VeriCloud:Blockchain-Aided Bloom Filter Verification System For Secure Cloud Storage

Guide: Dr.Sindhu S

Abhinand C, Roll No:3
Arun V, Roll No:22
Merin P R, Roll No:37
Rameesa KT, Roll No:49

OUTLINE

- Objective
- Challenges
- Literature Survey
- Proposed System Design
- Implementation Details
- Current Progress
- Output Screenshots
- Timeline
- Future Scope
- Conclusion
- References

OBJECTIVE

- **To develop a privacy-preserving verification mechanism**
  Design a system that verifies the integrity of stored data without revealing its actual content, ensuring confidentiality and data privacy.

- **To utilize Bloom Filters for efficient data summarization**
  Implement Bloom Filters to generate compact data representations that reduce storage space, minimize computational overhead, and enable fast verification of large data.

OBJECTIVE

- **To integrate blockchain for secure and transparent verification**
  Employ blockchain technology to achieve immutable record-keeping and decentralized auditing, ensuring tamper-proof and publicly verifiable proof of data integrity.

CHALLENGES

- Managing large files efficiently for Bloom filter processing. Since Bloom Filters work on hashed data, the files had to be divided into smaller chunks before processing.

- Integrating a Bloom filter into the backend while maintaining high performance and accuracy

LITERATURE SURVEY

SL No.	Reference	Features
1.	Liang et al., 2023. Privacy-Preserving Bloom Filter-Based Keyword Search Over Large Encrypted Cloud Data, IEEE Transactions on Computers, Vol. 72, No. 11, November 2023.	A privacy-preserving keyword search scheme for encrypted cloud data uses Bloom filters for efficient matching. It lets users query files without exposing keywords or content to the provider. The approach ensures confidentiality, efficiency, and scalability in secure storage.

LITERATURE SURVEY

SL No.	Reference	Features
2.	S.M.Udhaya Sankar et al., "A Secure Third-Party Auditing Scheme Based on Blockchain Technology in Cloud Storage," International Journal of Engineering Trends and Technology, vol. 71, no. 3, pp. 23–32, Mar. 2023.	Blockchain-based public auditing system using UEG keys and RSA encryption to secure file access and verification. Smart contracts ensure tamper-proof, privacy-preserving audits without exposing file content.

LITERATURE SURVEY

SL No.	Reference	Features
3.	Chen et al., "A Decentralized Public Auditing Scheme for Secure Cloud Storage Based on Blockchain," Wireless Communications and Mobile Computing, vol. 2022, Article ID 3688164,Oct. 2022.	A decentralized public auditing scheme for cloud storage uses blockchain, smart contracts, dynamic hash tables, and e-voting to ensure data integrity without third-party auditors. Auditing tasks are shared across multiple cloud providers, with results securely recorded on blockchain.

LITERATURE SURVEY

SL No.	Reference	Features
4.	S. Seethalakshmi and B. Balakumar, "Data Deduplication in a Blockchain-Enabled Big Data Ecosystem: Secure and Efficient Cloud Storage," SEEJPH, vol. XXVI, 2025. ISSN: 2197-5248. Posted: 04-Jan-2025.	This paper proposes a blockchain-enabled framework for secure and efficient cloud storage in big data ecosystems. By integrating data deduplication, convergent encryption (3DES), and Ethereum blockchain, it reduces storage costs, ensures privacy, and strengthens security for large-scale data management.

