

Conferences > 2018 1st Annual International...

## Improved Cloud Computing Security

Publisher: IEEE Cite This PDF

Rasha Talal Hameed ; Abdulatif Ali Hussain ; Omar Abdulwahabe Mohamad ; Khamis A. Zidan ; Omar Talal Hamid ; Saba Abdulbaqi Salman All Authors

1 Cites in Paper 325 Full Text Views



**Need Full-Text**  
access to IEEE Xplore for your organization?  
[CONTACT IEEE TO SUBSCRIBE >](#)

**Abstract**

**Document Sections**

- I. Introduction
- II. Cryptography Techniques
- III. Cloud Computing Keys System
- IV. Proposed Algorithm to Protect Data
- V. Proposed Algorithm to Generating Dvoamic Keys in the Cloud Computing

[Show Full Outline ▾](#)

**Authors**

**Figures**

**References**

**Citations**

**Keywords**

**Abstract:**  
A large number of computers which are linked, workable and organized called cloud computing. In the cloud computing area, many challenges like security, reliability, execution, and balancing of the load. The most important of these issues is cloud security. In this paper, we describe the algorithm which is used to improve cloud security. The proposed algorithm has been designed and implemented for generating dynamic keys in cloud computing based on multiple techniques. These techniques in our proposal have used the coding, permutations and reorder bit by the search method in artificial intelligence. Also, it depends on polynomial equations to expand the original key. The algorithm has the ability to manage clients, generating secret keys of varying length and damage the key after a period of use. Also, the proposed block cipher algorithm has been designed and implemented to protect the data that is sent between clients with high complexity based on a number of techniques.

**Published in:** 2018 1st Annual International Conference on Information and Sciences (AICIS)

**Date of Conference:** 20-21 November 2018 **DOI:** 10.1109/AICIS.2018.00041

**Date Added to IEEE Xplore:** 14 February 2019 **Publisher:** IEEE

**ISBN Information:** **Conference Location:** Fallujah, Iraq

**I. Introduction**  
A Cloud Computing is a service support by information technology via the internet. There are many risks when data transmitted or received such as hacking, loss of data, and modifying. The cloud services are used a third side which creates fr & the bluster to its privacy and security [1]. The most important data which is one path can be accomplished by several encryption approaches. This steps are: 1) Generating the privacy and keeps up the originality [2], [3] and [4]. Cryptography uses in many in different applications such as databases, electronic banking, military networks, and the different technology of user [5].

Sign in to Continue Reading

**More Like This**

**Implementation of an Encoding System with Dynamic Key Change Based on Pseudorandom Sequence Generators**  
2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)  
Published: 2024

**Attribute-based Encryption in Cloud Computing Environment**  
2020 International Conference on Computing, Electronics & Communications Engineering (ICCECE)  
Published: 2020

[Show More](#)

**The IEEE Open Journal of Power Electronics** has received its first Activated Go to Se