The use of a public key and private key for authentication was observed to be highly effective. The Ganache was also observed to be better than other method for creating blockchains. Some studies did not effectively study the result obtained from the studies that were performed. Several existing techniques for authentication and authorization were also studied. From studies based on blockchain it was observed that the blockchain technology was better than traditional methods like cryptography.

As most of the existing literature that studied the effect of blockchain on the security of the cloud environment did not perform any implementation of the block chain as system will developed in this approach where the blockchain will be implemented in the cloud environment. A web application will be developed which can be used for uploading files to a cloud storage. The authentication, authorization and access control will be performed using block chain. Ganache will be used for implementing the blockchain and the web application will be developed using the Python framework Django.

3 Research Methodology

3.1 Overall working

The overall system developed here consists of a web application and a blockchain framework. The web application and the blockchain was created separately and then integrated (Figure (1)). The authentication, authorization and access control were implemented by the blockchain, the admin also performed authentication while the users of the web application had access control over the data that they had uploaded to the cloud storage.

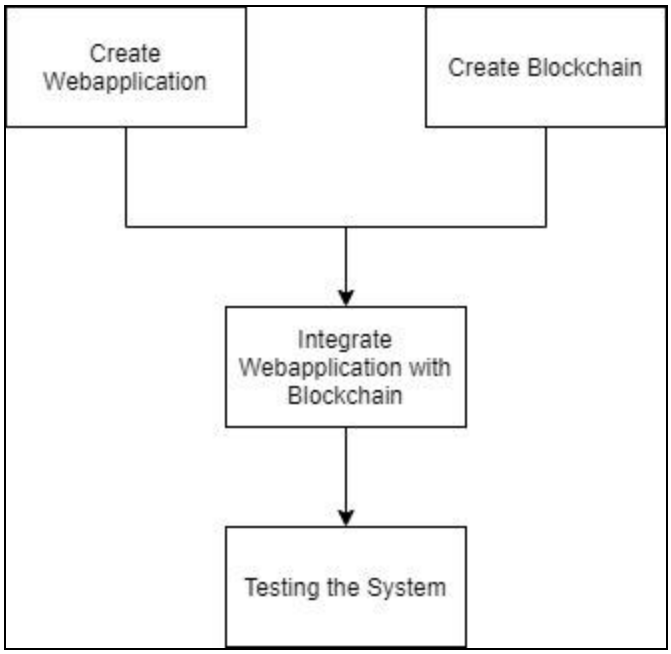

Figure (1): The overall working

3.2 Web application

The web application was created first. The web application has an MVT model and consists of a user side and a server side. The web application has two user roles: the admin and the user. The admin is the administrator of the web application, and the user is a normal user of the web application. The admin only can monitor the web application while the users can upload a file into the cloud storage. For using the web application, the users must first register or create an account in the web application while the admin has access to the web application without creating an account. The users can use the web application by signing into the web application using the username and password that they have used for creating an account while the admin was provided a default username and password for logging into the web application. The users can upload a file to the cloud storage, view the files that they have uploaded and download the previously uploaded files. The admin has the responsibility of approving the request of the user for creating an account in the web application. The user can only use the web application after the admin has approved their request.

3.3 Blockchain

3.3.1 Authentication

Determining whether a person, or organization is permitted to access a particular system or organization is what an authentication procedure entails. It can be done by determining if the credentials of a person trying to access the system matches with the valid credentials provided by the user to the system. This ensures that no unauthorized person will gain access to the system.

In the web application developed here the authentication was performed when the user registers or creates an account in the web application. Every user who had permission to access the web application was given a public key which was created when the nodes were created for the blockchain. For registration, the user must provide a username, password, and the public key, that they were provided, as input. The user was only registered when the admin performs validation. The admin was able to see all the request for registration from the users and the validation was performed by determining if the public key entered by the user corresponds to a private key which was created when a node is created in the blockchain. If a private key corresponding to the public key was found that user was registered and the users whose public key does not match any private key were not given access to the web application. So only the authorized users who should have access to the web application were found out.

3.3.2 Access control

Access control enables only the owner of the data to view the data uploaded to the cloud. Access control helps in preventing unauthorized people to have access to the data uploaded by a user and this will minimize the risk of data breach occurring.

The access control was performed here using the username of the user and the private key. After registration, the user was be provided the private key as this private key is required while uploading the file to the cloud. So, for uploading the file, the file to be uploaded is selected and the private key provided to the user was also provided as input. Before the completion of the file upload to the cloud it was determined if the private key entered by the user corresponds to the public key that was given by the specific user at the time of registration, this ensures that no one other than the specific user was able to access the resources of the cloud for storing files. The users can also download and view the previously uploaded files. For downloading the files also, the users must provide the private key assigned to them and before the download it was determined if the private key entered by the user corresponds to the public key given by the user at the time of registration. This means that the files uploaded by a person can only be accessible to that person only and no other person even if they somehow get the access to the account of the person will not be able to access the files without knowing the private key assigned to the user. Each user was able to view only the files uploaded by them and these files cannot be accessed by any other person and can only be accessed by the person who uploaded the files to the cloud. This is done using the username of the user which was stored during the file upload. This will allow data to be accessed by only the owners of the data.

3.3.3 Authorization

Authorization determines the level of access privileges, and it works in accordance with the access control. The authorization works based on access rules and these access rules were set based on the access control. The access rules will be set when the files are uploaded and only a person authorized to access the data in this case a file has access to the file.