LITERATURE SURVEY

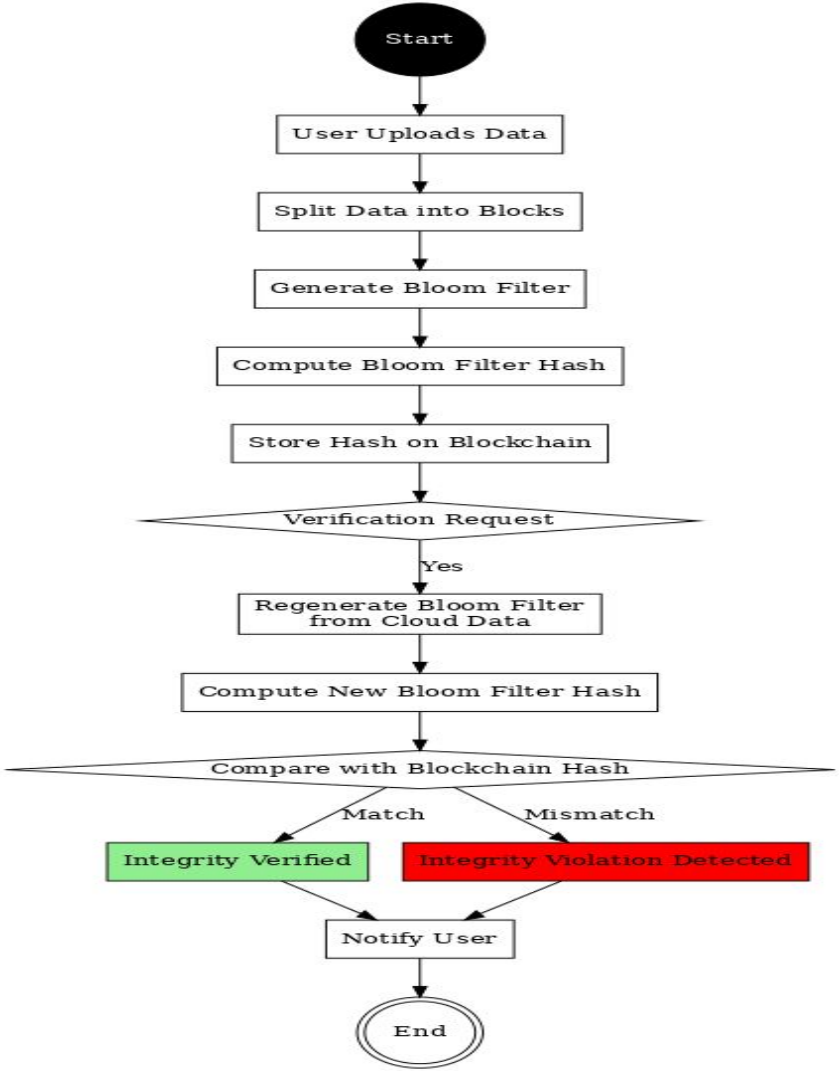
SL No.	Reference	Features
5.	Gebretsadik, F.G., Nayak, S., & Patgiri , R., *"eBF: an Enhanced Bloom Filter for Intrusion Detection in IoT,"* Journal of Big Data, vol. 10, article no. 102, 2023.	This paper proposes **eBF, an enhanced Bloom Filter** designed for Intrusion Detection in IoT systems. It significantly reduces memory usage (up to 15.6× less than standard filters), improves insertion and lookup speed, and minimizes false positives, making it a highly efficient and accurate solution for securing IoT and Big Data applications.

