Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 8 ~ Issue 6 (2022) pp: 27-32
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Data Encryption Strategy to Withhold Privacy Based On Data-Weights

Dr.RAHIMUNNISA.K[1]
Department of Electronics and Communication Engineering , Easwari Engineering College, Chennai ,Tamil Nadu ,India.

KEERTHANA.M[2]
Department of Electronics and Communication Engineering, Easwari Engineering College, Chennai ,Tamil Nadu ,India.

POOJITHA.S.K[3]
Department of Electronics and Communication Engineering, Easwari Engineering College, Chennai ,Tamil Nadu ,India.

ABSTRACT: Increased usage of data in today's world, places data safety concern at the top of privacy risk management agenda. It is an inescapable challenge to face the arising consequences of the privacy issue.The execution time in data encryption occupies the next place of concern in data processing and transmissions.With reference to the theme , an approach is designed to attain the privacy protection scope under the utilization of a selective encryption strategy named Dynamic encryption strategy . The usage of strategy under D2ES model evaluates the performance of the experiment, on the basis , which provides the proof of privacy enhancement under required execution time constraints.

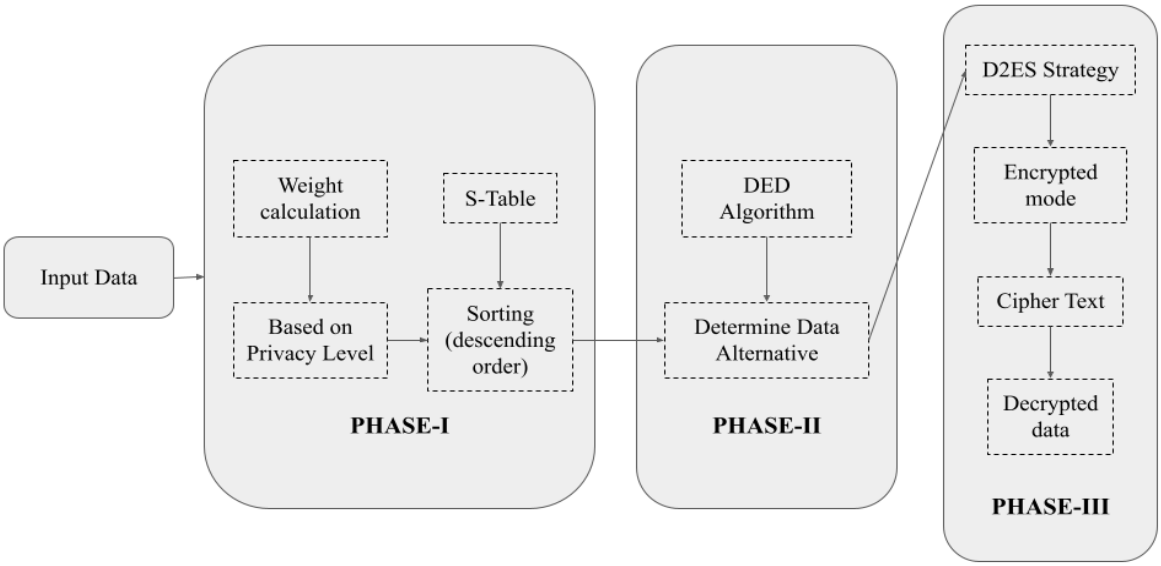
KEYWORDS: Privacy, Time constraint, Encryption, Decryption, Data package, Transmission, Weight calculation, Sorting, Key value, Encode, Cipher text, D2ES strategy, DED algorithm

***R**eceived 12 June, 2022; **R**evised 24 June, 2022; **A**ccepted 26 June, 2022 © The author(s) 2022.*
P**ublished with open access at **www.questjournals.org

