View access options

Export citation

Overview Citations References (19)

October 2023 · 4(6)
DOI: 10.1007/s42979-023-02155-8

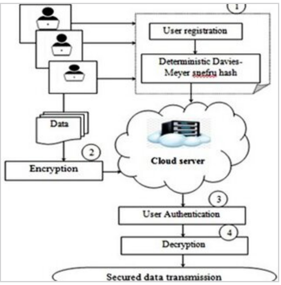
S. Radha · Jeyalaksshmi S.

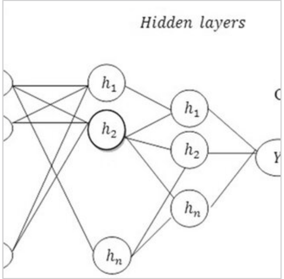
Citations 0

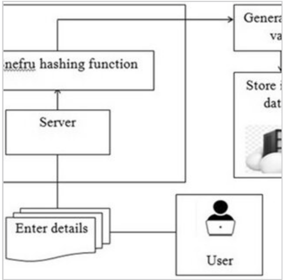
Reads 37

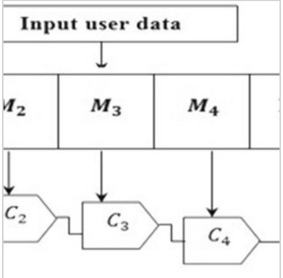
Abstract and figures

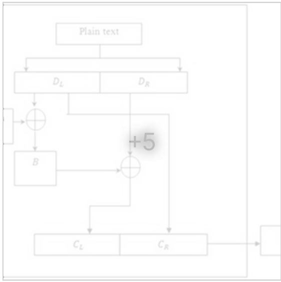
Advanced technology of Cloud Computing (CC) is to provide the services without straight executive of users and demand for resources. It is very scalable and vigorous as well as offers data access anywhere at any time over a cloud environment. Due to many users using the same shared computing resource, security is the more significant of cloud data privacy. User authentication is mainly perceptive defense issue in CC from unauthorized user accessed in cloud services. Various methods are improved in authentication security. However, it failed to improve the complexity of user authentication. Therefore, a novel technique called Deterministic Hash and Linear Congruential BlowFish Authenticated Extreme Learning (DHLCBAEL) method is redeveloped for improving accuracy and reducing the time consumption of accurate authentication. A different layer of isolated nodes is utilized by feed-forward neural network with extreme learning machine technique. The DHLCBAEL method includes four different layers, namely, input, two hidden layers, and an output layer carried for efficient user authentication. Initially, the number of users is specified to input layer by DHLCBAEL method. After that, DHLCBAEL method comprises two steps, namely User Registration and User Authentication at the hidden layer 1 and hidden layer 2, respectively. In the user registration step, the user registers their details and stores them on the cloud server using the Deterministic Davies–Meyer Snefru hash function. After that authentication process is carried out during data transmission. To encrypt the data, the symmetric key of cloud user uses the Lehmer congruential BlowFish cryptography algorithm. Next, it sends the ciphertext to cloud server. When the employer needs to enter the information using cloud server, then validate the authentication server their employer identity. During the authentication process, the DHLCBAEL method authenticates the user with help of a simple matching coefficient. When a user is legitimate or authorized, allows decrypting the data. Otherwise, the server denied the data access. In this way, user authentication performance by maximum accuracy and minimum time consumption is obtained at output layer. Performance evaluation of proposed DHLCBAEL method is implemented the various metrics, namely, data confidentiality, authentication time, authentication accuracy, as well as space complexity using amount of data with number of CU. The achieved outcomes specify to performance of proposed DHLCBAEL method increases authentication accuracy and confidentiality rate with minimum time and space complexity when comparative analysis of existing methods.