3.3.4 Block

Blocks are the containers of information in the blockchain. Blocks will be added when information is added to the blockchain. Here, blocks containing two kinds of information were created. One kind of block contained the details of the user whose request for registration has been validated i.e., the username, password, and public key along with a timestamp that indicates the time at which the block was created. All blocks contain a timestamp based on the time it was created. The other kind of block contains the data added when a file was uploaded i.e., the name of the user, the private key, the name of the file and a file id which was automatically created along with the time stamp of the block.

3.3.5 Smart contract

Smart contracts are programs that run automatically based on the satisfaction of a pre-determined condition. Here, the smart contract consists of the steps to be followed for uploading the blocks. So, the smart contract contains the code to store the username, password, and public key of a user to a block only when the public key entered by the user at the time of registration was found to be in accordance with a private key created in the block chain, during validation by the admin. The smart contract also contains the code about the data to be added to a block when a file is uploaded to the cloud by a user.

4 Design and implementation

4.1 Design

The nodes of the blockchain were be created using the Ganache-truffle suite workspace. The ganache is a component present in the Truffle suite framework. Truffle functioned as the environment for development, framework for testing and pipelines for assets. The ganache can be defined as a development tool used for running a local blockchain network for creating decentralized applications. The ganache offers a safe and deterministic environment for the creation, testing and the deployment of smart contracts. Using the Ganache will help in saving time and money during the development of block chains (Weston, 2022). The Ganache will also offer flexibility for the faster uploading of the smart contract. Ten nodes were created by default when a blockchain was created in the Ganache-truffle suite workspace. Each node contains a specific private key and a public key corresponding to the private key. The blockchain also consisted of blocks which were uploaded when a data is added. The data to be added to the blocks was determined by the algorithm in the smart contract. Amazon web service (AWS) was used as the cloud storage for storing the data.

