Henry Bish

M12301126

11/29/2021

Data Security and Privacy

Project 3: Searchable Encryption

OS: Windows 10 version 1909 OS build 18363.1916

Python 3.9.7

External Requirements: click==7.1.2, pathlib==1.0.1, pycryptodome==3.10.4

How to compile:

1. Setup a virtual environment
2. Activate virtual environment
3. Run “pip install .” at ./se_m12301126 directory to compile code

Understanding File Structure:

./se_m12301126/se : This is analogous to a build and source folder

./se_m12301126/se/cli.py : click function that passes to commands

./se_m12301126/se/commands: Analogous to src. This is the folder where all the source code is

./se_m12301126/requirements.txt : Dependency list for se install. Same as external requirements.

./se_m12301126/data : Data folder

./se_m12301126/data/files : Folder holding plaintext files

./se_m12301126/data/ciphertexts : Folder holding ciphertext

./se_m12301126/setup.py : allows pip to install pow

./se_m12301126/report.pdf : the report you are reading

How to run:

Notes: All directory directions are run through pathlib so either / or \ can be used in writing directory paths. / is used in the default values.

KeyGen: se keygen

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se keygen --help
Usage: se keygen [OPTIONS]

Options:
  --sk_prf TEXT  name for new secret prf key
  --sk_aes TEXT  name for new secret aes key
  --help         Show this message and exit.
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126>
```

Figure 1: keygen help text

```
se keygen --sk_prf='./data/new_prf_key.txt' --sk_aes='./data/new_aes_key.txt'
```

Figure 2: Example of how to input custom values

Default values:

- --sk_prf = ’./data/sk_prf.txt’
- --sk_aes = ’./data/sk_aes.txt’

Enc: se enc

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se enc --help
Usage: se enc [OPTIONS]

Options:
  --sk_prf TEXT     name for new secret prf key
  --sk_aes TEXT     name for new secret aes key
  --index_loc TEXT  location where inverted index will be stored
  --files_loc TEXT  location of folder holding plaintext files
  --cf_loc TEXT     location of folder holding ciphertext files
  --help            Show this message and exit.
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126>
```

Figure 3: enc help text

```
se enc --sk_prf='./data/sk_prf.txt' --sk_aes='./data/sk_aes.txt' --index_loc='./data/index.txt'
se enc --files_loc='./data/files' --cf_loc='./data/ciphertexts'
```

Figure 4: Example of how to input custom values

Default values:

- --sk_prf = ’./data/sk_prf.txt’
- --sk_aes = ’./data/sk_aes.txt’
- --index_loc = './data/index.txt'
- --files_loc = ’./data/files’
- --cf_loc = ’./data/ciphertexts’

Token: se token

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se token --help
Usage: se token [OPTIONS]

Options:
  --keyword TEXT    keyword to search
  --sk_prf TEXT     location of the prf secret key
  --token_loc TEXT  location that the token generated will be saved
  --help            Show this message and exit.
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126>
```

Figure 5: token help text

```
se token --keyword='bengals' --sk_prf='./data/sk_prf.txt' --token_loc='./data/token.txt'
```

Figure 6: Example of how to input custom values

Default values:

- --sk_prf = ’./data/sk_prf.txt’
- --token_loc=’.data/token.txt’

Search: se search

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se search --help
Usage: se search [OPTIONS]

Options:
  --index_loc TEXT  location of the inverted index
  --token_loc TEXT  location that the token generated will be saved
  --cf_loc TEXT     folder that holds the ciphertext files
  --sk_aes TEXT     name for new secret aes key
  --help            Show this message and exit.
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126>
```

Figure 7: search help text

```
se search --index_loc='./data/index.txt' --token_loc='./data/token.txt' --sk_aes='./data/sk_aes.txt'
```

Figure 8: Example of how to input custom values

Default values:

- --index_loc = './data/index.txt'
- --token_loc=’.data/token.txt’
- --cf_loc = ’./data/ciphertexts’
- -- sk_aes = ’./data/sk_aes.txt’Results

Results

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se keygen
PRF secret key is 1eea5509f2f62fd7feb4ec6382ad61fe2dcc1c011a802465d27ae512e1997532
AES secret key is f34c205f8cf1905eb21d19437388c5329bdcb997c90cd15d02307bcfb037f2a8
```

Figure 9: Results of running keygen

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se enc
The inverted index is :
1e0880d9d7ddb88f4f4cef868aa1345f : ['c1.txt', 'c4.txt', 'c6.txt']
08a495f984f515b42c06652bc61d877f : ['c1.txt', 'c4.txt', 'c5.txt']
0a1b820965e52d05533caa8a5ca30b70 : ['c1.txt', 'c2.txt', 'c3.txt', 'c5.txt']
4b69c8b2e8b7d132b5e07a95fbfbce79 : ['c2.txt']
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126>
```

Figure 10: Results of running enc

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se token --keyword='bengals'
Inputted token is bengals
Generated token is 1e0880d9d7ddb88f4f4cef868aa1345f
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126>
```

Figure 11: Results of running token

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se search
['c1.txt', 'c4.txt', 'c6.txt']
b'bengals steelers packers '
b'steelers bengals'
b'bengals'
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126>
```

Figure 12: Results of running search with the encrypted token bengals

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se search
['c1.txt', 'c4.txt', 'c5.txt']
b'bengals steelers packers '
b'steelers bengals'
b'steelers packers'
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126>
```

Figure 13: Results of running search with the encrypted token steelers

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se search
['c1.txt', 'c2.txt', 'c3.txt', 'c5.txt']
b'bengals steelers packers '
b'packers patriots'
b'packers'
b'steelers packers'
```

Figure 14: Results of running search with the encrypted token packers

```
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126> se search
['c2.txt']
b'packers patriots'
(.venv) PS C:\Users\bishhc\Documents\DataSecurity\se_m12301126>
```

Figure 15: Results of running search with the encrypted token patriots