LITERATURE SURVEY

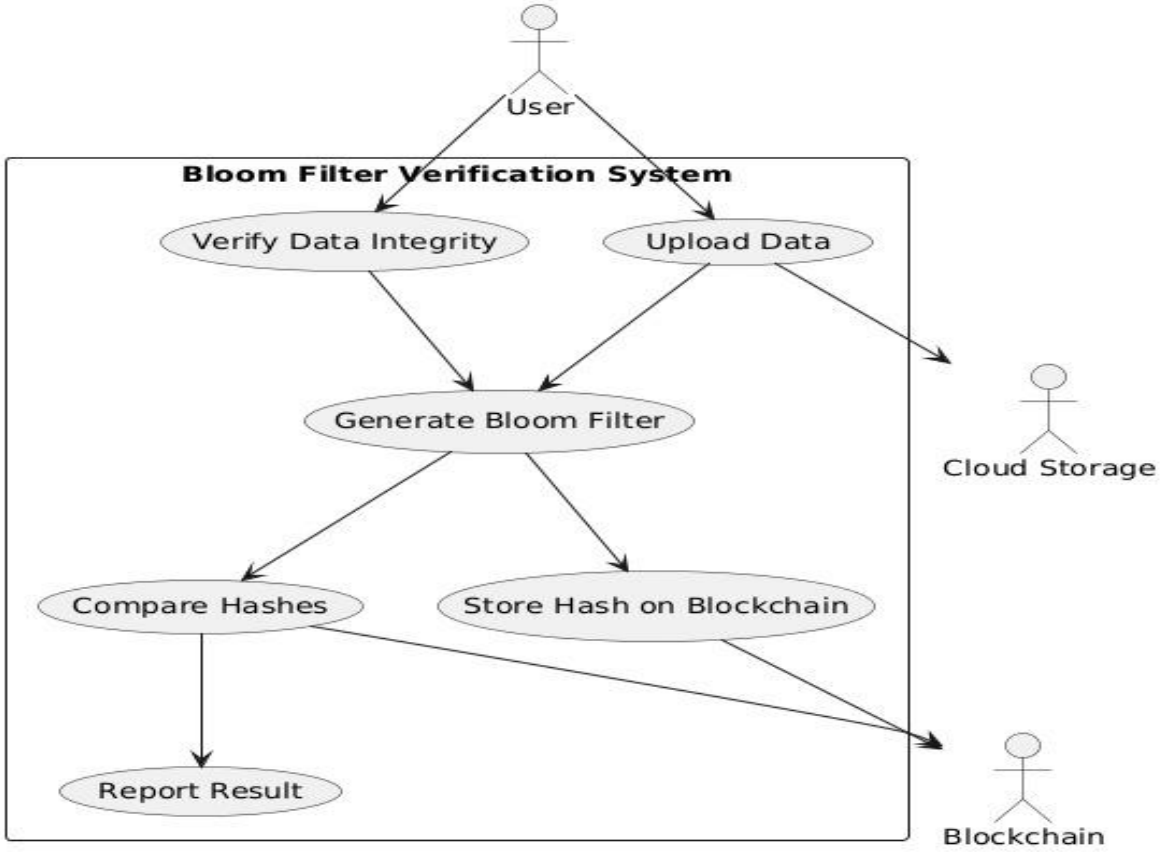
SL No.	Reference	Features
6.	Kasu, P.; Hamandawana, P.; Chung, T.-S. CRBF: Cross-Referencing Bloom-Filter-Based Data Integrity Verification Framework for Object-Based Big Data Transfer System. Appl. Sci. 2023, 13, 7830.	The paper proposes a Cross-Referencing Bloom Filter (CRBF) framework for data integrity verification in object-based big data transfer systems. It reduces computation and memory overhead while eliminating false positives, ensuring accurate and efficient end-to-end integrity checks with minimal impact (<5%) on transfer performance.

