



All



ADVANCED SEARCH

Conferences > 2023 International Conference... ?

Hyperledger Blockchain and Lightweight Bcrypt Symmetric Key Encryption to Boost Cloud Computing Security Effectiveness

Publisher: IEEE

Cite This



A. Banushri ; R.A. Karthika All Authors ...



162 Full Text Views

Alerts

Manage Content Alerts Add to Citation Alerts

Abstract

Document Sections

- I. Introduction
- II. Related Studies
- III. Proposed Method
- IV. Results and Discussion
- V. Conclusion

Authors

Figures

References

Keywords

Metrics

More Like This



Download PDF

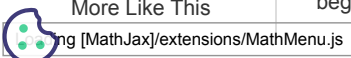
Abstract:

One of the key business models of contemporary information technology is cloud computing. It offers users a range of services (hardware, software) with little user engage... **View more**

Metadata

Abstract:

One of the key business models of contemporary information technology is cloud computing. It offers users a range of services (hardware, software) with little user engagement and at a reasonable price. Utilising a cloud environment raises several challenges, chief among them being security and privacy. This study explores the issues and proposes a Lightweight Bcrypt Symmetric Key (LBSK) data encryption and decryption technique with key rotation. A variety of algorithms and Blockchain technologies are used to protect the information. Encryption is one of the most fascinating features of data security technology. An Aggregated Authority Certificate Provider (AACP) is recommended with blockchain authentication for secured cloud data audit, which lessens the burden on the data owner. The suggested AACP continuously runs on a cloud server and tracks user requests. For the non-trusted provider, the Hyperledger blockchain proxy re-encrypts data to increase protection and privacy. The Blockchain algorithm was used to encrypt the data from beginning to end, and it was then saved in the cloud. Without storing the data locally, a security degree, public verification, and performance factors must be taken into consideration. Compared to current methods, the proposed strategy is intended to deliver a better result. The Blockchain technique was used to encrypt the data from beginning to end, and it was then saved on the cloud. Public verification and performance considerations raise the



security level for remote data verification without storing the data locally. In comparison to current methods, the proposed method offers a better result.

Published in: 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)

Date of Conference: 10-11 August 2023

DOI: 10.1109/ICCPCT58313.2023.10245926

Date Added to IEEE Xplore: 22 September 2023

Publisher: IEEE

► ISBN Information:

Conference Location: Kollam, India

☰ Contents

I. Introduction

The resources that are used to finish the process, in addition to the computing devices, can also be kept in the cloud. Similarly to that, big data is stored in the cloud. In general, there is a higher likelihood that data saved in the cloud will be stolen by unauthorized users. The businesses keep their info in the cloud and give users access to it. The organization's material is diverse and cannot be accessible to all users. Therefore, the user must be constrained by some guidelines. The method used to protect the data stored in the cloud is called cloud security. Numerous services, including Software as a Service (SaaS), Platform as a Service (PaaS), Data as a Service (DaaS), and others, are offered by the Cloud Ecosystem at different levels. Regardless of the service offered, all services utilize cloud-based data. The results of the services rely on many parameters, and the parameters are used to determine which data is accessed by the services from the cloud. The user will only be able to access the data if he has the necessary access, and the data dependency is dependent on the access restriction.

Authors	▼
Figures	▼
References	▼
Keywords	▼
Metrics	▼

More Like This

Blockchain Security Encryption to Preserve Data Privacy and Integrity in Cloud Environment

2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)

Loading (MathJax)extensions/MathMenu.js

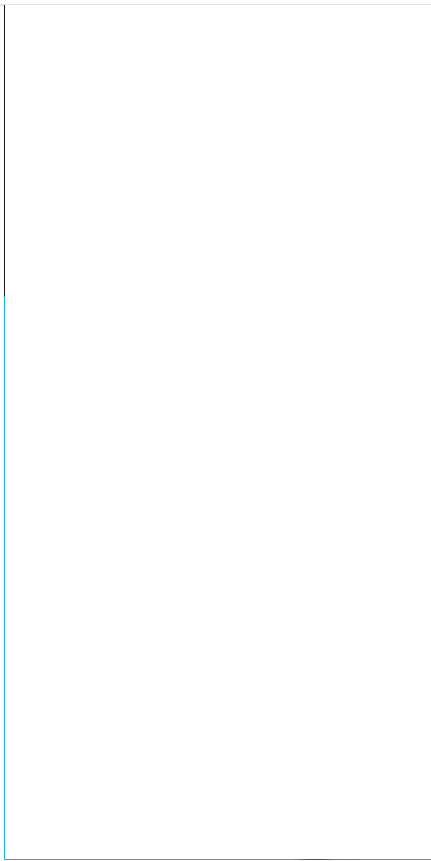
Published: 2023

Privacy Preserving in Blockchain Based on Partial Homomorphic Encryption System for Ai Applications

2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW)

Published: 2018

Show More



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow



About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

IEEE Account

» Change Username/Password

» Update Address
Loading MathJax Extensions/MathMenu.js

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

- » Communications Preferences
- » Profession and Education
- » Technical Interests

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » Contact & Support

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.