I. INTRODUCTION

The global penetration of big data technology has significantly extended the channels of obtaining information through all platforms, resulting in privacy concerns.Furthermore, as an emerging technology, big data has spread into innumerable industries, resulting in the public introduction of many new service deployments, such as mobile parallel computing and distributed scalable data storage. Big data has been widely employed in a variety of industrial domains and studied in recent research due to its status as one of the technical mainstreams.To resolve the inconsistency, a Dynamic Data Encryption approach was implemented to ensure data package safety dependent on privacy levels. The D2ES model in the experiment mainly focuses on two approaches. The first addresses on classifying data packages based on privacy level and the next approach determines whether data packages can be encrypted within the time constraints.DED algorithm under D2ES model checks for constraint limits and works for data encryption alternatives.The algorithm provides maximum privacy weight value .In combination with sequel and python programming language ,plain text is being uploaded into a parallel python based webpage . Encryption process is carried out in reference with weight value which in accordance generates a STABLE (sorting table) . Further cipher text is being generated based on the STABLE. The generated cipher text indicates the privacy enhancement of the experiment. The level of privacy is the most important component in data security. As a result, by achieving maximum data security, the level of privacy is raised in compliance. The above approach is primarily used in Big Data environments where the encryption process is critical for data security. The DED (Dynamic Encryption Determination) technique is primarily utilised to achieve the goal under the D2ES strategy (Dynamic Data Encryption Strategy). The approach also selectively encrypts the data to maximise the protection level under execution time constraints .

II.PROPOSED METHODOLOGY



Input data packages are loaded into the privacy weight value calculation system.
In accordance with the D2ES model and DED algorithm the highest possible privacy weight value is calculated.The loaded data packages are directed into the first phase of the experiment.

PHASE -I:

Loaded data undergoes a weight calculation mechanism and is classified based on the privacy level.The data packages which hold maximum weights are considered to be under highest privacy protection scope. Corresponding weights are sorted in order with the following lower privacy protection scope.

The above data packages are sorted under privacy scope based on the weight values .Data packages are further classified into a table based on the privacy scope.The data is sorted under descending order based on the previous privacy scope.The above organised values are formed into a table named S-TABLE .S-TABLE (ie..) sorting table displays data corresponding to privacy weight value in descending order . The sorted table always corresponds to a data sequence only under descending order.The corresponding sorted data is progressed to the next Phase.(ie…)PHASE-II .

PHASE-II:

The following sorted data from phase-I is incorporated into this phase. The sorted data undergoes a DED algorithm check.The previous sorted table estimates time constraint for each data package . The data packages that hold minimum time constraints are left in the same process. Those data packages which hold higher execution constraints are moved for algorithm check procedure . DED (Dynamic Encryption Determination algorithm) takes in data packages which consume high time constraints and checks for alternatives.The algorithm works for alternative data formats which confine minimum time constraint.Dynamic encryption algorithm also ensures maximum safety in encryption and transmission of data packages.Thus the above data from S-TABLE undergoes data alteration process using DED algorithm and shifts to the next phase .

PHASE-III:

The sorted data from phase-II is incorporated under D2ES strategy in phase-III.

The data packages are fed into the model wherein the data sets undergo an encryption process. The data packages are encrypted based on the random key generation process. The random key generates a random key which encrypts data with highest privacy. The first package in S-TABLE with highest privacy is encrypted initially with a key generation process resulting in maximum privacy protection scope.The encrypted data package can be decrypted with the key value which is formed during random key generation process. The resulting decrypted value ensures the highest privacy protection scope following the execution time constraint limit.Thus this decrypted value corresponds the data package with highest Privacy Weight Value(PWV).

III.DYNAMIC DATA ENCRYPTION STRATEGY(D2ES)-MODEL

Inorder to enhance the data privacy , D2ES model is implemented into the process.The main objective of the model is to minimise the inconvenience caused during the data transmission. To attain the intent , two major techniques are carried over under the process.
I-Classify data packages based on the privacy level.
II-Depicts whether data packages can be encoded under execution time constraints.
In accordance with the DED algorithm , the privacy level has been enhanced in the encryption process.

IV.DYNAMIC ENCRYPTION DETERMINATION ALGORITHM

Dynamic encryption algorithm is intended to strengthen the privacy protection strategy under the process.The main objective is to determine the time constraints and to check for data alternatives . Algorithm selects data packages with the highest priority first and calculates the estimated time for the remaining data packages.With reference to the priority levels, DED algorithm generates S-TABLE and M-TABLE.