PROPOSED SYSTEM DESIGN

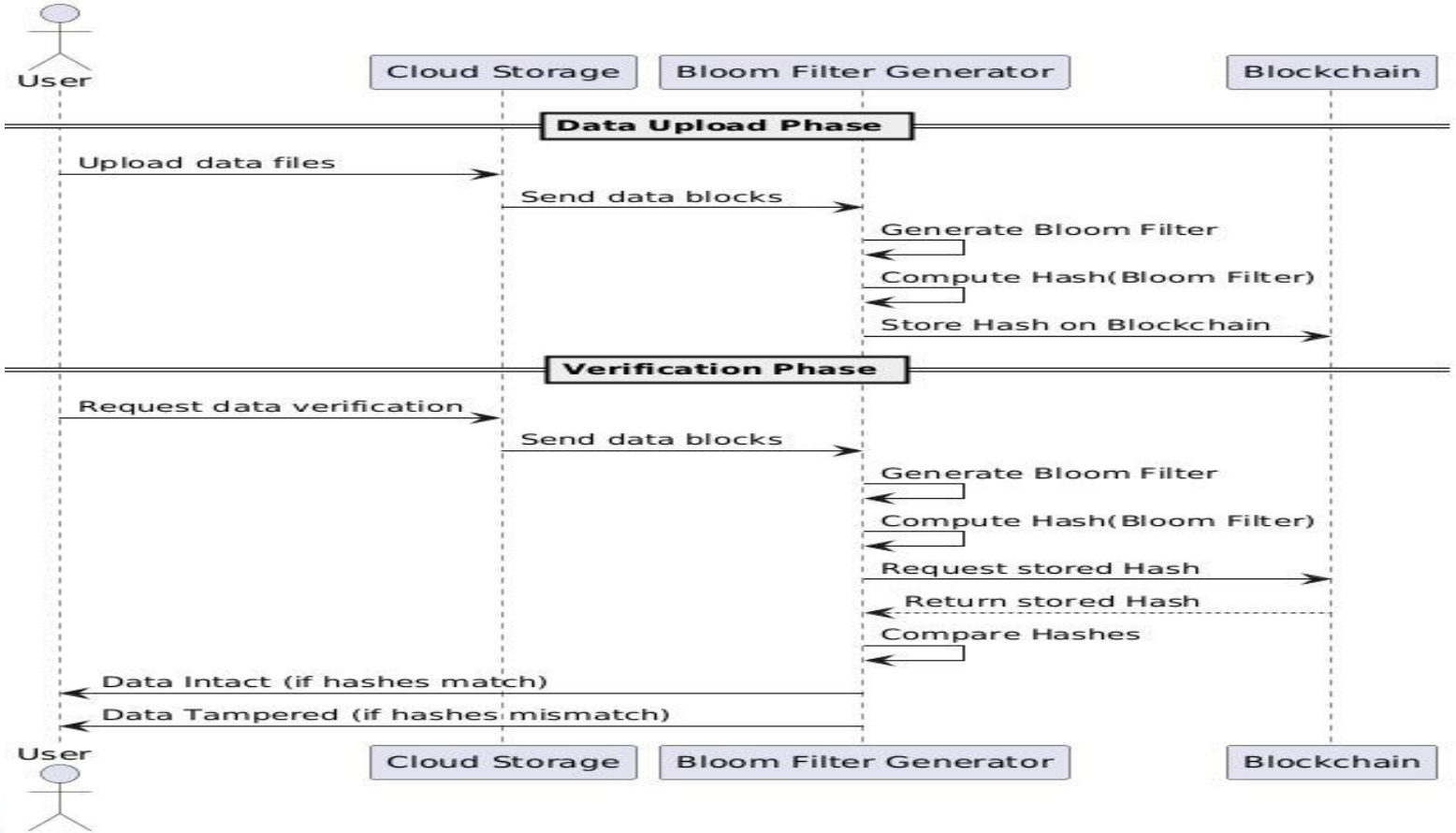
- **Activity Diagram**



Use Case Diagram



Sequence diagram



IMPLEMENTATION DETAILS

- **Programming Languages and Tools Used:**
  - **Python** - Bloom Filter generation for file integrity verification.
  - **React** - Used for building the frontend user interface
  - **FastAPI** - Used for creating the backend for file upload, retrieval, and management.

IMPLEMENTATION DETAILS

- **Key Features Implemented:**
  - File Upload System
    - Drag-and-drop interface
    - 10MB file size limit
  - File Operations (Dashboard)
    - View: Display text file contents in modal
    - Download: Retrieve files with original filenames
    - Delete: Remove files from storage

IMPLEMENTATION DETAILS

- Bloom Filter Implementation
  - Chunking: File is divided into binary chunks for processing.
  - Hashing: Each chunk is hashed using SHA-256 to ensure uniqueness.
  - Initialization: A Bloom Filter is created with capacity set based on the number of chunks and a small error rate for efficient storage.
  - Insertion & Display: Chunk hashes are inserted, and the Bloom Filter bit array is displayed as 0s and 1s in grouped blocks for visualization.

