National College of Ireland

Configuration Manual

MSc Research Project
Msc CYBER SECURITY

Salman Ahmed
Student ID: x23189801

School of Computing
National College of Ireland

Supervisor: Jawad Salauddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Salman Ahmed
Student ID:	x23189801
Programme:	Msc Cyber Security **Year:** 24-25
Module:	PRACTICCUM 2
Lecturer:	Jawad salauddin
Submission Due Date:	12 Dec. 24
Project Title:	Practiccum2
Word Count:	**Page Count:**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Salman ahmed
Date:	12 Dec. 24

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

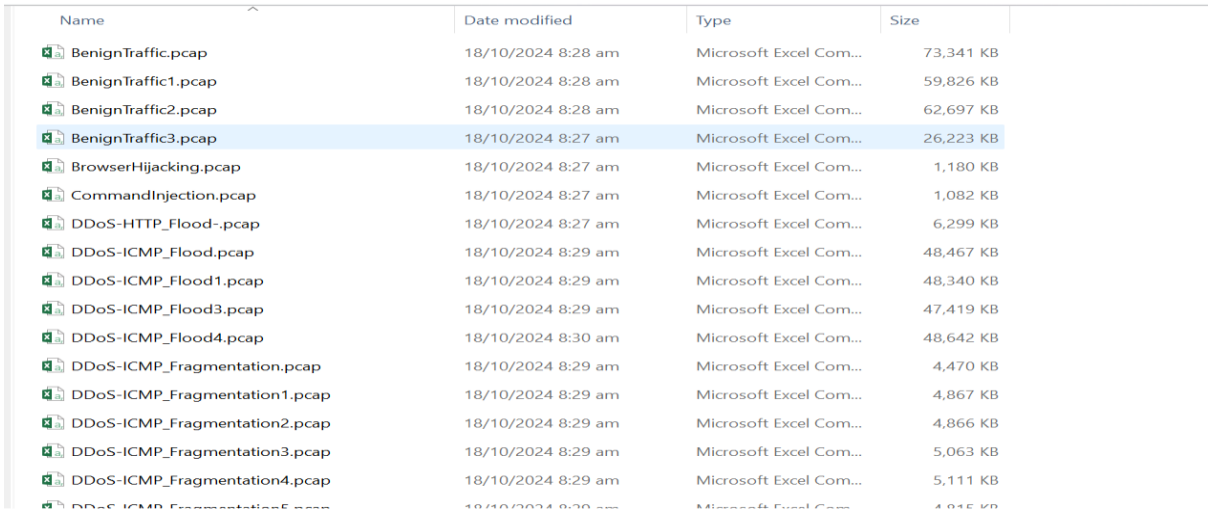
Salman Ahmed
Student ID: x23189801

1 Data Coverage

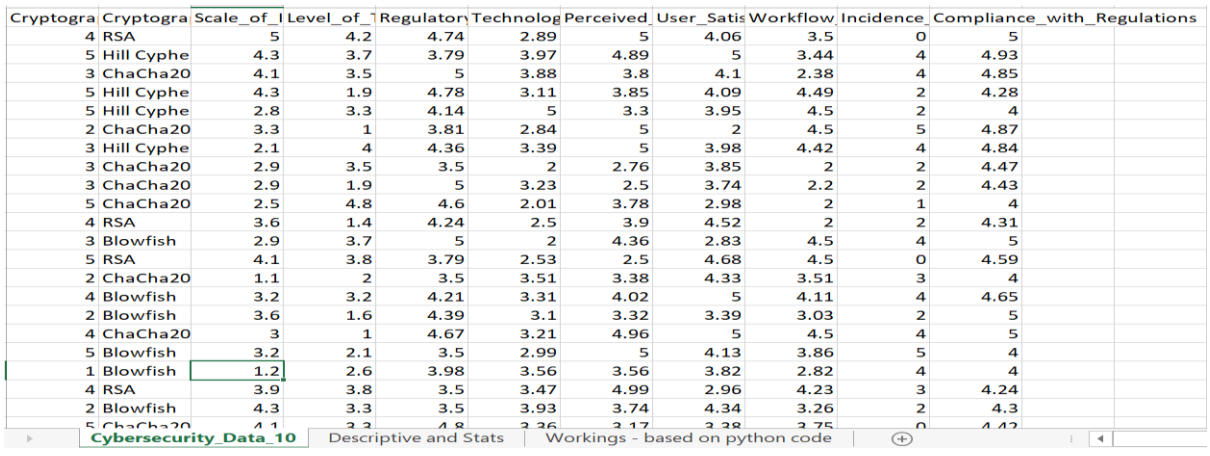
The study utilizes the combination of secondary and observational data to examine cryptographic techniques efficiency and effectiveness in protecting the financial data.