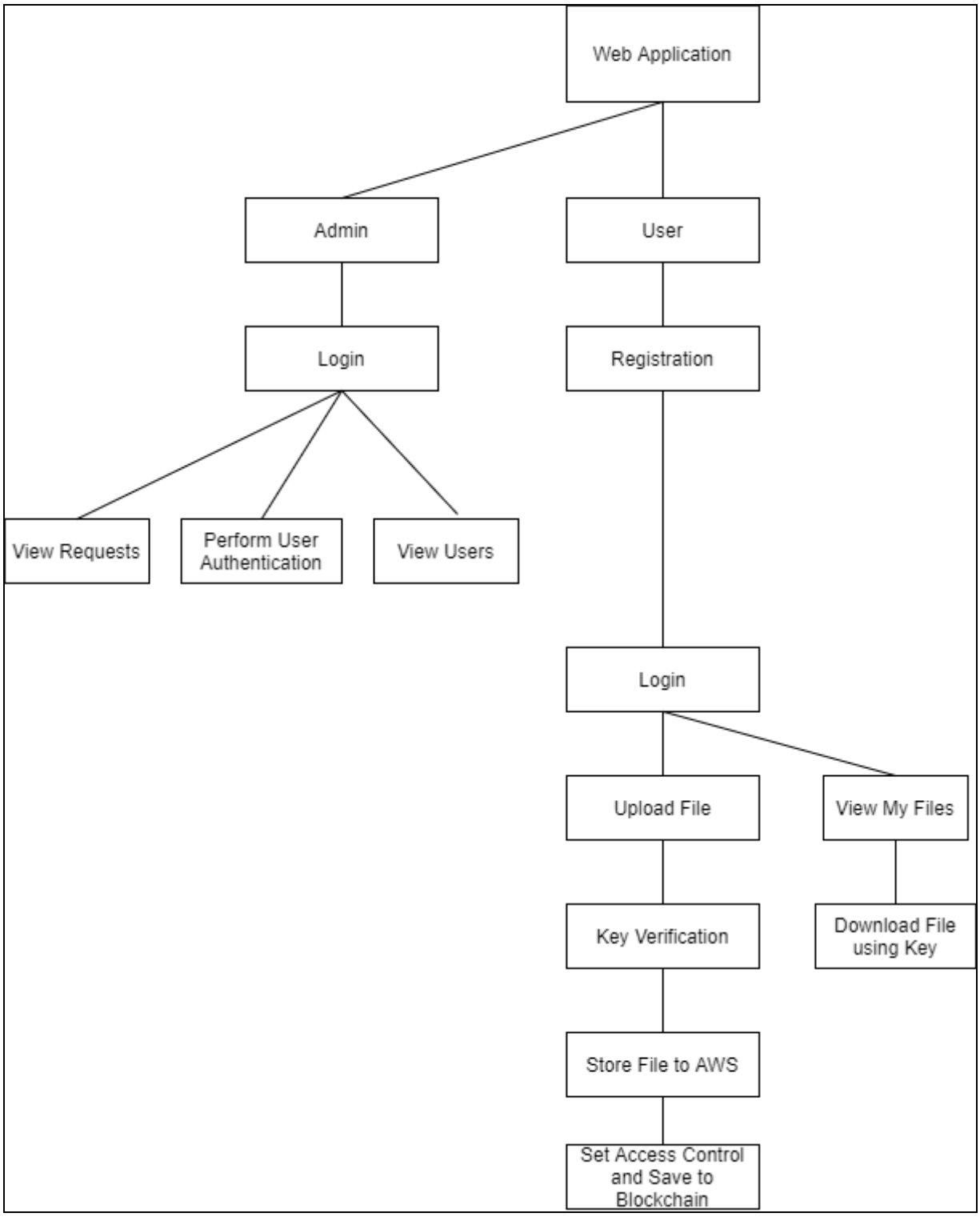

Figure (2): Architecture of the system

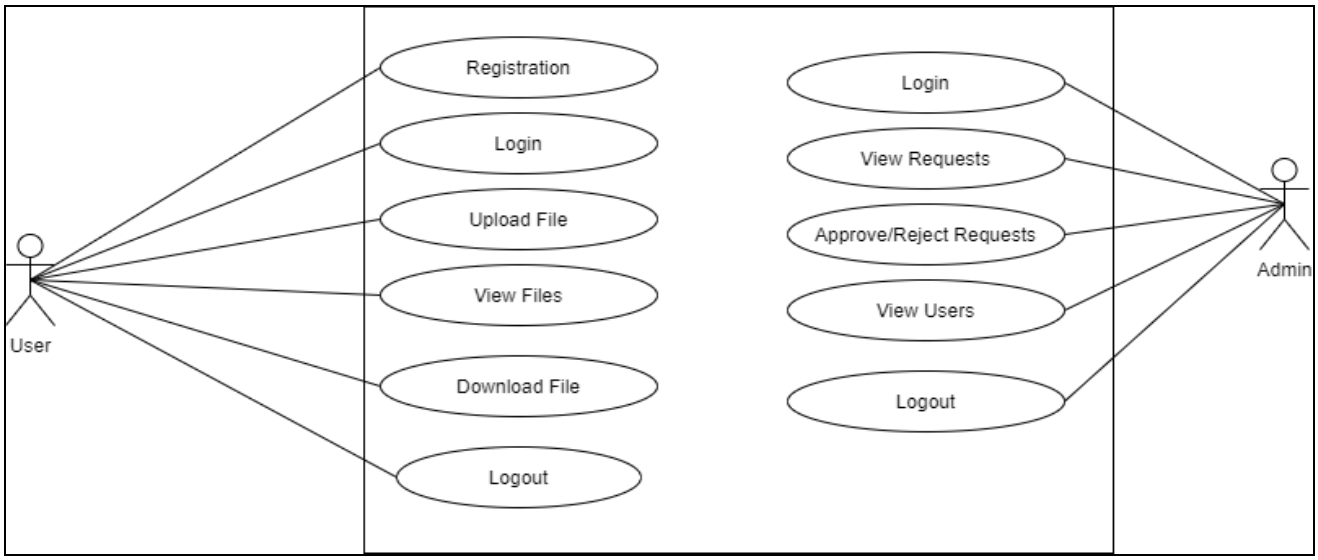

Figure (3): Use-case diagram

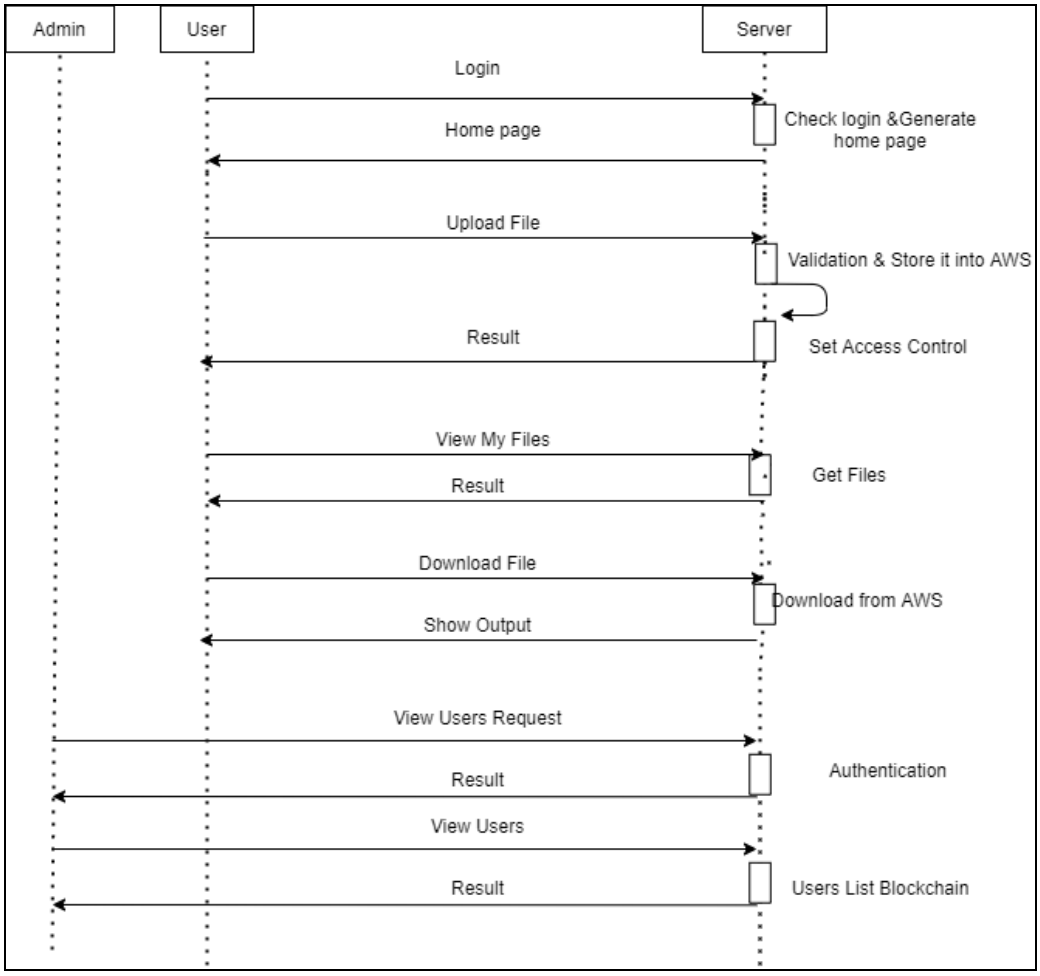

Figure (4): Sequence diagram

The main design of the system developed consists of two users: the admin and the user (Figure (2)). The admin was able to view the requests from the users for account creation, view the users and perform user authentication while the user was able to upload and save

files securely in the cloud. The different actions that can be performed by the user and admin is shown in figure (3) while the working sequence of the system is shown in figure (4).

