IEEE.org IEEE *Xplore* IEEE SA IEEE Spectrum More Sites Donate Cart Create Account Personal Sign In

Browse My Settings Help

Access provided by:
Vels Institute of Science Technology & Advanced Studies (VISTAS)

Sign Out

Access provided by:
Vels Institute of Science Technology & Advanced Studies (VISTAS)

Sign Out

All

ADVANCED SEARCH

Conferences > 2023 2nd International Confer...

SSS-EC: Cryptographic based Single-Factor Authentication for Fingerprint Data with Machine Learning Technique

Publisher: IEEE

Cite This PDF

M. Nandhini Sharphathy ; V. Sumalatha **All Authors** •••

1
Cites in Paper

53
Full Text Views

Alerts

Manage Content Alerts

Add to Citation Alerts

Abstract

Downl
PDF

Abstract:
The development of cloud computing technology and big data comprises more users to store their data in the cloud server. The increases in the data volume and storage are ... **View more**

Metadata

Abstract:
The development of cloud computing technology and big data comprises more users to store their data in the cloud server. The increases in the data volume and storage are subjected to the increased risk of data access with unauthorized users. Traditionally, to improve data authorization the cloud data is encrypted before uploading to the server. To improve cloud authentication Single Factor Authentication (SFA) techniques are evolved. However, conventional SFA is not efficient for sensitive information that is able to be accessed by third parties. To overcome this limitation, this research proposes a Single-factor Samoa Substring Escrow Cryptography scheme (SSS-EC). The proposed SSS-EC model uses fingerprint biometric data for authentication in cloud data. Initially, Samoa Substring is implemented with the validation of the client single-factor i.e fingerprint data. The validated information is stored in the cloud escrow. The validated data is encrypted using homomorphic encryption. The encrypted data is accessed with the attribute structure those need to query and decrypt the data in the Samoa Substring. Upon the verification of the attribute i.e., fingerprint, cipher text based on Samoa Sub-String is shared between the owner and user without any keyword. The verification with the cipher text is performed with Elliptical Curve Cryptography (ECC). The implementation of the SSS-EC scheme improves authentication in the cloud. Finally, the Machine Learning (ML) method is implemented for the classification of the different attacks in the cloud server using CICIDS dataset. The

Keywords

Metrics

More Like This

simulation analysis of the proposed SSS-EC model with the existing authentication techniques such as Ring Learning with Errors (R-LWE) and Identity Concealed Authentication Scheme (ICAS) based on two factors is performed. The proposed SSS-EC exhibits higher authentication accuracy and reduced computational cost for the different users and cloud servers. The experimental results confirmed that the pr...

(Show More)

Published in: 2023 2nd International Conference on Edge Computing and Applications (ICECAA)

Date of Conference: 19-21 July 2023

DOI: 10.1109/ICECAA58104.2023.10212308

Date Added to IEEE *Xplore*: 16 August 2023

Publisher: IEEE

▸ **ISBN Information:**

Conference Location: Namakkal, India

Contents

I. Introduction

In recent years, the Single Factor Authentication (SFA) model has been adopted in a wide range of applications. In day-to-day life, network safety and privacy are increasing due to the emergence of technology (Tsiknas, K et al., 2021) [1]. The growth of internet applications and technologies such as Cloud exhibits significant effort towards networks and privacy (Chegini, H et al., 2021) [2]. The existing SFA comprises interrelated objects in which smart machines are connected without human intervention. Several applications such as farming, fingerprint, transportation, and so on used smart SFA devices (Kimani, K et al., 2019) [3]. Demands on application the SFA device properties are altered to minimise time and resource utilization (Saharkhizan, M et al., 2020) [4].

Sign in to Continue Reading

Authors

Figures

References

Citations

Keywords

Metrics

More Like This

Secured user's authentication and private data storage- access scheme in cloud computing using Elliptic curve cryptography
2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)

Published: 2015

Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems - performance analysis by simulations
2010 IEEE International Conference on Wireless Communications, Networking and Information Security
Published: 2010

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.

IEEE Account

» Change Username/Password

» Update Address

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