Parshvanath Charitable Trust's
A. P. SHAH INSTITUTE OF TECHNOLOGY
(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

Security on Public Cloud For file Storing

Group No. 03

Prabhanjan Amare – 15204039

Vaishnavi Rathod – 15104051

Kuvar Pratap Singh – 15204052

Project Guide

Prof: Apeksha Mohite

Contents

ABSTRACT

- We are working with honey and homomorphic encryption algorithm.

- When user saving file on cloud it is not secured, on some applications system admin can view files, but our apporach is to encrypt file on server with key it means whenever user will upload file on server he/she need to pass one key.

- This key may user can use as a unique key or same, after successfully uploaded file on server one email will shoot to user with file and its key for future ref and file will get ency and stored on server.

- If user want to retrived file again then simply he/she need to submit key before downloadng if key matches then successfully download file else one email will shoot to user alert user.and some wrong file will get download.

INTRODUCTION

- In the proposed system, the hybridization of homomorphic encryption and honey encryption technique will help to enhance the confidentiality of data.

- It will also improve the security of the data during data transmission through the digital communication channel.

- This hybridization technique can be used in various applications where data security is a major concern such as message transmission, cloud computation and defense sector.

Objectives

- In today's world of network, host, and application-level infrastructure security, data security becomes more important when using cloud computing at all "levels".

- The objective of this chapter is to help users evaluate their data security scenarios and make informed judgments regarding risk for their organizations.
- As with other aspects of cloud computing and security, not all of these data security facets are of equal importance in all topologies (e.g., the use of a public cloud versus a private cloud, or non-sensitive data versus sensitive data).

Literature Review

Paper Title: Hybrid homomorphic encryption based on the GM encryption algorithm which is additively (single bit) homomorphic, and RSA algorithm which is multiplicative homomorphic is used.

Authors: Zainab.H.M , Khinu S.M.M, Thanda .W, Mostapha.D

Publication details : Published on 16th Annual Conference on Privacy, Security and Trust (PST) in 2018

Finding : http://www.ijecs.in/index.php/ijecs/article/view/3999

Advantages: Cloud storage providers add additional layers of security to their services. Since there are many people with files stored on the cloud, these providers go to added lengths to make sure your files don't get accessed by someone who shouldn’t