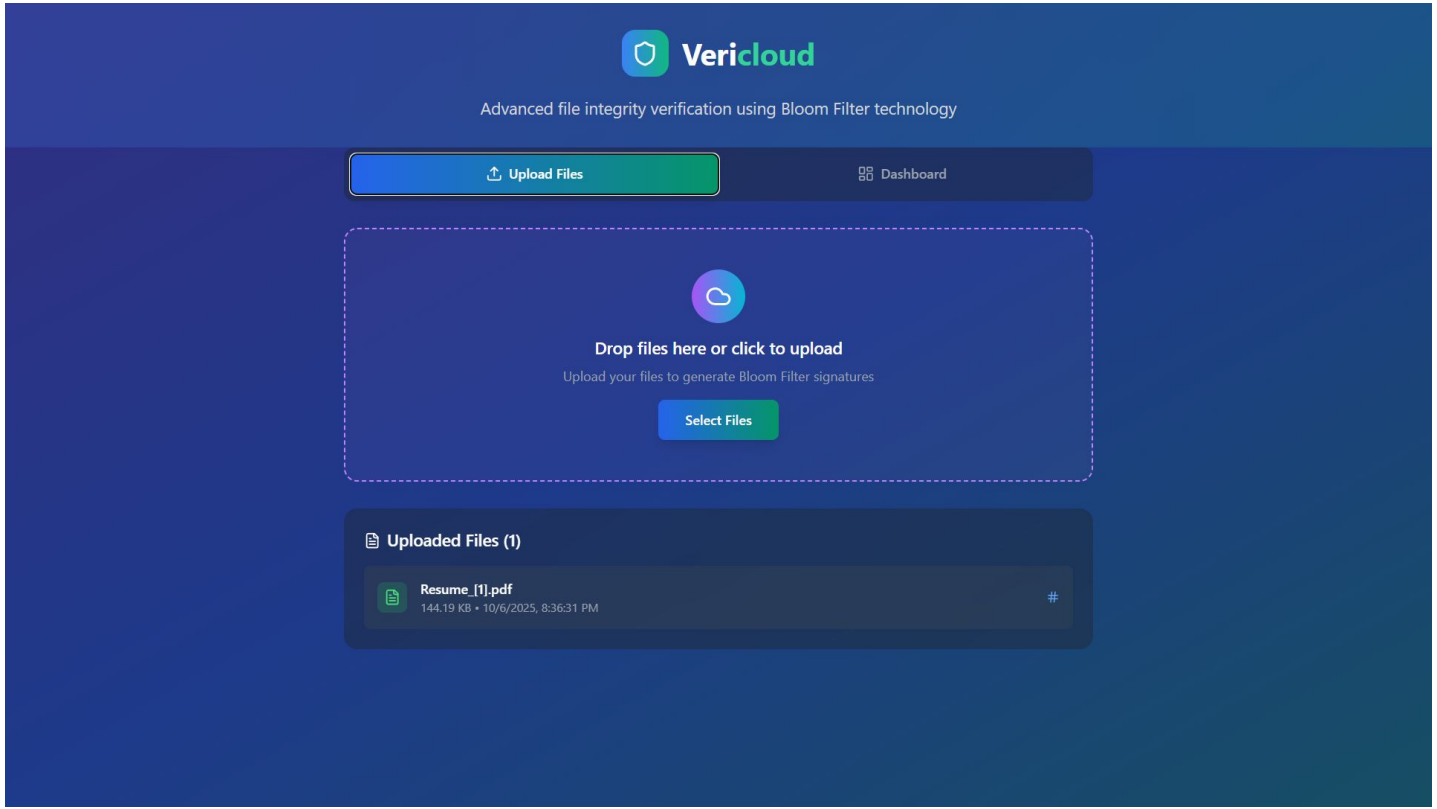
CURRENT PROGRESS

- The User Interface (UI) has been designed and implemented to provide a functional and user-friendly experience.
- The file upload feature has been successfully integrated, allowing users to upload files.
- The content extraction module is now in progress, focusing on extracting and processing data from the uploaded files

