

# Data Security in Cloud Computing Using AES Under HEROKU Cloud

**MICANS INFOTECH**

# Abstract

- ▶ Cloud security is an evolving sub-domain of computer and network security. Cloud platform utilizes third-party data centers model. An example of cloud platform as a service (PaaS) is Heroku.
- ▶ It supports several programming languages that are used for web application deployment model. Heroku is based on a managed container system, with integrated data services and a powerful ecosystem, for deploying and running modern apps.
- ▶ One essential issue in cloud computing is data security, which is handled using cryptography methods. A possible method to encrypt data is Advanced Encryption Standard (AES). In this paper, we implement Heroku as a cloud platform, then we implement AES for data security in Heroku.
- ▶ The performance evaluation shows that AES cryptography can be used for data security. Moreover, delay calculation of data encryption shows that larger size of data increases the data delay time for encrypting data.

# Existing

- ▶ Cloud computing technology can be implemented various architectures, and services with other technology with various software design approaches.
- ▶ Available service models for cloud computing, include infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Heroku is a cloud platform as a service (PaaS).
- ▶ Heroku supports various programming languages like Java, Node.js, Scala, Clojure, Python, and PHP. Heroku supports the development of cloud platform because it is free. Although it is free, it can also integrate with data services. It is a powerful system for deploying and running modern.

# Proposed

- ▶ It supports several programming languages that are used for web application deployment model.
- ▶ Heroku is based on a managed container system, with integrated data services and a powerful ecosystem, for deploying and running modern apps.
- ▶ One essential issue in cloud computing is data security, which is handled using cryptography methods.
- ▶ A possible method to encrypt data is Advanced Encryption Standard (AES). In this paper, we implement Heroku as a cloud platform, then we implement AES for data security in Heroku.

# HARDWARE REQUIREMENTS

- ▶ Processor – Pentium -III
- ▶ Speed – 1.1 Ghz
- ▶ RAM – 256 MB(min)
- ▶ Hard Disk – 20 GB
- ▶ Floppy Drive – 1.44 MB
- ▶ Key Board – Standard Windows Keyboard
- ▶ Mouse – Two or Three Button Mouse
- ▶ Monitor – SVGA

**MICANS INFOTECH**

# SOFTWARE REQUIREMENTS

- ▶ Operating System : Windows 8
- ▶ Front End : Java /DOTNET
- ▶ Database : Mysql/HEIDISQL

**MICANS INFOTECH**

# Conclusion

- ▶ In this paper, we proposed data security in cloud computing using AES under Heroku cloud. The implementation for deploying Heroku as a cloud platform consists of several steps.
- ▶ Then, we implement a website as an application to data security. In the website, we implement AES as data security algorithm. The performance evaluation shows that AES cryptography can be used for data security.
- ▶ Moreover, delay calculation of data encryption shows that larger size of data increases the data delay time for encrypting data.

# Reference

- [1] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.
- [2] L. Kacha and Abdelhafi Zitouni, "An Overview on Data Security in Cloud Computing," *Cybern. Approaches Intell. Syst.*, vol. 661, pp. 250–261, 2017.
- [3] J. R. N. Sighom, P. Zhang, and L. You, "Security Enhancement for Data Migration in the Cloud," *Secur. Enhanc. Data Migr. Cloud*, vol. 9, no. 23, pp. 1–13, 2017.
- [4] S. Kumari, Princy, Reema, and S. Kumari, "Security in Cloud Computing using AES & DES," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 5, no. 4, pp. 194–200, 2017.
- [5] D. Meng, "Data security in cloud computing," in *Computer Science & Education (ICCSE), 2013 8th International Conference on*, 2013, pp. 810–813.