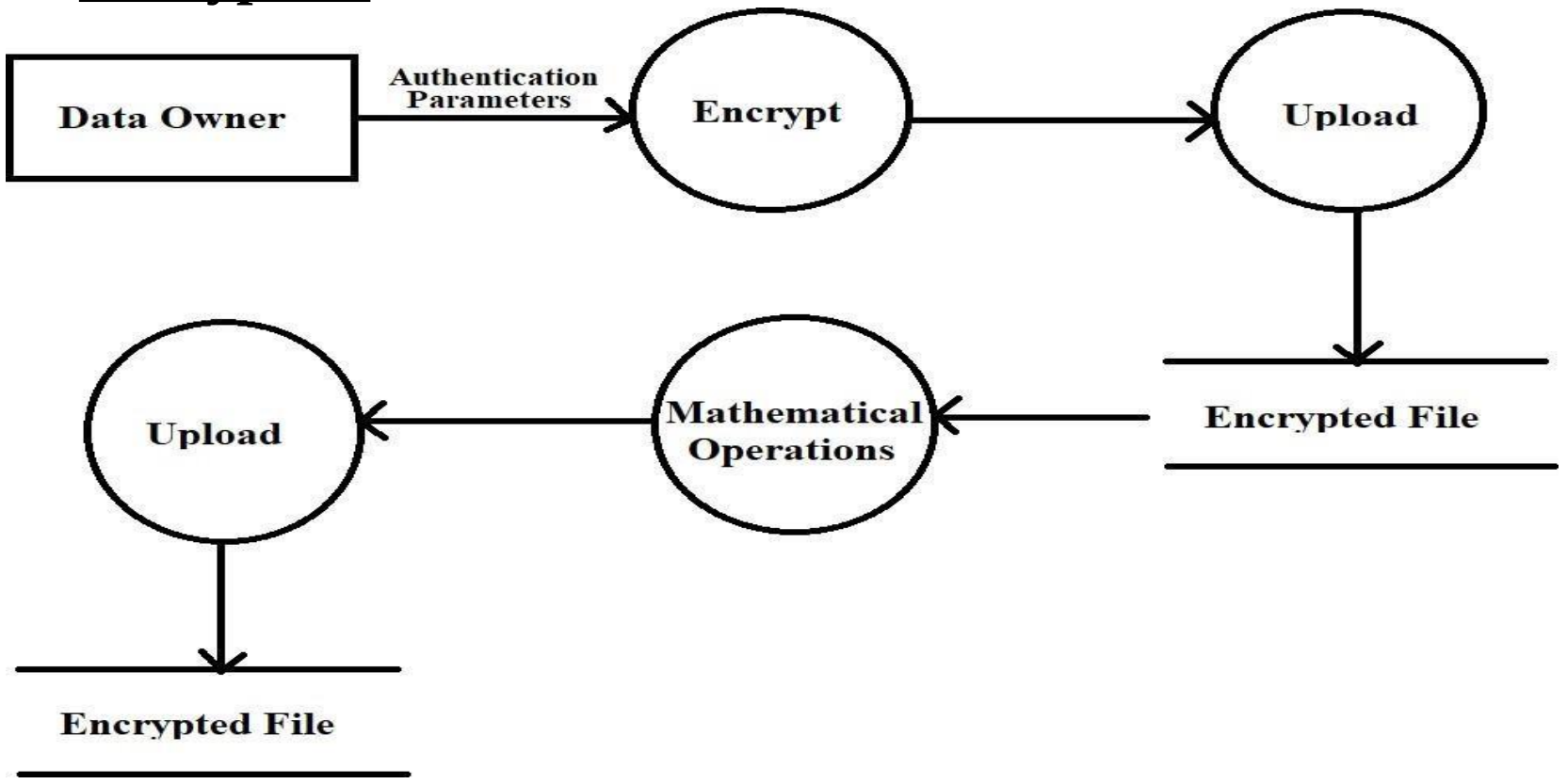
Disdvantages: Cloud based storage is dependent on having an internet connection. If you are on a slow network you may have issues accessing your storage. In the event you find yourself somewhere without internet, you won't be able to access your files.

Problem defination

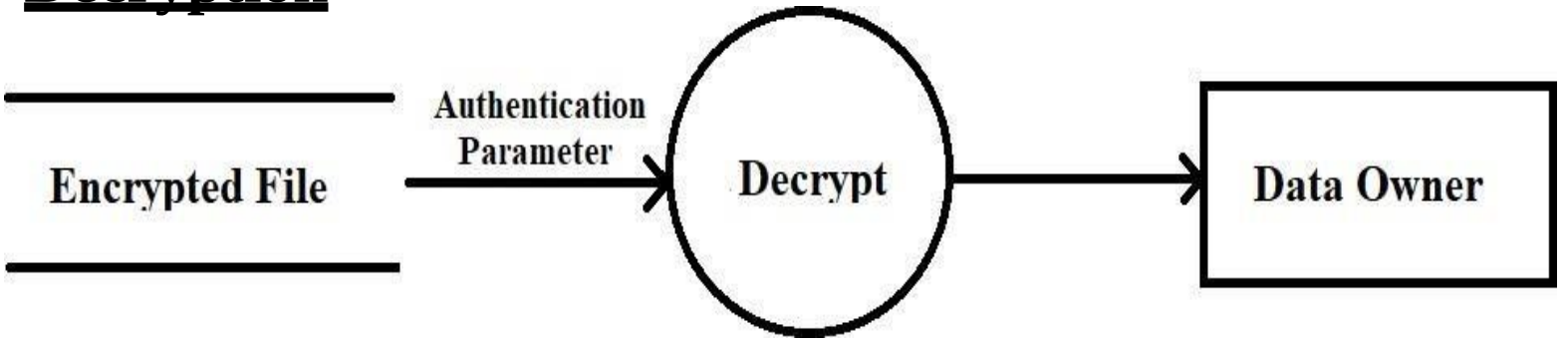
- With the rapid development of Cloud computing, more and more users deposit their data and application on the cloud.But the development of Cloud computing is hindered by many Cloud security problem.
- Cloud computing has many characteristics, e.g. multi-user, virtualization, scalability and so on.
- Because of these new characteristics, traditional security technologies can't make Cloud computing fully safe.
- Performing any mathematical operations on these data needs to be first decrypted which may sometimes lead to elevation of privilege as an unauthorized user may try to gain crucial data which is not meant for that user.
- However the attacker can try accessing those data which are in encrypted form using brute force attack. Thus, the confidentiality of data will be lost which is the major concern in digital communication.

