DECENTRALIZED DATA SECURITY USING BLOCKCHAIN

(PROJECT PHASE- II)
submitted in partial fulfillment of the requirements for the award of the degree in

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE AND ENGINEERING
DATA SCIENCE (ARTIFICIAL INTELLIGENCE)

By

SUJITH KUMAR D (211191101151)

V.V.S SRAVANTH (211191101161)

SURENDER B (211191101153)

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING

APRIL 2025

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report (Project Phase-II) is the bonafide work of

Mr. SUJITH KUMAR D Reg. No: 211191101151,

Mr. V.V.S SRAVANTH Reg. No: 211191101161,

Mr. SURENDER B Reg. No: 211191101153,

Who carried out the project entitled **"DECENTRALIZED DATA SECURITY USING BLOCKCHAIN"** under our supervision from December 2024 to April 2025.

Internal Guide	Project Coordinator	Department Head
Mrs. S. AMUTHA	**Mr. M. ARUN**	**Dr. S. GEETHA**
Assistant Professor	**Assistant Professor**	**Professor & HOD**
Dept of CSE	**Dept of CSE**	**Dept of CSE**
Dr. MGR Educational and Research Institute, Deemed to be University	Dr. MGR Educational and Research Institute, Deemed to be University	Dr. MGR Educational and Research Institute, Deemed to be University

Submitted for Viva Voce Examination held on _____

Internal Examiner
(Name in Capital letters with Signature)

External Examiner
(Name in Capital letters with Signature)

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

DECLARATION FORMAT

We **SUJITH KUMAR.D (211191101151), V.V.S SRAVANTH (211191101161), SURENDER.B (211191101153),** hereby declare that the Project Report (Project Phase-II) entitled **"DECENTRALIZED DATA SECURITY USING BLOCKCHAIN"** is done by us under the guidance of **S AMUTHA** is submitted in partial fulfillment of the requirements for the award of the degree in **BACHELOR OF TECHNOLOGY** in **Computer Science and Engineering** specialization in **Data Science (Artificial Intelligence).**

DATE:

PLACE:

1.

2.

3.

SIGNATURE OF THE CANDIDATE(S)

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

ACKNOWLEDGEMENT

We would first like to thank our beloved Founder Chancellor sir **Thiru**.**Dr. A.C.SHANMUGAM, B.A., B.L.,** President **Er. A.C.S.Arunkumar, B.Tech., M.B.A.,** and Secretary **Thiru A.RAVIKUMAR** for all the encouragement and support extended to us during the tenure of this project and also our years of studies in his wonderful University.

We express my heartfelt thanks to our Vice Chancellor **Prof. Dr. GEETHALAKSHMI** in providing all the support of my Project (Project Phase-II).

We express my heartfelt thanks to our Head of the Department, **Prof. Dr. S.Geetha**, who has been actively involved and very influential from the start till the completion of our project.

Our sincere thanks to our Project Coordinators **Mr. M Arun** and Project guide **Mrs. S. Amutha** for their continuous guidance and encouragement throughout this work, which has made the project a success.

We would also like to thank all the teaching and non teaching staffs of Computer Science and Engineering department, for their constant support and the encouragement given to us while we went about to achieving my project goals.

CONTENT

LIST OF ABBREVIATIONS

DDoS	Distributed Denial of Service
DPR	General Data Protection Regulation
Pow	Proof of Work
DLF	Distributed Ledger Technology
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
UI	User Interface
API	Application Programming Interface
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithm
TPS	Transaction Per Second
NIST	National Institute of Standards and Technology
PKC	Public Key Cryptography
NFT	Non-Fungible Token
Pos	Point of Sale(dependent if related to blockchain payment)

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

In the real world many types of Legal documents exist and the government is managing all these documents in a single centralized server. These servers will be managed by Admin and can be bribed to alter any legal document and there will be no direct way to detect such alteration. Another most important issue is cyber-attack where attackers can hack centralized server and may crash or steal data and in such situations all data will be lost.To overcome from above issue we are planning to migrate legal or criminal documents management to Blockchain technology which has inbuilt support for data security, verification and decentralized storage.

In an increasingly interconnected world, data security has become a paramount concern, with centralized systems often falling victim to breaches, unauthorized access, and manipulation. To address these challenges, decentralized data security solutions powered by blockchain technology have emerged as a promising alternative. Blockchain's inherent characteristics transparency, immutability, and decentralization—provide a robust foundation for secure data storage, access control, and transfer without relying on a central authority. This paper explores the potential of blockchain in securing sensitive data, focusing on its ability to enhance confidentiality, integrity, and availability while reducing vulnerabilities associated with traditional centralized systems. Key mechanisms such as cryptographic encryption, smart contracts, and consensus protocols are discussed as they contribute to a secure, tamper-proof, and verifiable data ecosystem. Additionally, we examine various use cases across industries such as healthcare, finance, and supply chain management, where blockchain-driven decentralized security models are already being implemented. The challenges and limitations of blockchain in data security, including scalability, energy consumption, and regulatory concerns, are also addressed, along with potential solutions for overcoming these barriers. Overall, the paper demonstrates that blockchain technology holds significant promise in transforming data security paradigms, offering a decentralized, transparent, and more resilient approach to safeguarding sensitive information in the digital age.

Keywords: Blockchain technology, Decentralized storage, Data security, Transparency, Immutability, Smart contracts, Cryptographic encryption, Consensus protocols, Tamper-proof.

MAJOR DESIGN CONSTRAINTS AND DESIGN STANDARDS TABLE

Student Group	SUJITH KUNAR.D 211191101151	V.V.S. SRAVANTH 211191101161	SURENDER.B 211191101153
Project Title	DECENTRALIZED DATA SECURITY USING BLOCKCHAIN		
Program Concentration Area	Blockchain Technology, Cybersecurity, Data Privacy		
Constraints Example	Economic, Environmental, Sustainability, Ethical.		
Economic	Yes		
Environmental	Yes		
Sustainability	Yes		
Implementable	Yes		
Ethical	Yes		
Health and Safety	Yes		
Social	Yes		
Political	Yes		
Other	Implementable		
Standards			
1	**ISO/IEC 27001**: Information security management.		
2	**ISO/TC 307**: Standards specific to blockchain and distributed ledger technologies.		
3	**GDPR Compliance**: For data privacy and protection, especially in the legal sector.		
Prerequisite Courses for the Major Design Experiences	Blockchain Fundamentals, Cryptography and Network Security, Data Privacy and Cybersecurity		