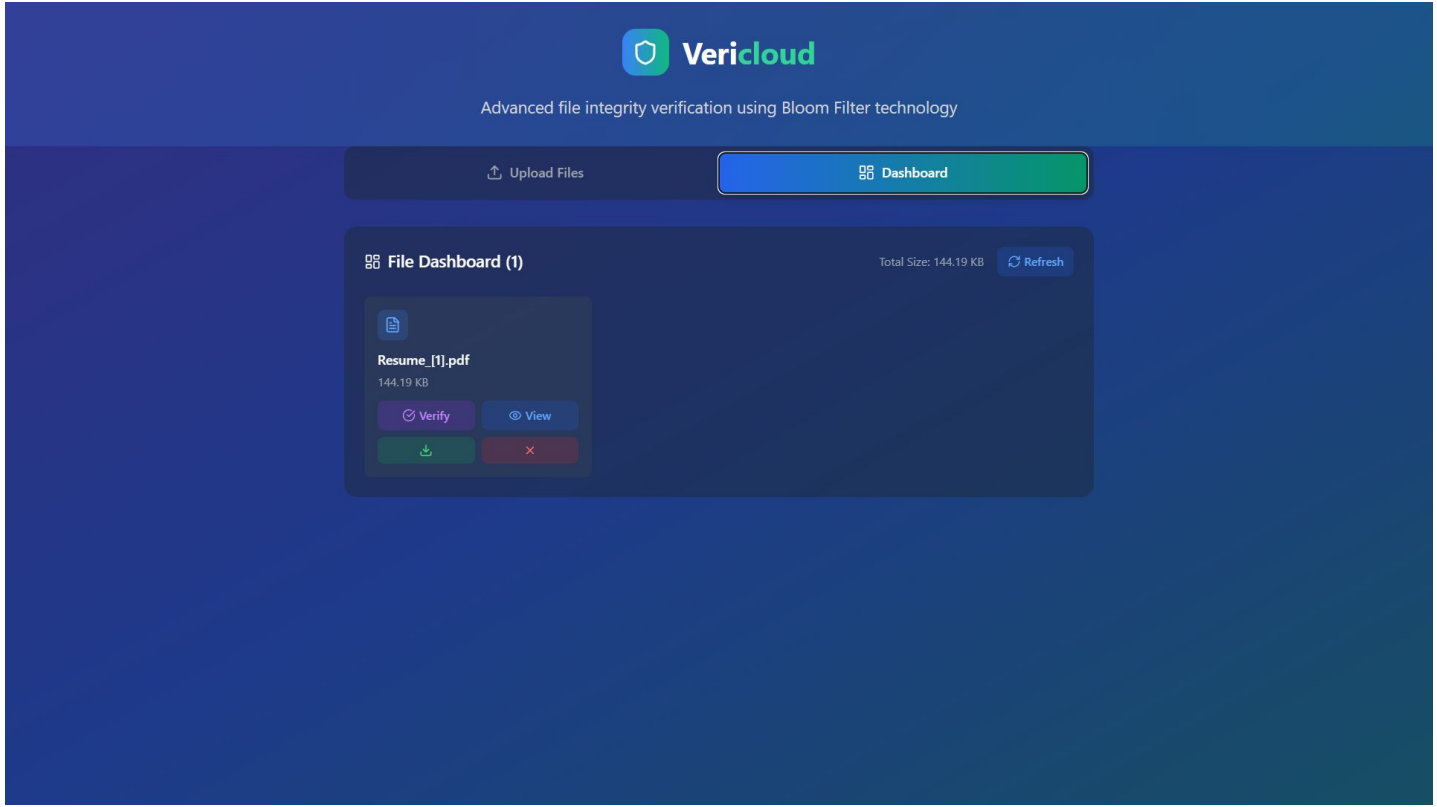
CURRENT PROGRESS

- **Bloom Filter Generation**:The Bloom filter has been developed as a standalone component to efficiently process input data.A file is divided into chunks, and the hash of each chunk is appended to the Bloom filter.These are combined to form the final bit array representing the entire file, ready for future backend integration.

