National College of Ireland

Enhancing Health Information Privacy Using Hybrid Cryptosystem Model in Cloud Computing

MSc Research Project
Research And Computing

Neethu Devassy
Student ID: x21106312

School of Computing
National College of Ireland

Supervisor: Aqeel Kazmi

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: .....Neethu...Devassy.....

Student ID: .....x21106312.....

Programme: .....Research...And...Computing..... **Year:** .....2022.....

Module: .....MSc...Research...Project.....

Lecturer: .....Aqeel...Kazmi.....

Submission Due Date: .....01/02/2022.....

Project Title: .....Enhancing...Health...Information...Privacy...Using...Hybrid...Cryptosystem...Model...In...Cloud...Computing.

Word Count: ..... **Page Count:** ...8.....

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: .....

Date: .....

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):	

Enhancing Health Information Privacy Using Hybrid Cryptosystem Model in Cloud Computing

Neethu Devassy
Student ID: x21106312

1 Introduction

The configuration guideline's objective is to provide a quick overview of the requirements required to build this application. It would provide direction for the methodical procedures needed to properly create, operate, test, or reproduce the project.

The remaining sections of the whole document are divided into the following sections. Module 2 specifies the configuration of the system, Module 3 Libraries needed, Module 4 Database Tables, Module 5 Implementation of PGP technique, Module 6 Cloud Deployment.

2 Configuration of System

2.1 ASP .Net Environment Setup

The C# language was used to code the entire application. The project's code was created with Visual Studio Code (VSCode) platform. Free download and setup of VSCode are available on the internet. It was selected since it is a freeware tool that works with many different platforms and allows you to program in a variety of languages. The preferred text editor is Visual Studio 2022's version 15.0