Existing System Architecture/Working

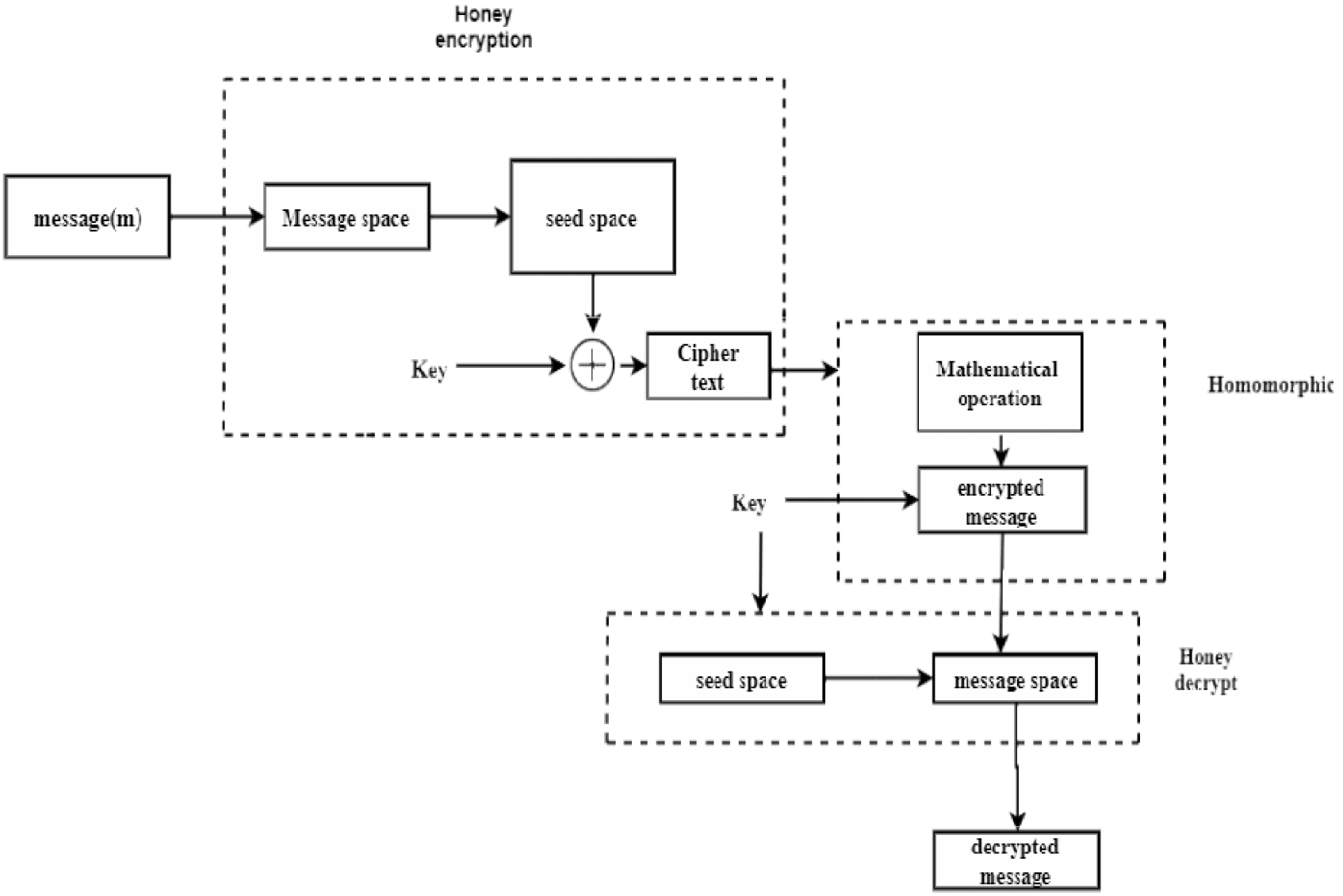
Encryption



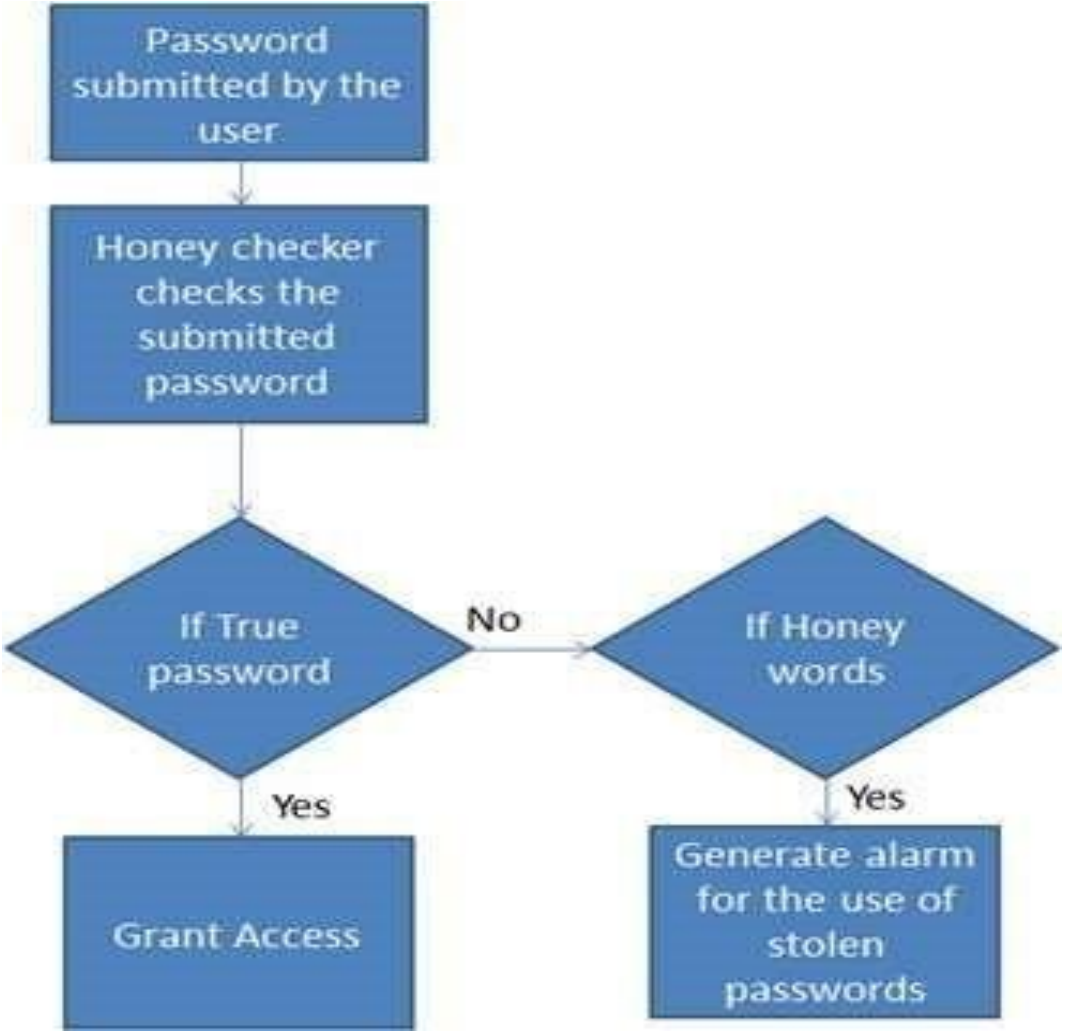
Decryption



Proposed System Architecture/Working



Honey encryption algorithm



SCOPE

- The proposed system will provide security beyond conventional brute-force bounds which will provide better confidentiality of data as these will make unauthorized accessing of data difficult for non-legitimate users.
- The proposed system can be used in various applications where protecting the private data is important such as mobile phone numbers, online payment transactions and debit card details.
- It will provide an additional data protection on the public cloud computing where large amount of crucial data are stored.

Thank You...!!