4.2 Implementation

The system was implemented using Python. The web application was created using the Django framework. The front end of the web application was created and designed using HTML, CSS and JavaScript and the working of the backend of the web application was based on Python. The web application and the blockchain was integrated using the library 'web3' in Python.

The web application and the blockchain were integrated. The final form of the web application consists of a log in interface where the inexperienced users can register or create accounts and the already registered users and admin were able to log in to the application by providing their username and password. The user on logging in reached a home page where the user can upload the files to the cloud (Figure (5)) and view the files. The user was also able to log out from the web application. The user can view all the files that they have uploaded and the time and date at which they have uploaded the files corresponding to each file. The admin on logging in reached the home page of the admin. The admin was able to view the requests from the users for creating an account and the admin was able to perform validation based on the click of the button with the text 'Approve'. The admin was able to reject the requests for creation of account manually while the authentication process took place automatically when the admin approves a request. The admin was also able to view all the users who have successfully registered or created an account in the web application (Figure (6)).

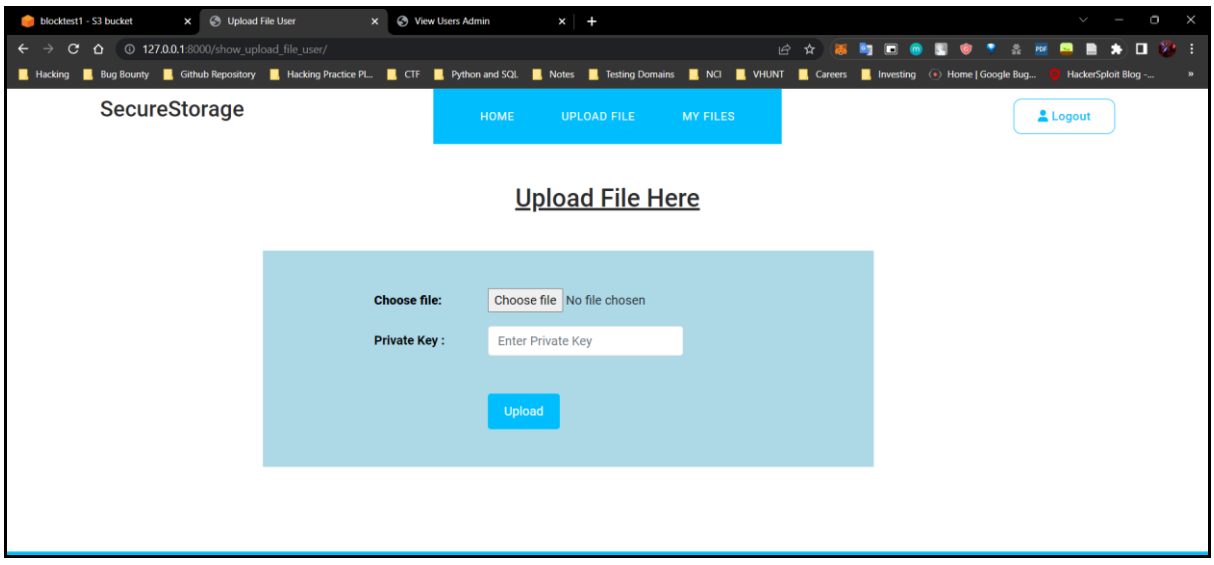

Figure (5): The page where a user can upload a file

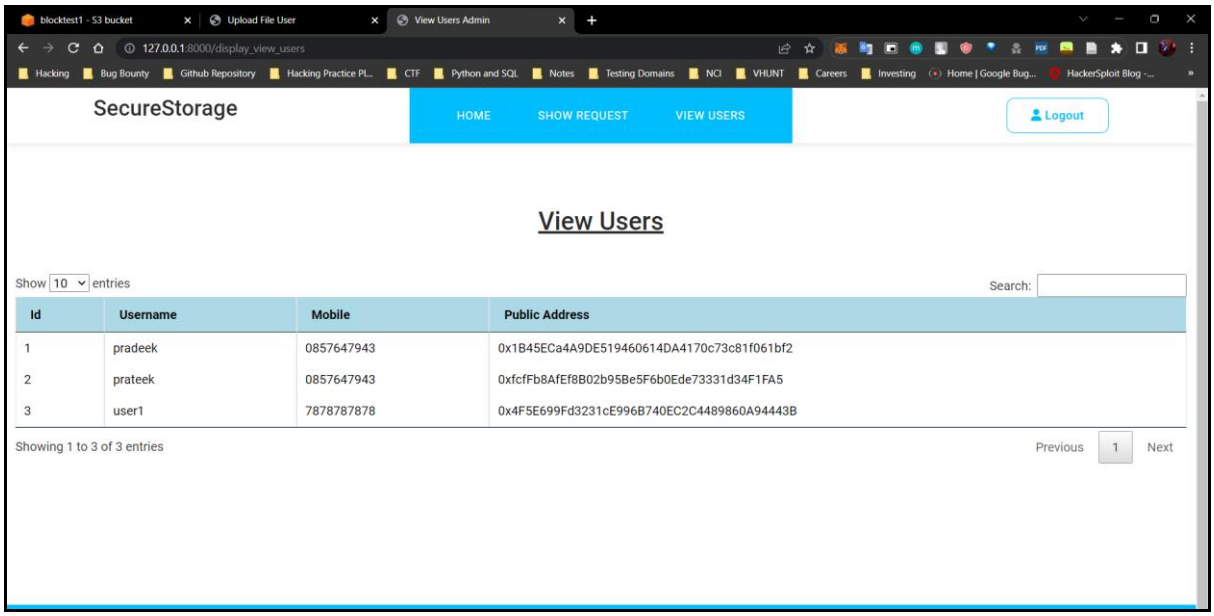

Figure (6): The page where the admin can view the users

A bucket was created in Amazon s3 for storing the files uploaded to the cloud using the web application. The files were stored in the bucket and for integrating the Python based web application with AWS the library ‘Boto3’ was used. The service used was ‘s3’. The web application was connected to the cloud using the service name, region name, access key id, which was 'AKIA2MS6662K5RTMAREU' here and the secret access key.

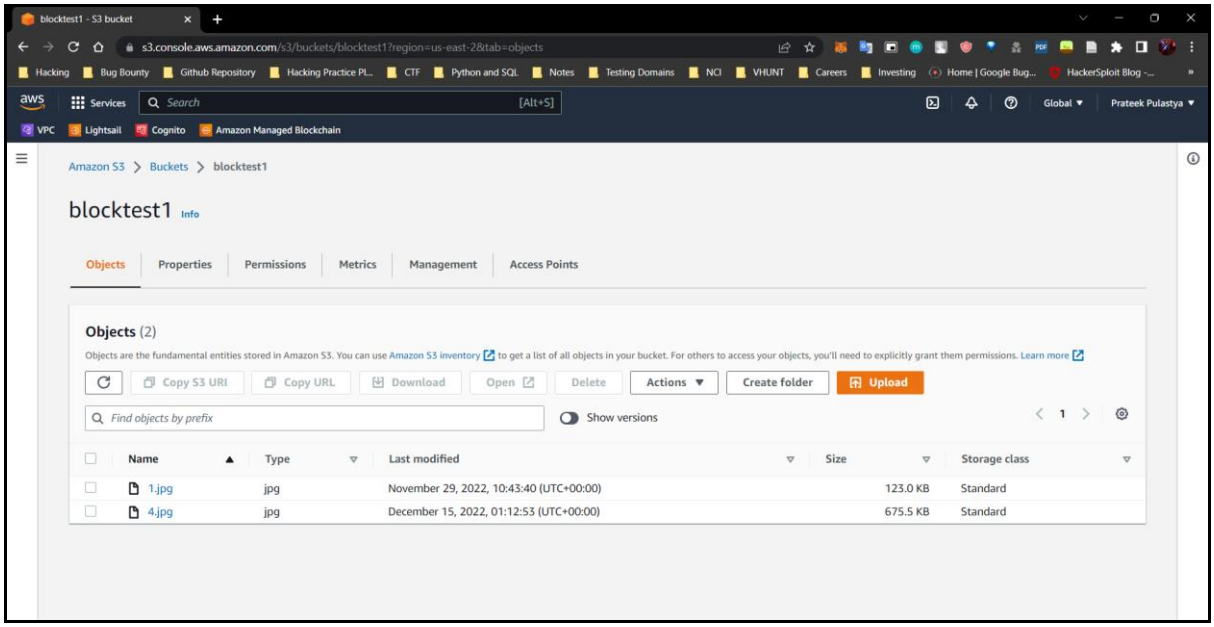

