Configuration Manual

MSc Research Project
MSc in Cybersecurity

Anuja Moruskar
Student ID: X22232362

School of Computing
National College of Ireland

Supervisor: Prof. Niall Heffernan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Anuja Mahadev Moruskar		
Student ID:	x22232362		
Programme:	MSc in Cybersecurity	**Year:**	2023-2024
Module:	Practicum		
Lecturer:	Prof. Niall Heffernan		
Submission Due Date:	12/08/2024		
Project Title:	Securing Financial Transactions with Hybrid ECC and AES Encryption Algorithm		
Word Count:	**Page Count:** 5		

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: Anuja Moruskar

Date: 12/08/2024

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

Anuja Moruskar
Student ID: X22232362

1 Introduction

Configuration Manual contains detailed information about the project's setup and implementation. The main objective of this document is to provide overview of the steps taken to complete the project and to understand the requirements necessary for project implementation. The document provides clear guidance on steps required to take in order to deploy Hybrid algorithm (ECC and AES) on cloud for data security. The main objective of this project is to provide data security for financial transaction with the help of hybrid encryption techniques.

2 System Configuration

2.1 Hardware Configuration:

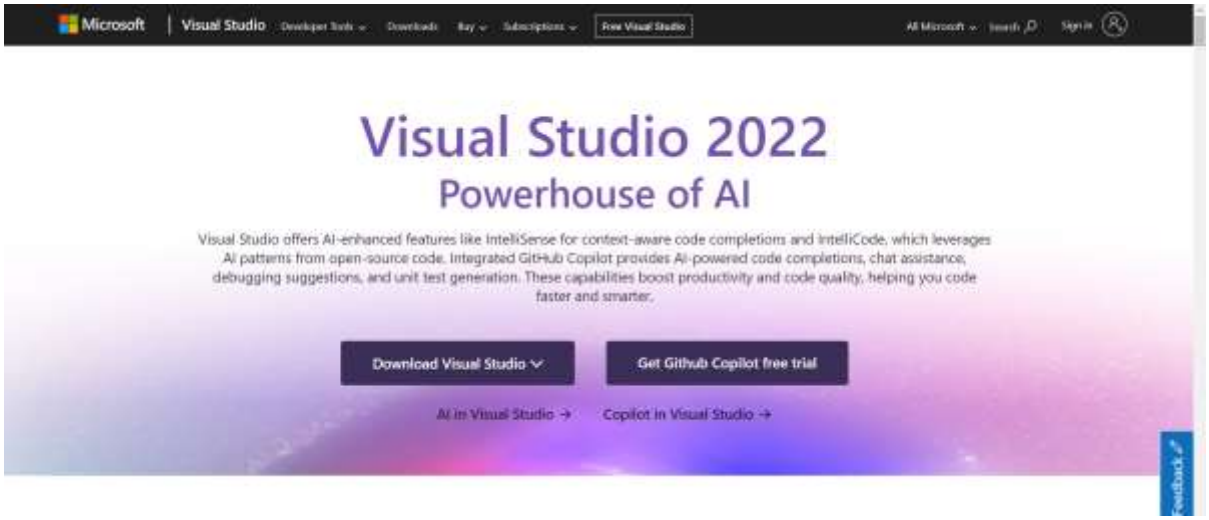
Hardware	**Configuration**
Processor	Intel i7
RAM	16 Gb
Hard disk	512Gb

2.2 Software Configuration:

Operating System	Windows 11
Tool	Visual Studio 2022's version 15.0
Programming language	C# .Net Framework
Database	Microsoft SQL Server 2019
Database Tool	Microsoft SQL Management Studio version 19.0.2.
Cloud Platform	Microsoft Azure