I-S-TABLE:
sorted table based on file size and determined execution time

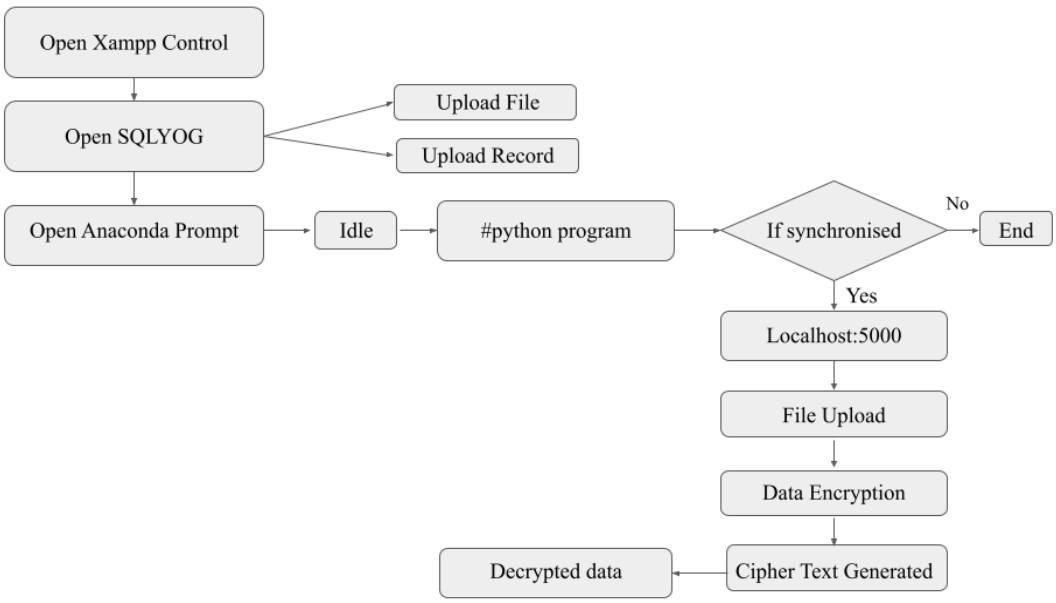
II-M-TABLE:
Table displaying calculated weights in reference with privacy level.

In accordance with the S-TABLE,M-TABLE the parameters calculate in DED algorithm are as follows:

- Privacy weight value
- Total execution time remaining

Based on the PWV(privacy weight value) the data packages are encrypted as per the S-TABLE (sorting table).

V.EXPERIMENTAL SETUP

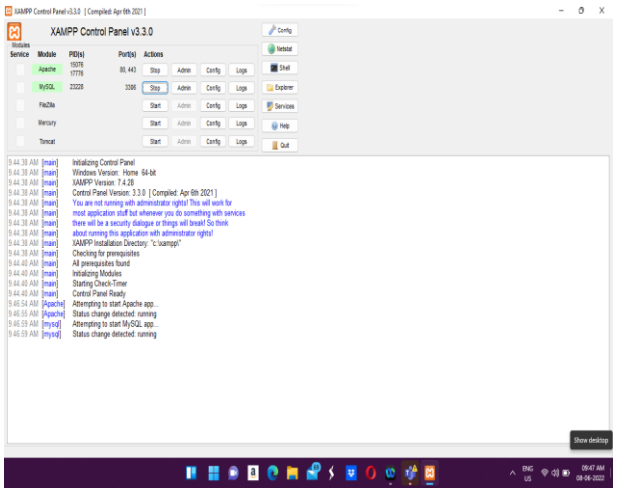


- PC/LAPTOP
- OS-WINDOWS
- RAM-2GB MIN
- HARD DISK-150GB
- MOUSE
- PLATFORM-ANACONDA
- BACKEND-XAMPP CONTROL
- BACKEND-SQLYOG
- LANGUAGE-PYTHON