A few secondary data has been utilized from UNSW-NB15 data points which covers huge record of raw-network packets.

Rest of the data has been observational from reports and financial breaches along with variables from high-end reports of renowned institutions.



Name	Date modified	Type	Size
BenignTraffic.pcap	18/10/2024 8:28 am	Microsoft Excel Com...	73,341 KB
BenignTraffic1.pcap	18/10/2024 8:28 am	Microsoft Excel Com...	59,826 KB
BenignTraffic2.pcap	18/10/2024 8:28 am	Microsoft Excel Com...	62,697 KB
BenignTraffic3.pcap	18/10/2024 8:27 am	Microsoft Excel Com...	26,223 KB
BrowserHijacking.pcap	18/10/2024 8:27 am	Microsoft Excel Com...	1,180 KB
CommandInjection.pcap	18/10/2024 8:27 am	Microsoft Excel Com...	1,082 KB
DDoS-HTTP_Flood-.pcap	18/10/2024 8:27 am	Microsoft Excel Com...	6,299 KB
DDoS-ICMP_Flood.pcap	18/10/2024 8:29 am	Microsoft Excel Com...	48,467 KB
DDoS-ICMP_Flood1.pcap	18/10/2024 8:29 am	Microsoft Excel Com...	48,340 KB
DDoS-ICMP_Flood3.pcap	18/10/2024 8:29 am	Microsoft Excel Com...	47,419 KB
DDoS-ICMP_Flood4.pcap	18/10/2024 8:30 am	Microsoft Excel Com...	48,642 KB
DDoS-ICMP_Fragmentation.pcap	18/10/2024 8:29 am	Microsoft Excel Com...	4,470 KB
DDoS-ICMP_Fragmentation1.pcap	18/10/2024 8:29 am	Microsoft Excel Com...	4,867 KB
DDoS-ICMP_Fragmentation2.pcap	18/10/2024 8:29 am	Microsoft Excel Com...	4,866 KB
DDoS-ICMP_Fragmentation3.pcap	18/10/2024 8:29 am	Microsoft Excel Com...	5,063 KB
DDoS-ICMP_Fragmentation4.pcap	18/10/2024 8:29 am	Microsoft Excel Com...	5,111 KB



Cryptogra	Cryptogra	Scale_of_	Level_of_	Regulator	Technolog	Perceived	User_Satis	Workflow	Incidence_	Compliance_with_Regulations
4	RSA	5	4.2	4.74	2.89	5	4.06	3.5	0	5
5	Hill Cyphe	4.3	3.7	3.79	3.97	4.89	5	3.44	4	4.93
3	ChaCha20	4.1	3.5	5	3.88	3.8	4.1	2.38	4	4.85
5	Hill Cyphe	4.3	1.9	4.78	3.11	3.85	4.09	4.49	2	4.28
5	Hill Cyphe	2.8	3.3	4.14	5	3.3	3.95	4.5	2	4
2	ChaCha20	3.3	1	3.81	2.84	5	2	4.5	5	4.87
3	Hill Cyphe	2.1	4	4.36	3.39	5	3.98	4.42	4	4.84
3	ChaCha20	2.9	3.5	3.5	2	2.76	3.85	2	2	4.47
3	ChaCha20	2.9	1.9	5	3.23	2.5	3.74	2.2	2	4.43
5	ChaCha20	2.5	4.8	4.6	2.01	3.78	2.98	2	1	4
4	RSA	3.6	1.4	4.24	2.5	3.9	4.52	2	2	4.31
3	Blowfish	2.9	3.7	5	2	4.36	2.83	4.5	4	5
5	RSA	4.1	3.8	3.79	2.53	2.5	4.68	4.5	0	4.59
2	ChaCha20	1.1	2	3.5	3.51	3.38	4.33	3.51	3	4
4	Blowfish	3.2	3.2	4.21	3.31	4.02	5	4.11	4	4.65
2	Blowfish	3.6	1.6	4.39	3.1	3.32	3.39	3.03	2	5
4	ChaCha20	3	1	4.67	3.21	4.96	5	4.5	4	5
5	Blowfish	3.2	2.1	3.5	2.99	5	4.13	3.86	5	4
1	Blowfish	1.2	2.6	3.98	3.56	3.56	3.82	2.82	4	4
4	RSA	3.9	3.8	3.5	3.47	4.99	2.96	4.23	3	4.24
2	Blowfish	4.3	3.3	3.5	3.93	3.74	4.34	3.26	2	4.3