Figure (7): AWS S3 Bucket shows the file uploaded in the website.

5 Evaluation

5.1 Experimental setup

The web application was run and for evaluating the performance of the web application several tests like creating an account, accessing an unauthorized file was conducted to display the effectiveness of the system developed here.

5.2 Evaluation metrics

The results of the experiments can be seen as screenshots. These screenshots denote the results of the different tests that were performed on the web application and the output generated by the web application in the specific testing scenarios.

5.3 Experiments

The main experiments were conducted for evaluating the authorization and authentication abilities of the system developed here. Firstly, it was seen if the system performs user authentication. For this an account must be created using username and an invalid public key. This key was not generated by the blockchain and given to the user. So, if the system performs authentication correctly no user account will be created in this scenario. Another way in which authentication was evaluated was by uploading or downloading a file. The file uploading was performed using a key different from the private key assigned to the user and the file downloading was also performed using an invalid private key.

The authorization was evaluated by viewing the files uploaded by a particular user according to the way the system is designed one user will be able to see only the files that they have uploaded, and the files uploaded by no other users can be accessed.

5.4 Results

The system developed here effectively performed authentication, authorization, and access control when the tests were conducted. When the authentication of the system was evaluated, it was seen that when a user tried to create an account the request went to the admin and the admin was able to reject or accept the user based on the public key provided by the user (Figure (8)). This means that people who did not receive a public key based on the creation of the blockchain were not able to create an account in the web application. The block chain also automatically rejected the requests of the invalid people.

