

Cryptic Cloud

*Project Report submitted
in partial fulfillment of the requirement for the degree of*

Bachelor of Technology

Department of Information Technology

Submitted By

**Surya Prakash
Tripathi**
(19107767)

**Prabhat
Gaurav**
(19107744)

**Babhravi Raje
Sharma**
(19107715)

Under the Supervision of

Dr Rohit Raja
Head of the Department
Information Technology



**DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF STUDIES OF ENGINEERING & TECHNOLOGY
GURU GHASIDAS VISHWAVIDYALAYA, BILASPUR (C.G.) -**

495009

March - 2023



गुरु घासीदास विश्वविद्यालय

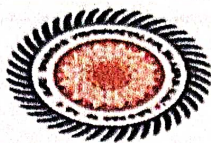
बिलासपुर (छ.ग.)

(केन्द्रीय विश्वविद्यालय)

कोटी, बिलासपुर-495009 (छ.ग.)

दूरभाष : 07752-260036, फैक्स - 07752-260154

वेबसाइट : www.ggu.ac.in



GURU GHASIDAS VISHWAVIDYALAYA
BILASPUR (C.G.)

(A Central University)

Koti, Bilaspur-495009 (C.G.)

Phone: 07752-260036, Fax : 07752-260154

Website : www.ggu.ac.in

CERTIFICATE

This is to certify that the project Report entitled “Cryptic-Cloud” project is being submitted by **Surya Prakash Tripathi** 19107767, **Babhravi Raje Sharma** 19107715, **Prabhat Gaurav** 19107744 in partial fulfilment for the **8th Semester of Bachelor of Technology in Information Technology** is a record of bonafide work carried out under my guidance and supervision. The results embodied in this project Report have not been submitted to any other University or Institute for the award of any Degree or any Diploma or any purpose whatsoever.

Signature

Dr. Rohit Raja
Head Of Department
Information
Technology

Abstract

One of the most pressing problems in cloud computing is data security and privacy regulation. Data kept in remote storage is dangerous and vulnerable to hacking. As a result, people are hesitant to trust their data in the cloud. Cloud customers want to know that they can access their data anywhere they want and that no one else can. Furthermore, user authentication via the cloud is a crucial consideration. After completing the survey and reviewing the research papers, it was discovered that the vital security problems of cloud computing are data leaking and distributed denial of service. (DDOS).

Implementing symmetric essential methods can increase data security by storing data on the server. Even if a person gains access, he cannot open the original data because it must be deciphered. Aside from storage security, enabling authorized user access may aid in avoiding DDOS because only real users will have access to the cloud.

A hybrid approach that combines elliptical curve cryptography and the symmetric essential technique is proposed. ECC is used to complete the user verification procedure and to keep sensitive data safe. The AES algorithm is utilized, which allows users to securely store and retrieve their data in the cloud by encrypting data on the client side and decrypting it after downloading from the cloud. Because the data user controls the private key, no one can decode the data, even if the hacker can obtain the data through some methods. Furthermore, while logging into the cloud server, the user will safely authenticate themselves by utilizing various input parameters. This approach can give consumers confidence in the security of data stored in the cloud.

Here, we will use an ECC and ECDH algorithm to achieve the same level of security as previous public critical cryptosystems while using a minor key size and strengthening the algorithm's security. The suggested solution's prototype would benefit from offering an appropriate access mechanism to prevent unwanted access to the information system and safe storage to allow data access through the cloud network.