Cybersecurity_Data_10 | Descriptive and Stats | Workings - based on python code

Research: Implementation of Advance Encryption Techniques to Protect Sensitive Financial Data from Cyber Threats
Salman Ahmed
Student ID:

Table 1: Descriptive Statistics of Variables in Cryptographic Implementation and Cybersecurity Impact

Variable	Mean	Standard Deviation	Min	Max
Type of Cryptographic Techniques	2.60	1.10	1.00	5.00
Scale of Implementation	3.40	1.40	1.00	5.00
Level of Training Provided	3.20	1.00	1.00	5.00
Regulatory Compliance	4.30	0.70	3.50	5.00
Technology Infrastructure	3.60	1.20	2.00	5.00
Compliance with Regulations	4.60	0.60	4.00	5.00
Perceived Level of Security	4.10	1.00	2.50	5.00
User Satisfaction	3.90	1.10	2.00	5.00
Workflow Efficiency	3.50	1.30	2.00	4.50
Incidence of Security Breaches	2.20	1.60	0.00	5.00

Table 2: Regression Analysis - Impact of Various Factors on Cybersecurity Effectiveness

Predictor	Coefficient (β)	Standard Error	p-value
Type of Cryptographic Techniques	0.21	0.06	0.032
Scale of Implementation	0.31	0.07	0.018
Level of Training Provided	0.4	0.05	<0.01
Regulatory Compliance	0.48	0.06	<0.01
Technology Infrastructure	0.11	0.05	0.48

Table 3: Model Fit - SEM in Cryptographic Impleme ntation

Parameters Index	Value	Acceptable Thresholds

2 Language / Coding Used

Python has been used to simulate results and generate statistics from large dataset.

i-Square (js of Freedk²/df Ratio	RMSEA	SRMR	CFI	TLI
0.99974 4 0.24994	0.005	0.99982	N/A	N/A

Predictor	(Perceive	rceived See	r Bound (er Bound (Perceived Security Level)
Scale_of_I	0.00292	0.66262	-0.01021 0.01605
Level_of_	-0.00811	0.33345	-0.02454 0.00832
Regulator	0.00227	0.88106	-0.0275 0.03204
Technolog	-0.01293	0.11702	-0.0291 0.00324

Predictor	(Perceive	rceived See	r Bound (er Bound	ient (User	(User Satis	ower Bou	pper Bou	ompliance	liance wit	Bound (Co	Bound (Co	cidence o	nce of Sec	ound (Inc	ound (Inc	nt (Workf	Workflow	wer Boun	per Bound (W
Scale_of_I	0.00292	0.66262	-0.01021	0.01605	-0.00936	0.21589	-0.02419	0.00547	0.00129	0.68339	-0.00492	0.0075	-0.01479	0.30249	-0.04292	0.01333	0.00168	0.82538	-0.01321	0.01656
Level_of_	-0.00811	0.33345	-0.02454	0.00832	-0.00178	0.85051	-0.02034	0.01677	-0.00044	0.91078	-0.00822	0.00733	-0.00069	0.96921	-0.03589	0.0345	0.00214	0.82202	-0.01649	0.02076
Regulator	0.00227	0.88106	-0.0275	0.03204	0.01195	0.48579	-0.02166	0.04556	0.00791	0.27079	-0.00617	0.022	0.03572	0.27207	-0.02803	0.09948	0.01753	0.30846	-0.01621	0.05126
Technolog	-0.01293	0.11702	-0.0291	0.00324	0.01215	0.19216	-0.00611	0.0304	0.00208	0.59363	-0.00557	0.00973	-0.00749	0.67141	-0.04212	0.02713	0.00503	0.59074	-0.0133	0.02335