Content available from SN Computer Science

ResearchGate

Export citation

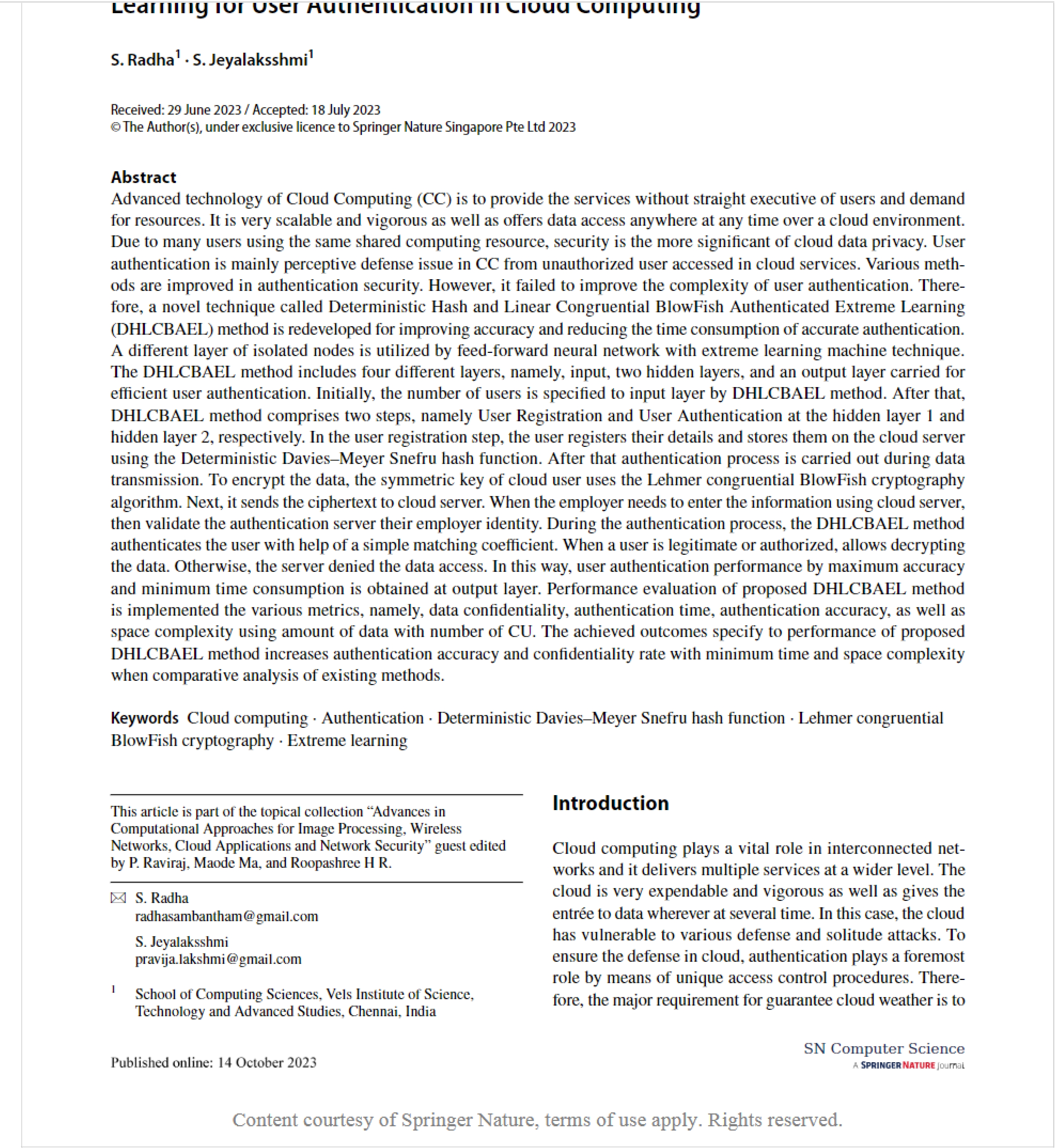
Publisher Previews (1)

A preview of this full-text is provided by Springer Nature.
Learn more

Content available from SN Computer Science

Page 1

Export citation



Learning for User Authentication in Cloud Computing

S. Radha[1] · S. Jeyalaksshmi[1]

Received: 29 June 2023 / Accepted: 18 July 2023

Abstract
Advanced technology of Cloud Computing (CC) is to provide the services without straight executive of users and demand for resources. It is very scalable and vigorous as well as offers data access anywhere at any time over a cloud environment. Due to many users using the same shared computing resource, security is the more significant of cloud data privacy. User authentication is mainly perceptive defense issue in CC from unauthorized user accessed in cloud services. Various methods are improved in authentication security. However, it failed to improve the complexity of user authentication. Therefore, a novel technique called Deterministic Hash and Linear Congruential BlowFish Authenticated Extreme Learning (DHLCBAEL) method is redeveloped for improving accuracy and reducing the time consumption of accurate authentication. A different layer of isolated nodes is utilized by feed-forward neural network with extreme learning machine technique. The DHLCBAEL method includes four different layers, namely, input, two hidden layers, and an output layer carried for efficient user authentication. Initially, the number of users is specified to input layer by DHLCBAEL method. After that, DHLCBAEL method comprises two steps, namely User Registration and User Authentication at the hidden layer 1 and hidden layer 2, respectively. In the user registration step, the user registers their details and stores them on the cloud server using the Deterministic Davies–Meyer Snefru hash function. After that authentication process is carried out during data transmission. To encrypt the data, the symmetric key of cloud user uses the Lehmer congruential BlowFish cryptography algorithm. Next, it sends the ciphertext to cloud server. When the employer needs to enter the information using cloud server, then validate the authentication server their employer identity. During the authentication process, the DHLCBAEL method authenticates the user with help of a simple matching coefficient. When a user is legitimate or authorized, allows decrypting the data. Otherwise, the server denied the data access. In this way, user authentication performance by maximum accuracy and minimum time consumption is obtained at output layer. Performance evaluation of proposed DHLCBAEL method is implemented the various metrics, namely, data confidentiality, authentication time, authentication accuracy, as well as space complexity using amount of data with number of CU. The achieved outcomes specify to performance of proposed DHLCBAEL method increases authentication accuracy and confidentiality rate with minimum time and space complexity when comparative analysis of existing methods.

