CYVERSE®

Safeguard your sensitive data in iRODS using data encryption feature available in GoCommands

Illyoung Choi
CyVerse /
University of Arizona
iychoi@arizona.edu

Edwin Skidmore
CyVerse /
University of Arizona
edwin@cyverse.org

Tony Edgin
CyVerse /
University of Arizona
tedgin@arizona.edu

Nirav Merchant
CyVerse /
University of Arizona
nirav@arizona.edu

May 29, 2024
iRODS User Group Meeting

Working with sensitive data

- Strict confidentiality required by law
  - Example: HIPPA (Health Insurance Portability and Accountability Act) for life sciences
  - Data must be encrypted during storage and transmission

- Simple and effective data security policy
  - End-to-end encryption of selected data
  - Consistent encryption methods for data sharing

iRODS as a storage solution for sensitive data

- Built-in iRODS security measures
  - Authentication (PAM)
  - Role-based Authorization
  - Audit Trails
  - Data Transfer Encryption (SSL)

- Responsibilities of infrastructure provider
  - Encrypt data during storage
  - Ensure user compliance with security policies

Encryption feature in GoCommands

- Strong data encryption
  - Encrypt and decrypt both file names and content

Mode	Algorithm	Key
AES	AES-256-CTR	Password
SSH	RSA + AES-256-CTR	SSH Public/Private Keys

- Seamless operations (user-friendliness)
  - Encrypt on “put”, decrypt on “get”
  - “ls” command displays original file names for authorized users

Configurations in GoCommands

- Encryption mode
  - Default is "SSH"
  - "--encrypt_mode" flag to change mode

- SSH RSA keys for encryption/decryption (SSH mode)
  - Default is "~/.ssh/id_rsa" or "~/.ssh/id_rsa.pub"
  - "--encrypt_pub_key" and "--decrypt_priv_key" flags to locate key files
  - Note: a public key for encryption, a private key for decryption

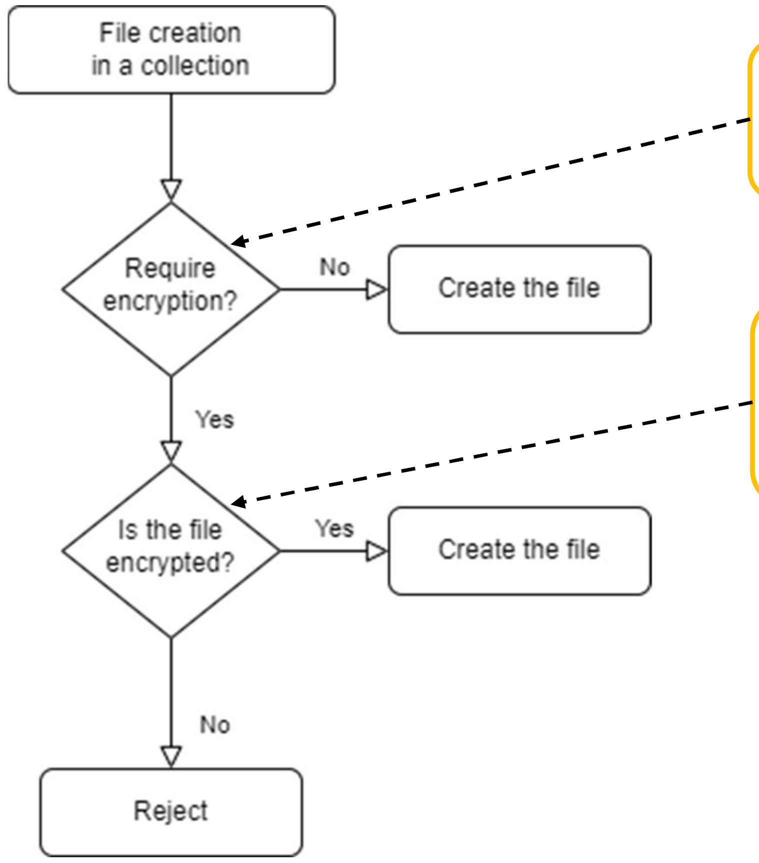
- Password for encryption/decryption (AES mode)
  - "--encrypt_key" and "--decrypt_key" flags

Configure a collection to require data encryption

- Set iRODS AVUs:

Attribute	Value	Note
“encryption::required”	“true” or “false”	
“encryption::mode”	“AES” or “SSH”	Default encryption mode

Enforcing data encryption with iRODS Rules



Check AVUs

"encryption::require"

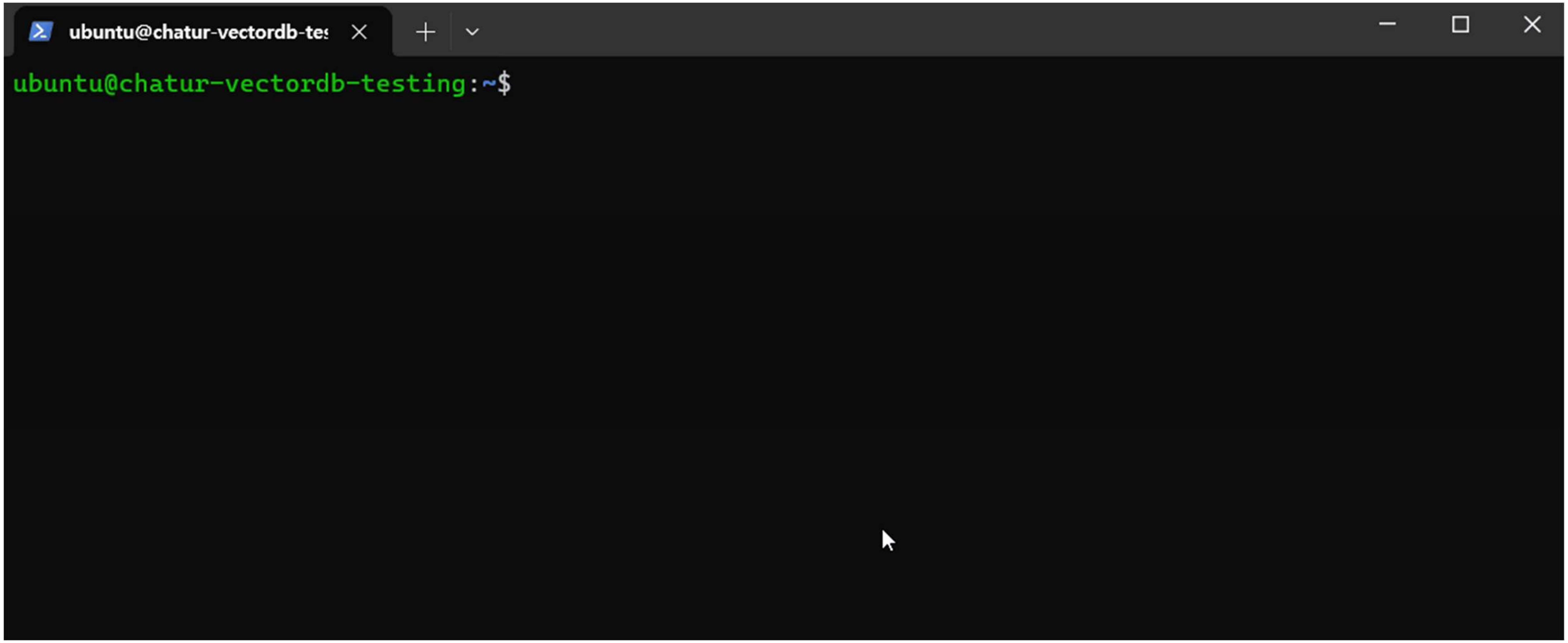
Check file extensions

hello.txt ➔ aqNisLexbJ7+A5I9S40xilt_+iUQPspwrw.rsaaesctr.enc

Implementation of iRODS Rules

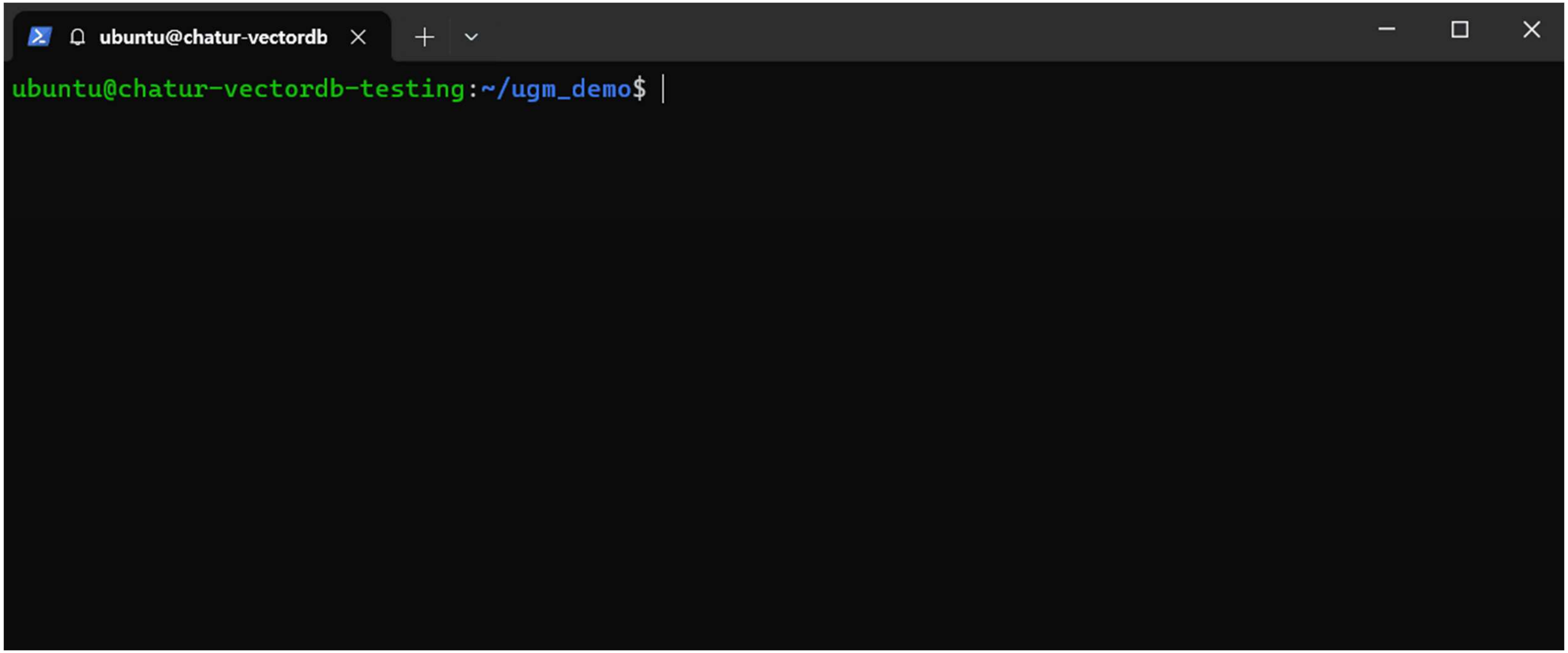
- PEPs for creating data objects
  - Reject data objects that are not encrypted
  - pep_api_data_obj_create_pre / pep_api_data_obj_create_and_stat_pre / pep_api_data_obj_open_pre / pep_api_data_obj_open_and_stat_pre
  - pep_api_data_obj_put_pre / pep_api_data_obj_copy_pre / pep_api_data_obj_rename_pre
- PEPs for creating sub-collections
  - Copy parent collection's AVUs to inherit
  - pep_api_coll_create_post / pep_api_data_obj_rename_post
- PEPs unhandled yet
  - pep_api_struct_file_ext_and_reg_pre: creates many sub-collections and data objects, "StructFileExtAndRegInp" serialization bug in iRODS < v4.3