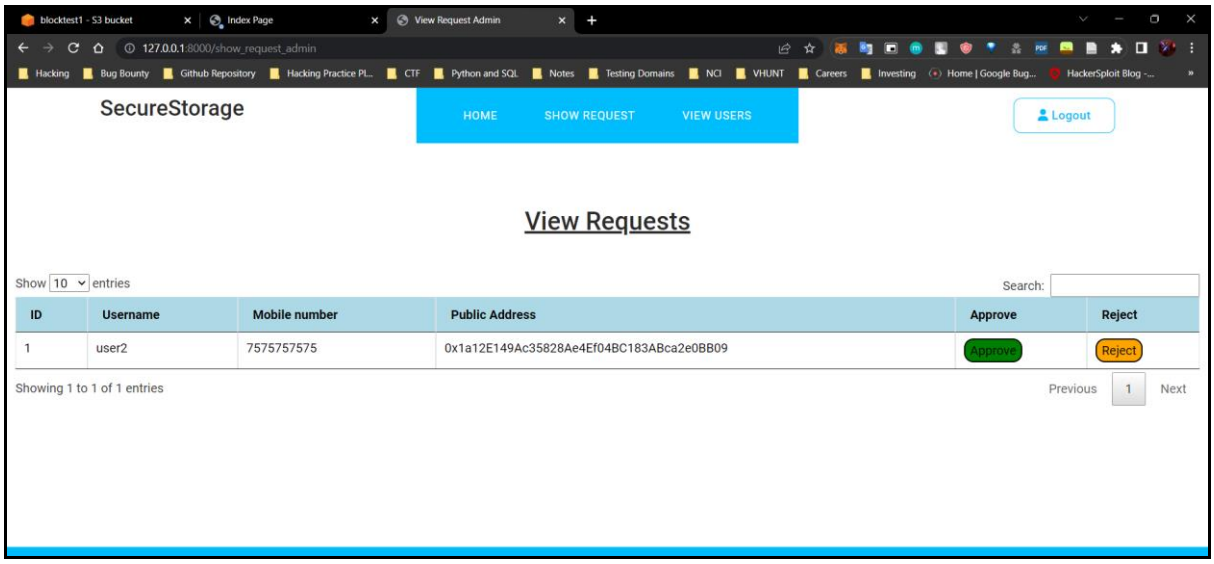

Figure (8): Requests received by the admin.

Now when the files were uploaded to the cloud using an invalid private key the file could not be uploaded. The same happened when the files of a particular user were downloaded using an invalid key. An alert showing 'Key error' was displayed by the web application in both scenarios (Figure (9)).

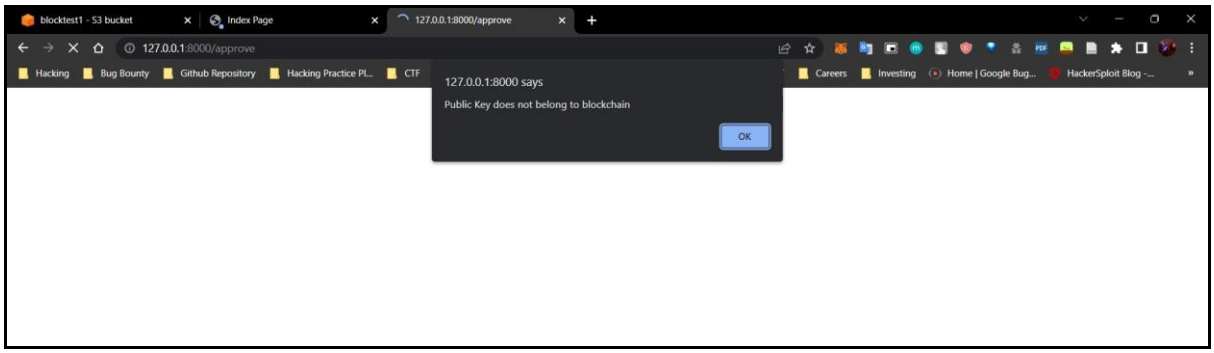

Figure (9): The alert when an invalid public key is used

For evaluating the authorization and access control the files that can be accessed by a particular was viewed and it was seen that only the files that a particular user uploaded could be accessible to that user. It was seen that the files of one user was not accessible to another user (Figure (10)).

