applied sciences

MDPI

Article

Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems

Zaid Alaa Hussien [1], Husam A. Abdulmalik [2], Mohammed Abdulridha Hussain [2], Vincent Omollo Nyangaresi [3], Junchao Ma [4,*], Zaid Ameen Abduljabbar [2,5,6,*] and Iman Qays Abduljaleel [7]

[1] Information Technology Department, Management Technical College, Southern Technical University, Basrah 61004, Iraq
[2] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
[3] Faculty of Biological & Physical Sciences, Tom Mboya University, Homabay 40300, Kenya
[4] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
[5] Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
[6] Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 518118, China
[7] Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah 61004, Iraq
* Correspondence: majunchao@sztu.edu.cn (J.M.); zaid.ameen@uobasrah.edu.iq (Z.A.A.)

Abstract: The information obtained from external sources within the cloud and the resulting computations are not always reliable. This is attributed to the absence of tangible regulations and information management on the part of the information owners. Although numerous techniques for safeguarding and securing external information have been developed, security hazards in the cloud are still problematic. This could potentially pose a significant challenge to the effective adoption and utilization of cloud technology. In terms of performance, many of the existing solutions are affected by high computation costs, particularly in terms of auditing. In order to reduce the auditing expenses, this paper proposes a well-organised, lightweight system for safeguarding information through enhanced integrity checking. The proposed technique implements a cryptographic hash function with low-cost mathematic operations. In addition, this paper explores the role of a semi-trusted server with regard to smart device users. This facilitates the formal management of information prior to distribution through the IoT-cloud system. Essentially, this facilitates the validation of the information stored and exchanged in this environment. The results obtained show that the proposed system is lightweight and offers features such as a safeguarding capability, key management, privacy, decreased costs, sufficient security for smart device users, one-time key provision, and high degree of accuracy. In addition, the proposed method exhibits lower computation complexity and storage expenses compared with those of other techniques such as bilinear map-based systems.

Keywords: data integrity; dynamic integrity checking; lightweight; semi-trust server; one time key; smart device user

Citation: Hussien, Z.A.; Abdulmalik, H.A.; Hussain, M.A.; Nyangaresi, V.O.; Ma, J.; Abduljabbar, Z.A.; Abduljaleel, I.Q. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. *Appl. Sci.* **2023**, *13*, 691. https://doi.org/10.3390/app13020691

Academic Editor: Dimitris Mourtzis

Received: 14 November 2022
Revised: 21 December 2022
Accepted: 30 December 2022
Published: 4 January 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The inherent adaptability and instantaneity serve to generate a number of advantages for the IoT. These include reductions in hardship in the regulation of storage, general information accessibility regardless of location, and evasion of capital costs for various items such as hardware, software, and individual upkeep [1].

The IoT-cloud system technology is recognised as being the most modern advancement for the structuring of IT corporations. This is because of its numerous unparalleled benefits such as on-demand self-service, pervasive network accessibility, context-independent asset sharing, quick asset flexibility, employment-based costs, and