Keywords Cloud computing · Authentication · Deterministic Davies–Meyer Snefru hash function · Lehmer congruential BlowFish cryptography · Extreme learning

Introduction

Cloud computing plays a vital role in interconnected networks and it delivers multiple services at a wider level. The cloud is very expendable and vigorous as well as gives the entrée to data wherever at several time. In this case, the cloud has vulnerable to various defense and solitude attacks. To ensure the defense in cloud, authentication plays a foremost role by means of unique access control procedures. Therefore, the major requirement for guarantee cloud weather is to

This article is part of the topical collection "Advances in Computational Approaches for Image Processing, Wireless Networks, Cloud Applications and Network Security" guest edited by P. Raviraj, Maode Ma, and Roopashree H R.

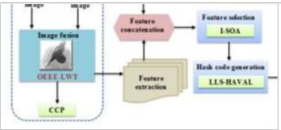
✉ S. Radha
radhasambantham@gmail.com

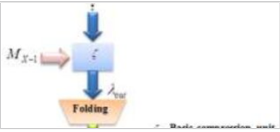
S. Jeyalaksshmi
pravija.lakshmi@gmail.com

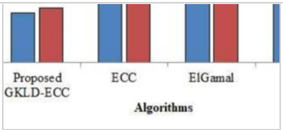
[1] School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies, Chennai, India

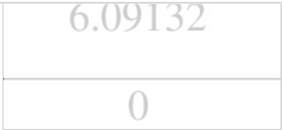
Published online: 14 October 2023

Export citation









Authorization Scheme for Secure Data Retrieval Using Lls-haval With Gkld-ecc in the Cloud

Preprint File available

April 2023 · 58 Reads

Chandra Shekhar Tiwari · Vijay Kumar Jha

The cloud platform is the best choice to provide more space for storing and transmitting data from one location to another in a fast manner for internet users. Nevertheless, while using cloud storage, several risks like data leakage and external attacks arise, especially owing to unauthorized users. Thus, to tackle these problems, this paper proposes Cued Click Points (CCPs) of the fused image with Galois...

Read more

View

ORTHOGONAL REGRESSED STEEPEST DESCENT DEEP PERCEPTIVE NEURAL LEARNING FOR IoT- AWARE SECURED BIG DATA COMMUNICATION

Article Full-text available

March 2023 · 18 Reads

Jordanian Journal of Computers and Information Technology

Saravanan V · Swapna S.L

The Internet of Things (IoT) is a collection of interconnected intelligent devices that exists within the larger network known as the Internet. With the increasing popularity of IoT devices, massive data is generated day by day. The collected data need to be continuously uploaded to the cloud server. Besides, the transmission of data in the cloud environment is performed via the internet, which faces numerous threats. However...

Read more

View

A novel and provably secure mutual authentication protocol for cloud environment using elliptic curve cryptography and fuzzy verifier

Article

August 2023 · 44 Reads · 1 Citation

Concurrency and Computation Practice and Experience

Export citation

distribute data processing among the various servers. Client stores their data on cloud server to maintain their data privacy and data security. The popular data security method which is called cryptography taking more time and space to encrypt and decrypt for data auditing...

Read more

View

Whirlpool Hash Mutual Biometric Serpent Authentication (WPHMBSA) for secured data access in cloud environment

Article

April 2022 · 9 Reads

Scientific and technical journal of information technologies mechanics and optics

Krishnan Mohana Prabha · Perumal Raja Vidhya Saraswathi · Saminathan Balamurali

Cloud systems allow data sharing capabilities for providing several benefits to users and organizations. However, authentication accuracy (AA) was not improved, and time consumption was not reduced. To increase authentication accuracy, Whirlpool Hash Mutual Biometric Serpent Authentication (WPHMBSA) Technique is designed to access data on a server in a secured manner. During the registration process, users' da...

Read more

View

ResearchGate

ResearchGate

Company

About us

Blog

Careers

Resources

Help Center

Contact us

Business Solutions

Marketing Solutions

Scientific Recruitment

Publisher Solutions

Export citation