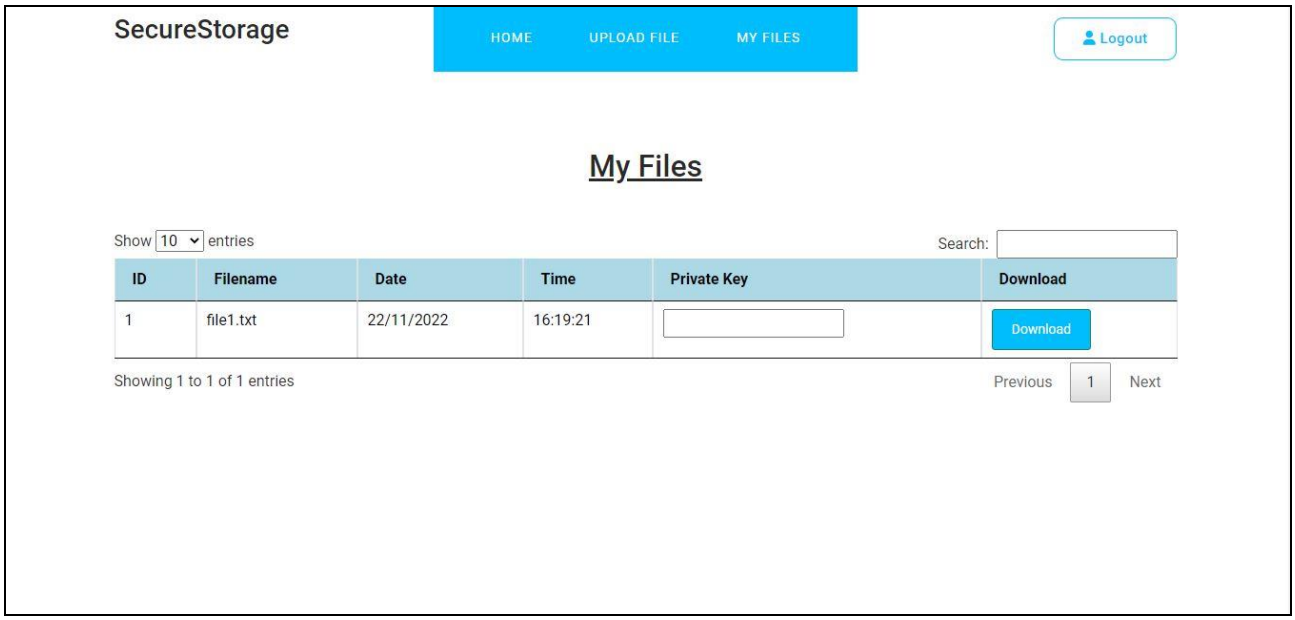

Figure (10): The files that can be viewed by a user

6 Discussion

A system for storing data to the cloud was implemented here and the system was made secure using the block chain. The web application works according to the way it was intended to work. A blockchain was successfully created with each nodes having a public and private key. The private and public key were used for authentication, authorization, and access control. Authentication was successfully performed as the users who are not meant to have access to the web application i.e.; those who have not received the public key which was created during the creation of the nodes in the block chain, were not able to access the web application as their request for creating an account were not be validated if the public key entered was not valid. The access control was also properly implemented as the users who do not have a private key were not able to access the sources of the cloud to upload and store a file and the users were also not be able to download and view files that they had previously uploaded if they do not have the private key. Each user was only able to access or download the files that they had uploaded. This was successfully implemented as no user was able to access the files uploaded by another user.

The system answered the research question associated with this approach. This showed that the system has been effectively implemented and has achieved its goals.

The answer to the research question can be seen from the working of the web application implemented here as authentication, authorization and access control were enhanced when the blockchain was used for a cloud environment. Blockchain provided better security than many other methods as it was based on the private and public key generated for each user and the authentication, authorization and access control was effectively implemented using blockchain. No user was able to access the web application or upload files to the cloud storage without the private or public keys created when the block chain was created. If the blockchain network had not been implemented the user authentication may have been conducted by the admin which will not be as effective as the authentication provided by the

blockchain method. The file upload to the cloud storage was also more secure as here the private key was also used and if the blockchain had not been used other methods would have to be used which are less secure than the blockchain technology. This can be seen as an improvement from several traditional methods.

It was observed from the existing literature that blockchain technology can provide effective access control, authentication, and authorization in a cloud environment and this is in line with the results of the system developed here. The public and private key methods were also found to be effective for securing the cloud environment, from the literature, this also matches the finding from the results of the system developed here as private and public keys generated by the blockchain is effectively used for providing security to the cloud. The ganache was found to be highly effective in creating blockchains than other methods according to the literature and this finding was also supported by the results of the system developed here as an effective blockchain framework was created using Ganache.

Using the blockchain for securing the cloud environment was highly effective but there are some limitations associated with the system developed here. The main limitation is that the retrieval of data from the cloud when using a local blockchain tends to be slow and sometimes the web application must be refreshed to complete the retrieval of data from the cloud. Another limitation of the approach is that if a specific user exposes the private key or public key an unauthorized person can use it to access the web application and resources of the cloud. Another limitation of the approach proposed here is that no analysis methods were used for evaluating the effectiveness of the performance of the system developed here as seen in the approach proposed by LI, (2022).

7 Conclusion and future work

A system for cloud storage which was secured using blockchain has been implemented here. The system was implemented in the form of a web application that can be used for storing data to the cloud. The web application can only be accessed by authorized users and this authorization was performed using the private key and public keys created for each node when a blockchain was created. These private and public keys were successfully used for performing authentication, authorization and for implementing access control. The blockchain created here was successfully integrated into the web application and the data was stored to the cloud storage in a successful manner. The cloud storage was setup using AWS.

In the future an analysis or evaluation method for determining the effectiveness of the security provided by the blockchain in a cloud environment, can be included in the approach.

References

Ajay, N., Mohan, H.S., Shwetha, B.V., Shrihari, M.R., Manjunath, P.V. and Anitha, T.N. (2022). Access Control Framework in the Cloud based on Multi-Blockchain with Light Privacy Protection. 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). doi:10.1109/icdcece53908.2022.9792816.

Alansari, S., Paci, F., Margheri, A. and Sassone, V. (2017). Privacy-Preserving Access Control in Cloud Federations. 2017 IEEE 10th International Conference on Cloud Computing (CLOUD). doi:10.1109/cloud.2017.108.

Algarni, S., Eassa, F., Almarhabi, K., Almalaise, A., Albassam, E., Alsubhi, K. and Yamin, M. (2021). Blockchain-Based Secured Access Control in an IoT System. Applied Sciences, 11(4), p.1772. doi:10.3390/app11041772.

Alsultan, T.M., Salam, A.A., Alissa, K.A. and Saqib, N.A. (2019). A Comparative Study of Biometric Authentication in Cloud Computing. [online] IEEE Xplore. doi:10.1109/ISNCC.2019.8909117.

Bulao, J. (2020). How Many Companies Use Cloud Computing? [31+ Stats for 2020]. [online] TechJury. Available at: https://techjury.net/blog/how-many-companies-use-cloud-computing/#gref.

