Data Integrity Audit Scheme Based on Blockchain Expansion Technology

A report submitted in partial fulfillment of the requirements for the award of a degree of

Bachelor of Technology

in

Computer Science and Engineering

by

G. Sairam

(21EG505828)

J. Dayamani

(21EG505831)

V. Likitha

(21EG505870)

Under the Guidance of

Dr. P. Ravinder Rao,

Asst. Professor, Department of CSE

Department of Computer Science and Engineering

ANURAG UNIVERSITY

Venkatapur (V), Ghatkesar (M), Medchal (D)., T.S-500088

(2023-2024)

DECLARATION

We hereby declare that the report entitled **"Data Integrity Audit Scheme Based on Blockchain Expansion Technology"** submitted for the award of the degree of **Bachelor of Technology (B. Tech)** in Computer Science and Engineering is a record of an original work done by us and the report has not formed the basis for the award of any degree, diploma, associateship or fellowship of similar other titles. It has not been submitted to any other University or Institution for the award of any degree or diploma.

G. Sairam

21EG505828

J. Dayamani

21EG505831

V. Likitha

21EG505870

Place:

Date:

ANURAG UNIVERSITY | SCHOOL OF ENGINEERING

CERTIFICATE

This is to certify that the report entitled **"Data Integrity Audit Scheme Based on Blockchain Expansion Technology"** is being submitted by **Mr. G. Sairam** bearing the Hall Ticket number **21EG505828**, **Ms. J. Dayamani** bearing the Hall Ticket number **21EG505831**, **Ms. V. Likitha** bearing the Hall Ticket number **21EG505870** in partial fulfillment for the award of the Bachelor of Technology in Computer Science and Engineering to the Anurag University is a record of bonafide work carried out by them under my guidance and supervision for the academic year 2023 to 2024.

The results embodied in this report have not been submitted to any other University or Institute for the award of any other degree or diploma.

Signature of Supervisor
Dr. P. Ravinder Rao
Assistant Professor
Department of CSE

Signature of Dean
Dr. G. Vishnu Murthy
Dean, CSE

External Examiner

ACKNOWLEDGEMENT

We would like to express our sincere thanks and deep sense of gratitude to project supervisor **Dr. P. Ravinder Rao,** Assistant Professor, Dept of CSE for his constant encouragement and inspiring guidance without which this project could not have been completed. His critical reviews and constructive comments improved our grasp of the subject and steered to the fruitful completion of the work. His patience, guidance and encouragement made this project possible.

We would like to express our special thanks to **Dr. V. Vijaya Kumar**, Dean School of Engineering, Anurag University, for his encouragement and timely support in our B. Tech program.

We would like to acknowledge our sincere gratitude for the support extended by **Dr. G. Vishnu Murthy**, Dean, Dept. of CSE, Anurag University. We also express our deep sense of gratitude to **Dr. V V S S S Balaram**, Academic Coordinator, **Dr. Pallam Ravi**, Project Coordinator and Project Review Committee members, whose research expertise and commitment to the highest standards continuously motivated us during the crucial stage of our project work.

G. Sairam
(21EG505828)

J. Dayamani
(21EG505831)

V. Likitha
(21EG505870)

ABSTRACT

A growing number of users are entrusting their data to the cloud, but ensuring data integrity poses a significant challenge. Blockchain, known for its decentralization and immutability, is increasingly being explored by researchers as a substitute for third-party auditors. This research introduces a data integrity system leveraging blockchain expansion technology, targeting the high costs associated with maintaining blockchain networks and the creation of new blocks. The rapid expansion of blocks in existing blockchain data integrity audits prompted this approach. In this system, users and cloud service providers (CSP) deploy smart contracts on both the main chain and sub-chains. To mitigate costs, resource-intensive computing tasks are offloaded to the sub-chain, and results are periodically submitted to the main chain for confirmation. The concept of non-interactive audits is introduced to maintain a smooth user experience by avoiding constant communication with CSP during audits. For enhanced data security, a reward pool mechanism is implemented. Rigorous analysis encompassing storage, batch auditing, and data consistency validates the scheme's correctness. Experiments conducted on the Ethereum blockchain platform illustrate the scheme's effectiveness in significantly reducing storage and computational overhead.

Keywords: Blockchain, cloud storage, data auditing, blockchain expansion, TPA.

CONTENTS

Title	Pageno
Abstract	v
List of Figures	viii
1.Introduction	**1**
1.1. Motivation	2
1.2. Problem Definition	3
1.3. Objective of the Project	4
2.Literature Survey	**5**
3.Analysis	**8**
3.1.Existing System	8
3.2.Proposed System	9
3.3.System Requirement Specification	9
3.3.1 Purpose	10
3.3.2 Scope	11
3.3.3Overall Description	12
4.Design	**13**
4.1. UML Diagrams	13
4.1.1 Use Case Diagram	13
4.1.2 Class Diagram	14
4.1.3 Sequence Diagram	16
4.2. System Architecture	17
5.Implementation	**18**
5.1.Modules	18
5.2.Module Description	19
5.3.Introduction to Technologies Used	20
5.4. Libraries/Packages	20
5.5. Sample Code	22

6.Test Cases **34**

7.Screenshots **35**

8.Conclusion **42**

9.Future Enhancement **43**

10. Bibliography **45**

LIST OF FIGURES

Figure No	Figure Name	Page No
Fig.4.1.1	Use Case Diagram	14
Fig.4.1.2	Class Diagram	15
Fig.4.1.3	Sequence Diagram	16
Fig.4.2	System Architecture	17
Fig.7.1	Home Page	35
Fig.7.2	User Page	35
Fig.7.3	TPA Page	36
Fig.7.4	Verifying	37
Fig.7.5	User Login	37
Fig.7.6	Cloud Authorization	38
Fig.7.7(a)	Download Request	38
Fig.7.7(b)	Download Request Granted	39
Fig.7.8(a)	Upload Page	39
Fig. 7.8(b)	Upload Page	40
Fig. 7.9	Attacker page	40
Fig.7.9(a)	Attacker Page	41
Fig.7.9(b)	Attacker Page	41
Fig.7.10	Result Page	41