OUTPUT SCREENSHOTS



OUTPUT SCREENSHOTS



OUTPUT SCREENSHOTS

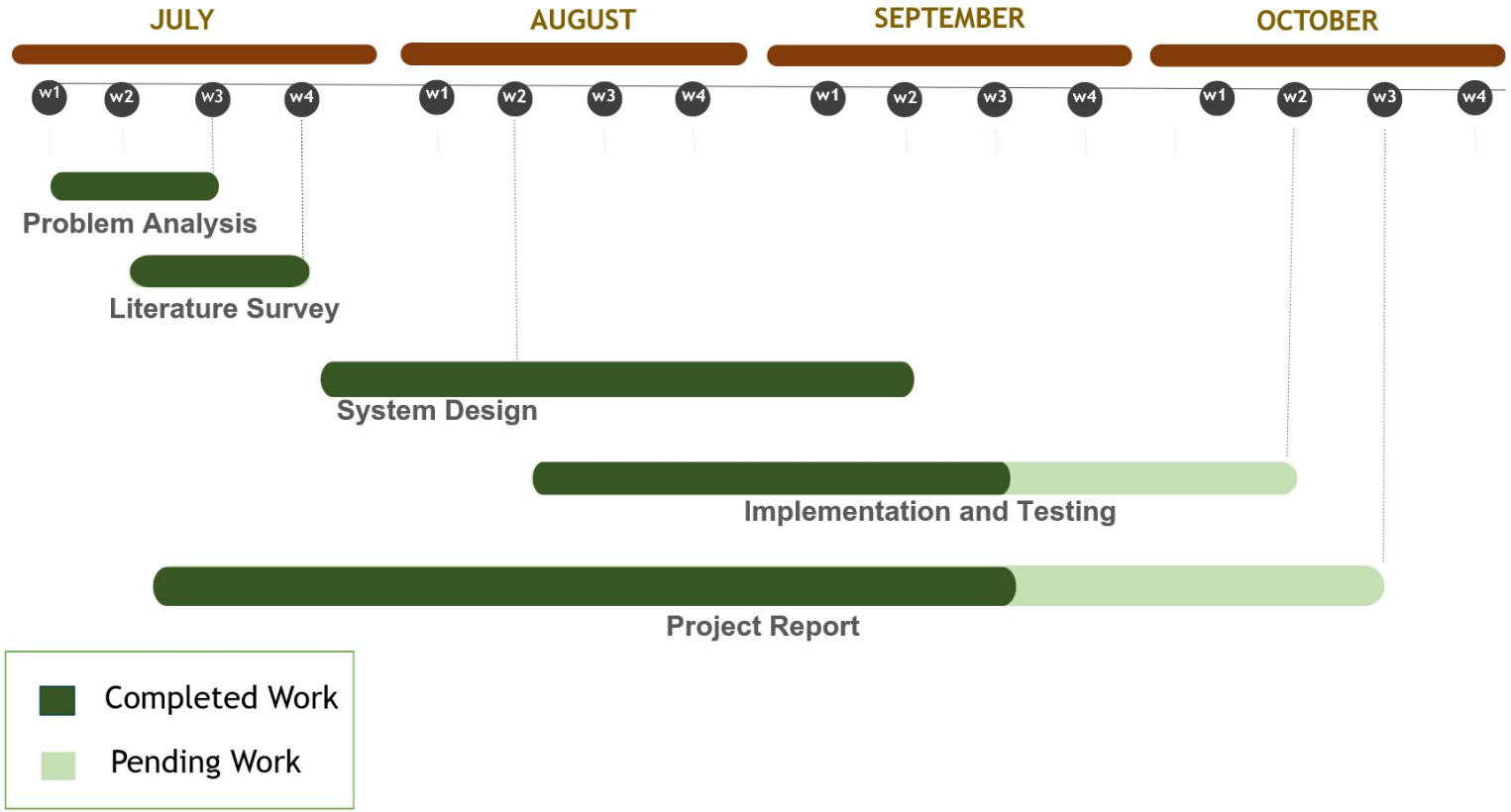
```python
# Step 4: Print Bloom Filter bit array as a grid of 0s and 1s
bit_array = bloom.bitarray.tolist()

# Set row width for better readability
row_width = 50
for i in range(0, len(bit_array), row_width):
    row = ''.join(['1' if bit else '0' for bit in bit_array[i:i+row_width]])
    print(row)
```

```
Inserted 831 chunks into Bloom Filter.

01000111111100111111000101001001001011001001110100000
00100010110001010010000000010101110100101001010100100
00100010011101001111000101100110111101100010001110
01100111011100011010001100001101011111000000011101
10101000010011011011011000000010000110101010111101
00111100111110011100111010010111100101000001100010
10011100000101000001011111001010001111011101010100
01011111110001110110011000010111111000111000010001
10101101111001011101001100100011011101101010011010
01010110111010100011101111011101100100011011101011
01111100000011001111101010101110010100011101111100
00001110100000100111110010110001001111000101001110
10101010010010111001001111101101001111000101100110
00110111111010010110100110111001010100111001110110
01001000000011010001000011110011010100011100100001
00000101101100100011011110111001111101110010000001
01101111111101011001101011000011001000100010101010
```