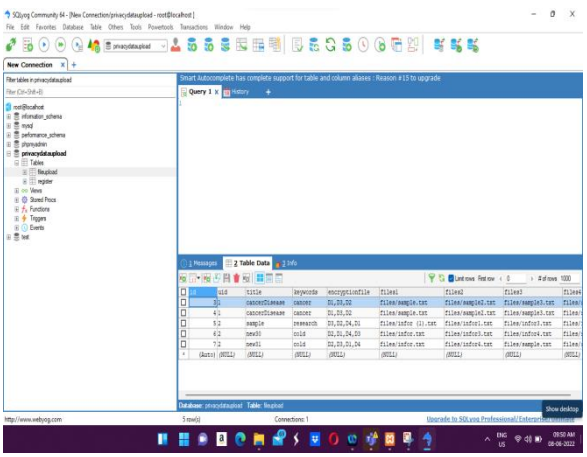
Open XAMPP CONTROL PANEL . A dialog box appears with the backend softwares to connect with the server . A Toggle button will ensure a connection between the softwares in server . click on the start/stop button to enable connection under a single server. First 2 columns in the xampp panel are Apache and MySQL. Enable the toggle button to connect with the above 2 softwares.(apache , MySQL).
The apache allows access to http.config files , py files, module.files and other databases . MySQL connection promotes access to all SQL databases , which is required to upload data , records into the experiment.Thus in this procedure , the Xampp control panel ensures connection between the softwares (SQLYOG, localhost:5000).
Next open , SQLYOG COMMUNITY. The sqlyog software is used to store databases in the software . sqlyog holds files and records that are required to process the experiment . under privacy data upload column (ie,..the experiment)
Load the data packages under fileupload and register rows . open the loaded data in a new table under both the rows (ie../ fileupload, register). The uploaded data is connected with the backend software (say, localhost:5000) using the XAMPP control panel. These data packages are stored under sqlyog for further manipulation and encryption.
After connecting XAMPP with SQLyog, Open the python file with ANACONDA PROMPT under the idle environment . open the precoded python file in the idle environment . tap the RUN module and wait until the module returns the connection scope between the softwares .
After confirming the synchronisation of the above code and sequel unlock,
localhost:5000 module-coded webpage. An http.config web page opens with login details.Pre- signed users can login the web page with direct access to their mail and password . New users can sign-in , in the process to create a new account for the experiment . After completing the access part , the webpage directs to a new slide . There, Create a name for the new encryption process, and upload the data packages in file format under file upload strategy . click on the file upload button which directs to another slide ,click on the new popup button (dynamic -strategy) , which displays the sorted value based on the privacy weight value .S-TABLE displays data in descending order based on privacy weight value . The S-TABLE adds a download option with it , which shows-off the decrypted text of the input data package .

VI.OUTPUT

XAMPP control panel:

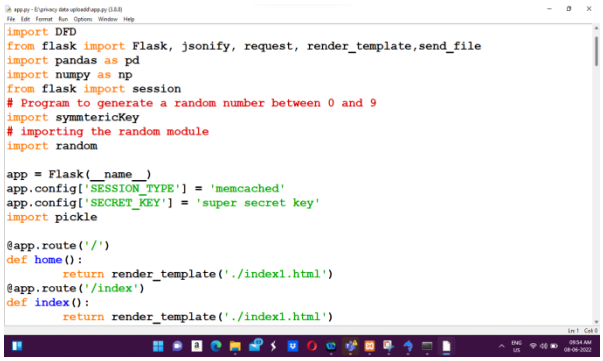


SQLyog:

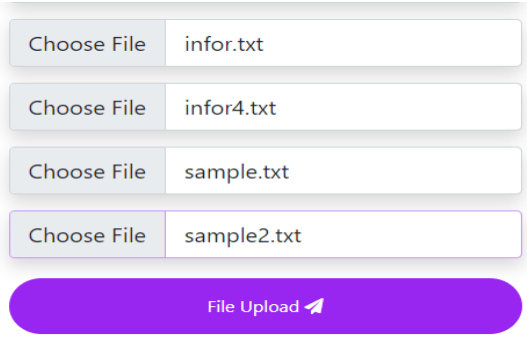


PYTHON program:

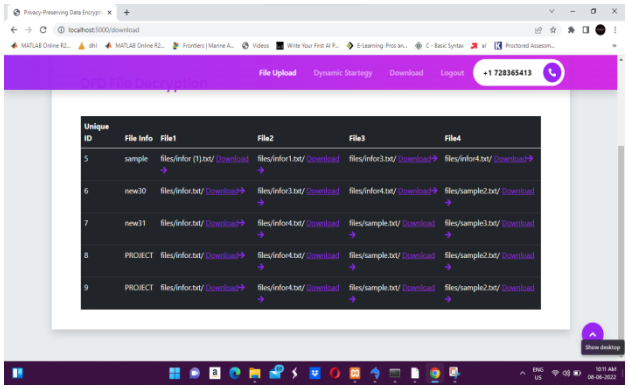
LOCALHOST:5000:



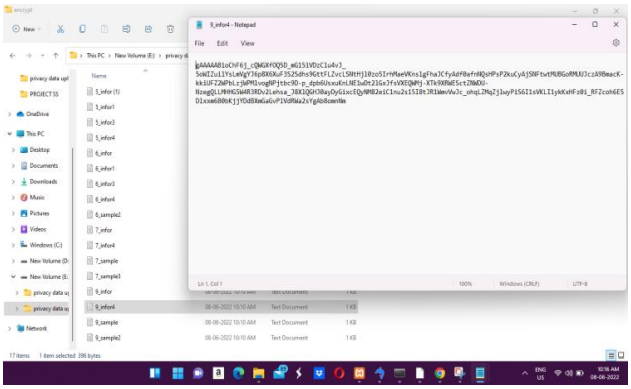
```
import DED
from flask import Flask, jsonify, request, render_template,send_file
import pandas as pd
import numpy as np
from flask import session
# Program to generate a random number between 0 and 9
import symmtericKey
# importing the random module
import random

app = Flask(__name__)
app.config['SESSION_TYPE'] = 'memcached'
app.config['SECRET_KEY'] = 'super secret key'
import pickle

@app.route('/')
def home():
        return render_template('./index1.html')
@app.route('/index')
def index():
        return render_template('./index1.html')
```