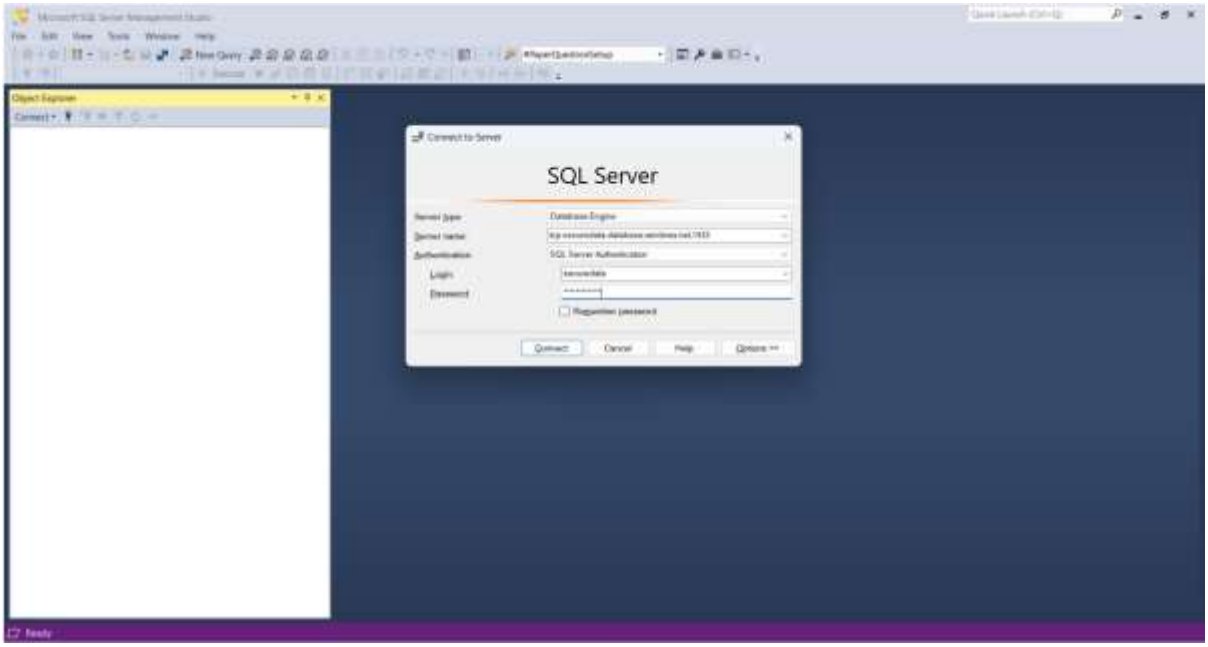
2.3 ASP .Net Environment Setup

The text editor recommended for this project the Visual studio 2022 version 15. The entire application is created using C# programming language on the .Net framework. Visual studio is available on the internet for free.



2.4 Database Server Setup

Microsoft SQL database is used in this project to store data of the application. Microsoft SQL Management studio version 19.0.2 is used for this project, and it is available online for free. Application connects to local as well as clous storage.



2.5 Libraries:

Below mentioned libraries are used to create the application.

```
1   using System;
2   using System.Collections.Generic;
3   using System.Configuration;
4   using System.Data;
5   using System.Data.SqlClient;
6   using System.Diagnostics;
7   using System.IO;
8   using System.Linq;
9   using System.Net.Mail;
10  using System.Security.Cryptography;
11  using System.Text;
12  using System.Web;
13  using System.Web.UI;
14  using System.Web.UI.WebControls;
15
```

2.6 Running Web API:

After successfully installing all required software tools follow below steps to open and run the project.