Code Structure:

```
import pandas as pd
import numpy as np
import semopy
from semopy import Model
from sklearn.preprocessing import StandardScaler

# Load the dataset
file_path = r"C:\Users\USER\Documents\Mani CAs\Datasets\Cybersecurity_Data_Entery.xlsx"
data = pd.read_excel(file_path)

# Select relevant independent and dependent variables
independent_vars = ['Scale_of_Implementation', 'Level_of_Training_Provided',
                    'Regulatory_Compliance', 'Technology_Infrastructure']
dependent_vars = ['Perceived_Security_Level', 'User_Satisfaction',
                  'Compliance_with_Regulations', 'Incidence_of_Security_Breaches',
                  'Workflow_Efficiency']

# Standardize the data (optional but recommended for SEM)
scaler = StandardScaler()
data_scaled = data[independent_vars + dependent_vars]
data_scaled = pd.DataFrame(scaler.fit_transform(data_scaled), columns=data[independent_vars + dependent_vars].columns)

# Define the SEM model
model_desc = """
# Measurement model
Perceived_Security_Level =~ Scale_of_Implementation + Level_of_Training_Provided + Regulatory_Compliance
User_Satisfaction =~ Technology_Infrastructure + Scale_of_Implementation
Compliance_with_Regulations =~ Regulatory_Compliance + Technology_Infrastructure
Incidence_of_Security_Breaches =~ Level_of_Training_Provided + Technology_Infrastructure
Workflow_Efficiency =~ Perceived_Security_Level + User_Satisfaction
"""

# Initialize the model
```

```
import pandas as pd
import statsmodels.api as sm
from sklearn.preprocessing import StandardScaler

# Load the dataset
file_path = r"C:\Users\USER\Documents\Mani CAs\Datasets\Cybersecurity_Data_Entery.xlsx"
data = pd.read_excel(file_path)

# Standardize the relevant columns of the data for fit indices calculation
data_scaled = data[['Scale_of_Implementation', 'Level_of_Training_Provided',
                    'Regulatory_Compliance', 'Technology_Infrastructure',
                    'Perceived_Security_Level', 'User_Satisfaction',
                    'Compliance_with_Regulations', 'Incidence_of_Security_Breaches',
                    'Workflow_Efficiency']]

# Standardizing the data
scaler = StandardScaler()
data_scaled = pd.DataFrame(scaler.fit_transform(data_scaled), columns=data_scaled.columns)

# Define the dependent variables and predictors
X = data_scaled[['Scale_of_Implementation', 'Level_of_Training_Provided', 'Regulatory_Compliance',
                 'Technology_Infrastructure']]  # Independent variables

# Add a constant to the independent variables for the intercept term
X = sm.add_constant(X)

# Path coefficients for different dependent variables
y_perceived_security = data_scaled['Perceived_Security_Level']
y_user_satisfaction = data_scaled['User_Satisfaction']
y_compliance_regulations = data_scaled['Compliance_with_Regulations']
y_security_breaches = data_scaled['Incidence_of_Security_Breaches']
y_workflow_efficiency = data_scaled['Workflow_Efficiency']

# Fit the models using ordinary least squares (OLS) for each dependent variable
```

References

UNSW-NB15 Data, (2022). Australian Centre for Cyber Security (ACCS) *https://www.kaggle.com/datasets/alextamboli/unsw-nb15/code*