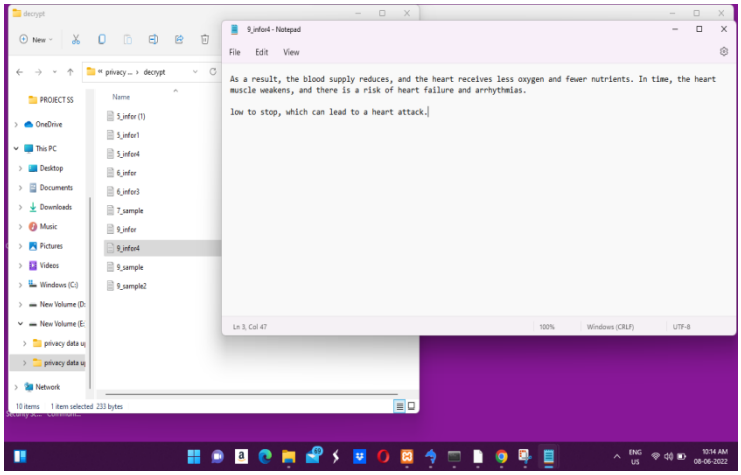
S-TABLE:



ENCRYPTED FILE:



DECRYPTED FILE:



Followed by the enabled connections ,encryption process returns the decrypted
Value of the input data packages corresponding to higher privacy enhancement within limited execution time constraints.

VII.RESULT AND DISCUSSION

The proposed approach proves higher privacy enhancement within limited execution time constraints. Utilization of DED algorithm under D2ES strategy
helped the process to attain a higher enhancement rate.The experimental evaluations exhibit high adaptivity with elevated execution results.The process also paves way for the extension of the experiment under cloud computing environment with increased encryption strategies to attain higher privacy levels..

REFERENCE

[1]. Keke Gai, Meikang Qiu, Hui Zhao "Privacy Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing" October.2021,Vol. 7.

[2]. Muhammad BaqerMollah et.al "Security and Privacy Challenges in Mobile Cloud Computing: Survey and way ahead" Journal of Network and Computer Applications, April 2017, Vol. 84.

[3]. Smitha Kurian, Bibek Gautam, Farhan Ahmed, Ganesh chaulagain, Manjunath Y "Privacy Preserving Data Encryption Strategy for Big Data on Cloud" June-August 2019, Vol.4.

[4]. Sellam V, S Vivek Reddy, K Praveen, G C Krishna, J Abhinay Rao "Secure Data Encryption Strategy for Big Data in Mobile Communication" October 2019, Vol.9.

[5]. Chandana K S, Ankitha K Udupa, Nalina V "Privacy Preserving Data Encryption Strategy in Cloud Computing" June 2020, Vol.16

[6]. NiLi, Zhenhua Chen, Jingjing Nie, Xingbing Fu, Xingxing Jia "Complementary set Encryption for Privacy Preserving Data Consolidation" May 2022, Vol.593.

[7]. Ch.Mounika, N.Koteswar Rao, P.Priya, R.Bhargavi, V.G.Kanya "Privacy Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing" April 2018, Vol.5.

[8]. Sumit Vikram Tripathi, Ritukar, Prof.Murthy B, Dr.K.S.Jagadeesh Gowda "Privacy Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing Environment" May 2018,Vol.7 .

[9]. Divya L, Dr.Udaya Rani "Privacy Preserving for Big Data in Mobile Cloud-Computing using Encryption Strategy" 2010.

[10]. G.Sravani, Dr.B.Geetha Vani "Execution of Data Encryption Strategy in Mobile Cloud Computing" July 2018, Vol.5.

[11]. Yibin Li et.al "Mobile Cloud Framework to prevent Data Over-Collection" 2016 Vol.6.

[12]. Zhibin Zhou, Dijiang Huang "Efficient and Secure Data Storage Operations for Mobile Cloud Computing" 2011, Issue 185