TIMELINE


JULY
AUGUST
SEPTEMBER
OCTOBER
w1
w2
w3
w4
Problem Analysis
Literature Survey
System Design
Implementation and Testing
Project Report
Completed Work
Pending Work

FUTURE SCOPE

- **Integration of Blockchain Layer**
  Implement a blockchain-based verification layer to ensure tamper-proof record keeping.

- **Performance Optimization**
  Enhance the system's efficiency to support large-scale data and faster verification.

FUTURE SCOPE

- **Cross-Platform Deployment**
  Extend the system for wider accessibility across multiple storage and user environments.

- **Improved Bloom Filter Optimization**
  Enhance the Bloom Filter design to reduce false positives and improve verification accuracy for larger data.

CONCLUSION

- This project aims to solve the problem of trust and tampering in cloud storage.

- This project aims to build a system that uses Bloom filters and Blockchain to check if data has been changed.

REFERENCES

- Liang et al., 2023. Privacy-Preserving Bloom Filter-Based Keyword Search Over Large Encrypted Cloud Data, IEEE Transactions on Computers, Vol. 72, No. 11, November 2023

- S.M.Udhaya Sankar et al., "A Secure Third-Party Auditing Scheme Based on Blockchain Technology in Cloud Storage," International Journal of Engineering Trends and Technology, vol. 71, no. 3, pp. 23–32, Mar. 2023.

- Chen et al., "A Decentralized Public Auditing Scheme for Secure Cloud Storage Based on Blockchain," Wireless Communications and Mobile Computing, vol. 2022, Article ID 3688164,Oct. 2022

REFERENCES

- S. Seethalakshmi and B. Balakumar, "Data Deduplication in a Blockchain-Enabled Big Data Ecosystem: Secure and Efficient Cloud Storage," SEEJPH, vol. XXVI, 2025. ISSN: 2197-5248. Posted: 04-Jan-2025

- Gebretsadik, F.G., Nayak, S., & Patgiri , R., *"eBF: an Enhanced Bloom Filter for Intrusion Detection in IoT,"* Journal of Big Data, vol. 10, article no. 102, 2023.

- Kasu, P.; Hamandawana, P.; Chung, T.-S. CRBF: Cross-Referencing Bloom-Filter-Based Data Integrity Verification Framework for Object-Based Big Data Transfer System. Appl. Sci. 2023, 13, 7830.

THANK YOU