Chandra Jadala, Dr. (2019). Authentication and Authorization Mechanism for Cloud Security. 10.35940/ijeat. F8473.088619. [online]. Available at: https://www.researchgate.net/publication/335842661_Authentication_and_Authorization_Mechanism_for_Cloud_Security

Chinnasamy, P., Vinodhini, B., Praveena, V., Vinothini, C. and Ben Sujitha, B. (2021). Blockchain based Access Control and Data Sharing Systems for Smart Devices. Journal of Physics: Conference Series, 1767(1), p.012056. doi:10.1088/1742-6596/1767/1/012056.

Dar, A.B., Baba, A.I., Lone, A.H., Naaz, R. and Wu, F. (2020). Blockchain Driven Access Control Mechanisms, Models and Frameworks: A Systematic Literature Review. Cryptology ePrint Archive. [online] Available at: https://eprint.iacr.org/2020/1379 [Accessed 24 Nov. 2022].

EL KAMOUN, Najib. (2017). AUTHENTICATION MECHANISMS IN CLOUD COMPUTING ENVIRONMENTS. International Journal on Information Technologies & Security. 9. 63-84.

Ghaffari, F., Bertin, E., Hatin, J. and Crespi, N. (2020). Authentication and Access Control based on Distributed Ledger Technology: A survey. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). doi:10.1109/brains49436.2020.9223297.

Gupta, Ashok & Siddiqui, Shams & Alam, Shadab & Shuaib, Mohammed. (2019). Cloud Computing Security using Blockchain. 6. 791-794. [online] Available at: https://www.researchgate.net/publication/335502544_Cloud_Computing_Security_using_Blockchain

Jemel, M. and Serhrouchni, A. (2017). Decentralized Access Control Mechanism with Temporal Dimension Based on Blockchain. 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE). doi:10.1109/icebe.2017.35.

Khieu, B. and Moh, M. (2019). CBPKI. Proceedings of the 2019 ACM Southeast Conference. doi:10.1145/3299815.3314433.

Kumar, S., Akbar Abbas Jafri, S., Nigam, N., Gupta, N., Gupta, G., and Singh, S.K. (2020). A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing. IOP Conference Series: Materials Science and Engineering, 748, p.012026. doi:10.1088/1757-899x/748/1/012026.

Lee, H., Kang, D., Lee, Y. and Won, D. (2021). Secure Three-Factor Anonymous User Authentication Scheme for Cloud Computing Environment. Wireless Communications and Mobile Computing, 2021, pp.1–20. doi:10.1155/2021/2098530.

Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q. and Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: a taxonomy, review, and future directions. Journal of Cloud Computing, 10(1). doi:10.1186/s13677-021-00247-5.

LI, X. (2022). A Blockchain-Based Verifiable User Data Access Control Policy for Secured Cloud Data Storage. Computational Intelligence and Neuroscience, 2022, pp.1–12. doi:10.1155/2022/2254411.

Masood, R., Shibli, M.A., Ghazi, Y., Kanwal, A. and Ali, A. (2015). Cloud authorization: exploring techniques and approach towards effective access control framework. Frontiers of Computer Science, 9(2), pp.297–321. doi:10.1007/s11704-014-3160-4.

Mell, P. and Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. [online] Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Mendki, P. (2021). Securing Cloud Native Applications Using Blockchain. 2021 12th International Conference on Information and Communication Systems (ICICS). doi:10.1109/icics52457.2021.9464583.

Mohammad, A. (2022). Distributed Authentication and Authorization Models in Cloud Computing Systems: A Literature Review. Journal of Cybersecurity and Privacy, 2(1), pp.107–123. doi:10.3390/jcp2010008.

Nepal, S., Chen, S., Yao, J. and Thilakanathan, D. (2011). DIaaS: Data Integrity as a Service in the Cloud. 2011 IEEE 4th International Conference on Cloud Computing. doi:10.1109/cloud.2011.35.

Pavithra, S., Ramya, S. and Prathibha, S. (2019). A Survey on Cloud Security Issues and Blockchain. 2019 3rd International Conference on Computing and Communications Technologies (ICCCT). doi:10.1109/iccct2.2019.8824891.

Rouhani, S. and Deters, R. (2019). Blockchain based access control systems: State of the art and challenges. 2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI). [online] doi:10.1145/3350546.3352561.

Sanghi, N., Bhatnagar, R., Kaur, G. and Jain, V. (2018). BlockCloud: Blockchain with Cloud Computing. [online] IEEE Xplore. doi:10.1109/ICACCCN.2018.8748467.

Son, S., Lee, J., Kim, M., Yu, S., Das, A.K. and Park, Y. (2020). Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain. IEEE Access, 8, pp.192177–192191. doi:10.1109/access.2020.3032680.

Sukhodolskiy, I. and Zapechnikov, S. (2018). A blockchain-based access control system for cloud storage. 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). doi:10.1109/eiconrus.2018.8317400.

Tapas, N., Merlino, G. and Longo, F. (2018). Blockchain-Based IoT-Cloud Authorization and Delegation. 2018 IEEE International Conference on Smart Computing (SMARTCOMP). doi:10.1109/smartcomp.2018.00038.

Vance, A. (2014). Flow based analysis of Advanced Persistent Threats detecting targeted attacks in cloud computing. 2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology. doi:10.1109/infocommst.2014.6992342.

Weston, G. (2022). What is Ganache Blockchain. [online] 101 Blockchains. Available at: https://101blockchains.com/ganache-blockchain/ [Accessed 24 Nov. 2022].

Yin, Y., Li, Y., Ye, B., Liang, T. and Li, Y. (2021). A Blockchain-Based Incremental Update Supported Data Storage System for Intelligent Vehicles. IEEE Transactions on Vehicular Technology, 70(5), pp.4880–4893. doi:10.1109/tvt.2021.3068990.