Quick Demo - put



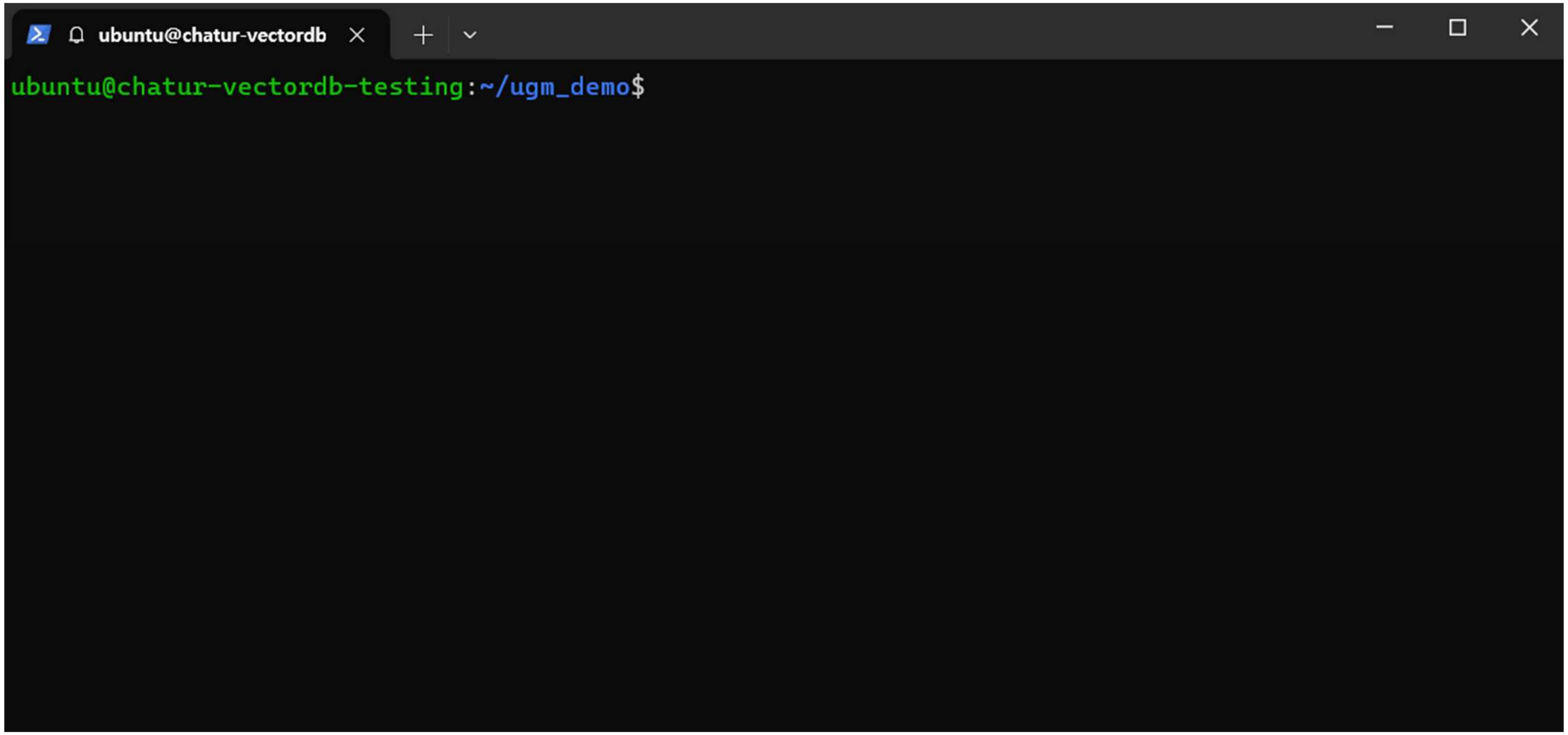
```
ubuntu@chatur-vectordb-testing:~$
```

Quick Demo - get



```
ubuntu@chatur-vectordb-testing:~/ugm_demo$
```

Quick Demo – encryption enforcement



```
ubuntu@chatur-vectordb-testing:~/ugm_demo$
```

Use-case: CyVerse Health

- iRODS-based data storage
  - SSL for data transfer encryption
  - **GoCommands** as a data access and encryption tool
  - **SFTP** (via SFTPGo for iRODS) for easy data access using GUI Tools (FileZilla / Cyberduck)

    (Encryption is not yet supported, future work)

Conclusion

iRODS as a secure data storage for sensitive data

- Encrypted data storage
- Enforce user compliance

Data encryption feature in GoCommands

- Strong data encryption for both file names and content
- Encryption modes: SSH (SSH RSA keys) or AES (password)

Data encryption enforcement in iRODS

- iRODS Rules reject creation of unencrypted files
- AVUs set to collections enforce encryption
- No additional setup required for users

Source code

GoCommands: https://github.com/cyverse/gocommands

iRODS Rules for encryption: https://github.com/cyverse/ds-playbooks/blob/main/irods/files/rule-bases/ipc-encryption.re

Questions?