Open Visual studio 2022 ⇨ File ⇨ Open Project ⇨ select .sIn file ⇨ Run

3 Implementation

Below steps are taken to implement the project

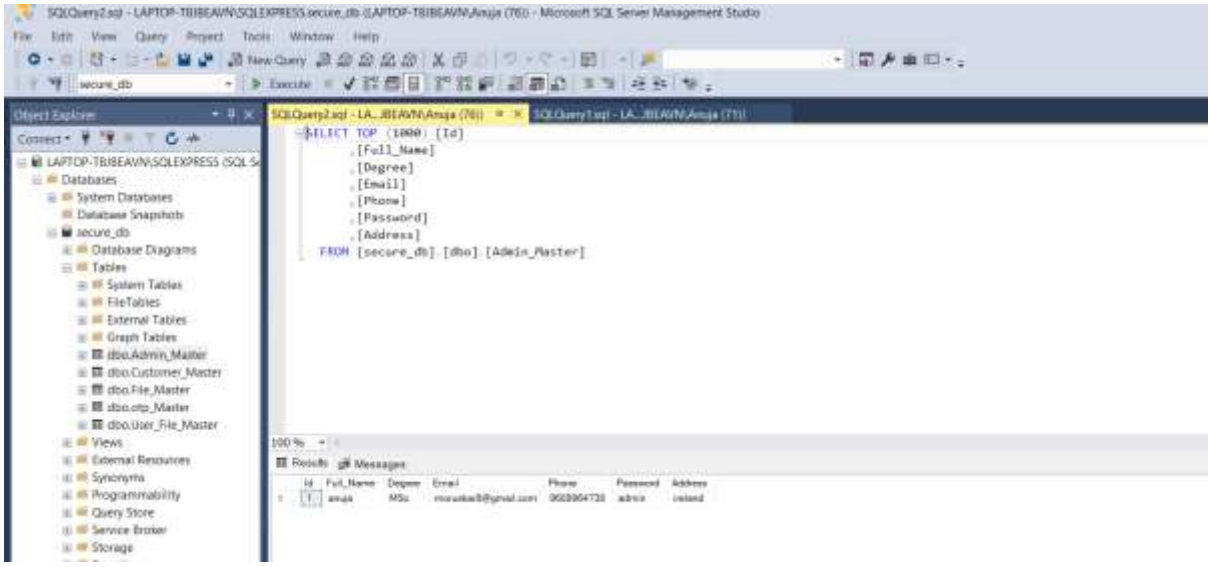
3.1 ECC algorithm for Key generation

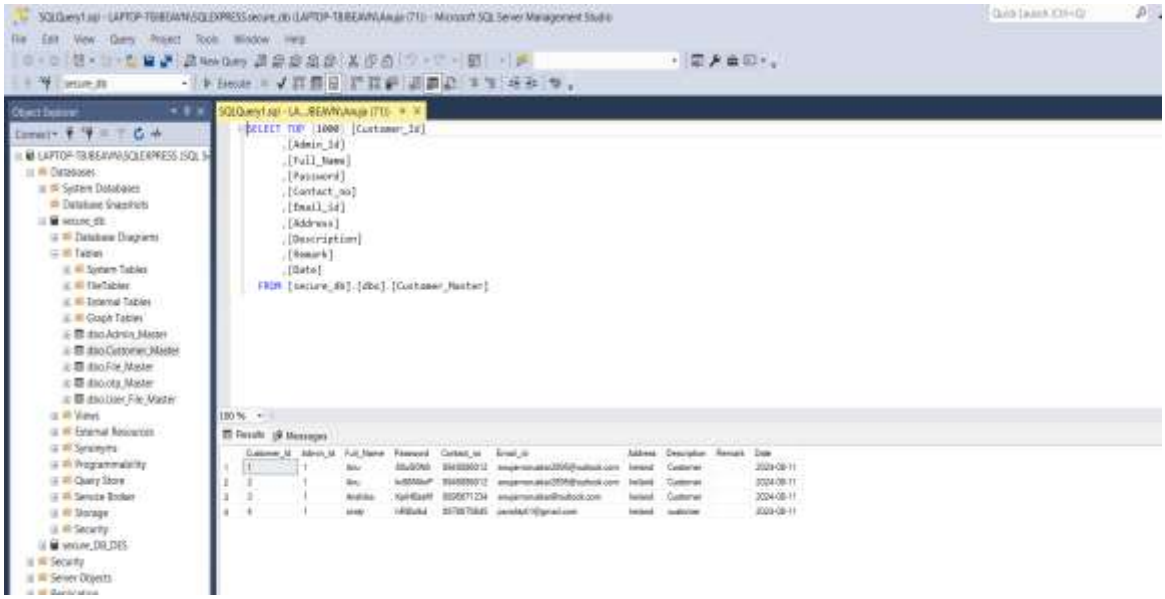
```
byte[] ECC_PublicKey;
byte[] iv;
string private_key = "";
string public_key = "";
using (var alice = new ECDiffieHellmanCng())
{
    var cngKey = CngKey.Create(CngAlgorithm.ECDiffieHellmanP256, null, new CngKeyCreationParameters { ExportPolicy = CngExportPolicies.AllowPlaintextExport });
    ECC_PrivateKey = cngKey.Export(CngKeyBlobFormat.EccPrivateBlob);
    ECC_PublicKey = cngKey.Export(CngKeyBlobFormat.EccPublicBlob);


    alice.KeyDerivationFunction = ECDiffieHellmanKeyDerivationFunction.Hash;
    alice.HashAlgorithm = CngAlgorithm.Sha256;

    ECC_PublicKey = alice.PublicKey.ToByteArray();


    public_key = Convert.ToBase64String(ECC_PublicKey);
    private_key = Convert.ToBase64String(ECC_PrivateKey);
    // ECC_PrivateKey = alice.
```

3.2 Code for Encryption using AES

```
string EncryptionKey = key;
using (Aes encryptor = Aes.Create())
{
    Rfc2898DeriveBytes pdb = new Rfc2898DeriveBytes(EncryptionKey, new byte[] { 0x49, 0x76, 0x61, 0x6e, 0x20, 0x4d, 0x65, 0x64, 0x76, 0x65, 0x64, 0x65, 0x76 });
    encryptor.Key = pdb.GetBytes(32);
    encryptor.IV = pdb.GetBytes(16);
    using (FileStream fsOutput = new FileStream(outputfilePath, FileMode.Create))
    {
        using (CryptoStream cs = new CryptoStream(fsOutput, encryptor.CreateEncryptor(), CryptoStreamMode.Write))
        {
            using (FileStream fsInput = new FileStream(inputFilePath, FileMode.Open))
            {
                int data;
                while ((data = fsInput.ReadByte()) != -1)
                {
                    cs.WriteByte((byte)data);
                }
            }
        }
    }
    FileInfo fi = new FileInfo(inputFilePath);

    long size = fi.Length;
```

3.3 Database created





4 Deployment on Cloud

Application is deployed on azure cloud using app services.