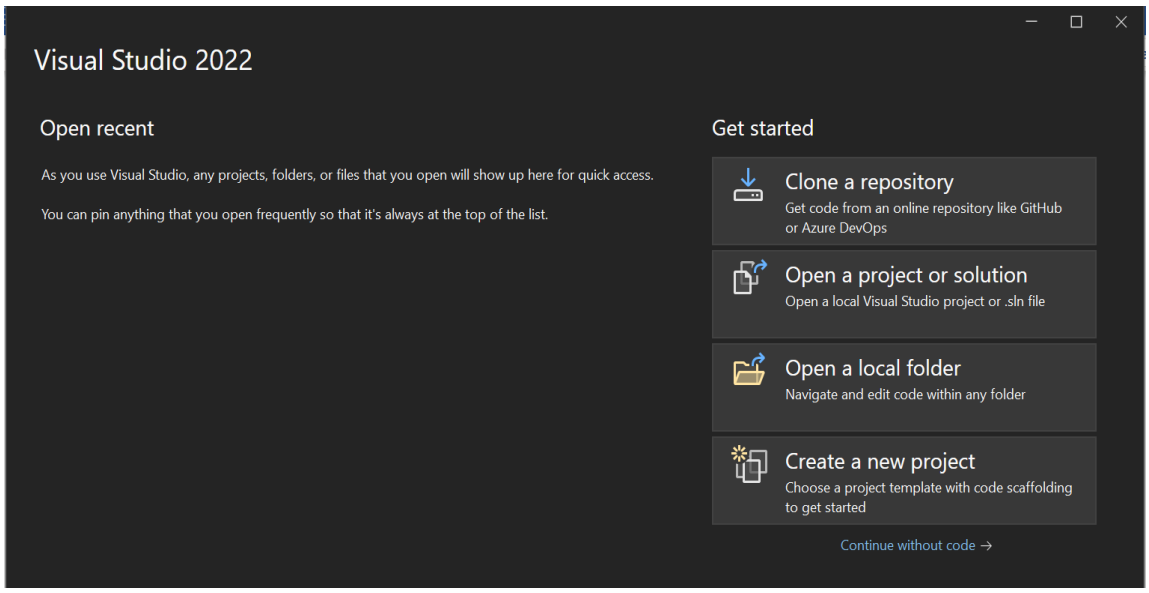

Figure 1: Visual Studio Code

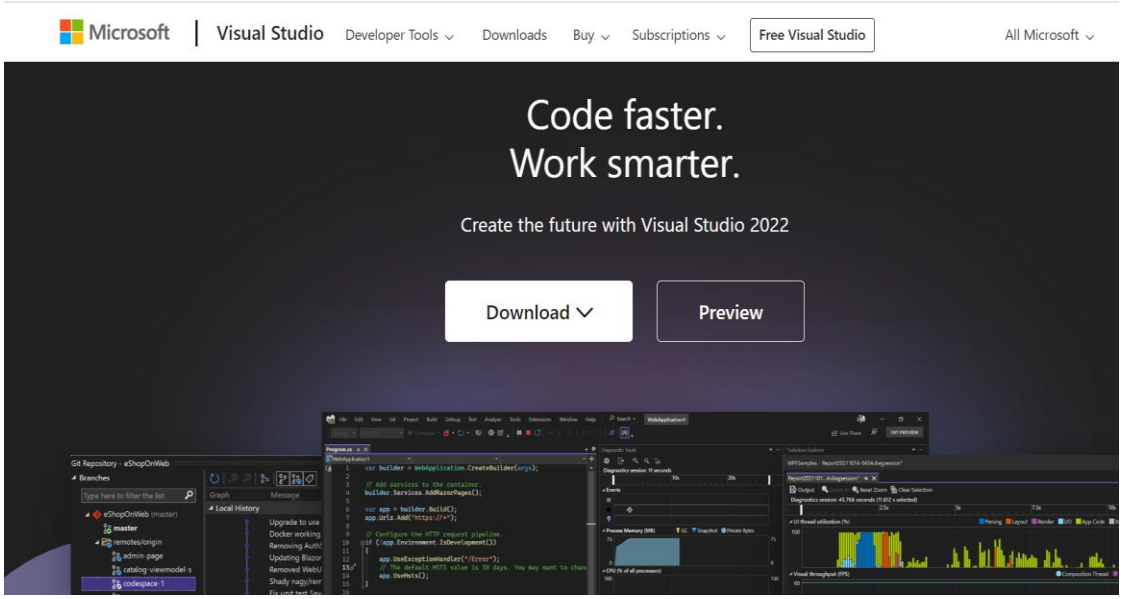

Figure 2: Download page of Visual Studio

2.2 Database Server Setup

The project uses a Microsoft SQL data base for the storage of application data. We can connect our application to both local and cloud data storage with the aid of this technology. The version of Microsoft SQL Management Studio used is 18.12.1. To connect to the database, the user must input the authentication credentials. It is possible to get open source versions of the SQL Management tool for free online.

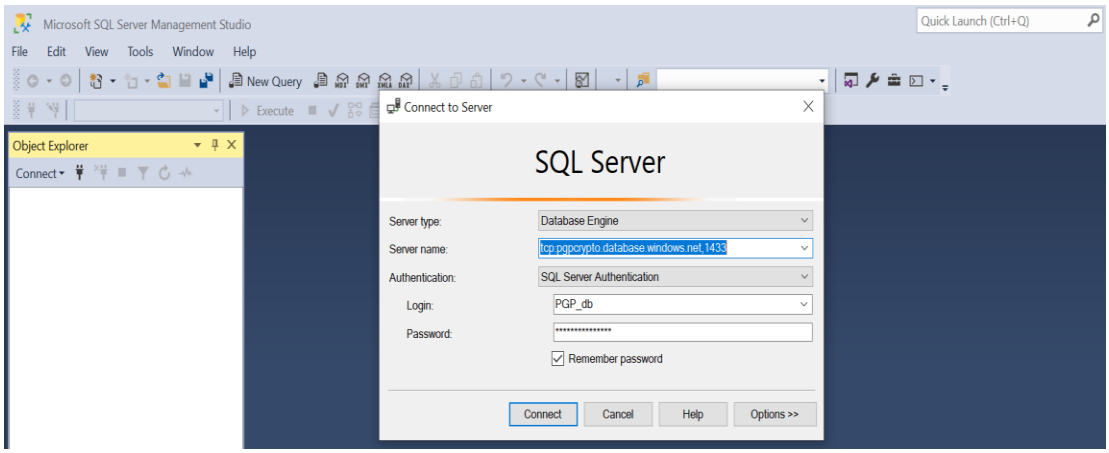

Figure 2: Microsoft SQL Management

2.3 Hardware specifications

- RAM: 8 GB
- Processor: Intel Core i5
- Hard Disk Drive: 10GB HDD

2.4 Software specifications

- OS Used: Microsoft Windows 10

• Language: C# .Net
• IDE used: Visual Studio Code

3 Libraries Used

The following is a list of the main libraries and import statements used to create the application.

```
using System;
using System.Collections.Generic;
using System.Configuration;
using System.Data;
using System.Data.SqlClient;
using System.Diagnostics;
using System.IO;
using System.Linq;
using System.Net.Mail;
using System.Security.Cryptography;
using System.Text;
using System.Web;
using System.Web.UI;
using System.Web.UI.WebControls;
```

Figure 3: Imported Libraries

```
using System;
using System.Collections.Generic;
using System.Diagnostics;
using System.Linq;
using System.Web;
using System.Web.UI;
using System.Web.UI.WebControls;
using System.Data;
using System.Data.SqlClient;
using System.IO;
using System.Security.Cryptography;
using System.Text;
using System.Configuration;
```

Figure 4: Imported Libraries

```
using System;
using System.Collections.Generic;
using System.Configuration;
using System.Data.SqlClient;
using System.Linq;
using System.Web;
using System.Web.UI;
using System.Web.UI.WebControls;

using System.Data;
using System.Net.Mail;
```

Figure 5: Imported Libraries

4 Database Tables Used

	user_id	full_name	contact_no	email_id	address	password	Modulous
4	5	ankit	8605973598	ankitkesarwani122@gmail.com	kandivali	5GOPXvkW	NULL
5	1011	sagar	9986598569	sagardfdwarchavan28@gmail.com	sdasdasdas	sagar	NULL
6	1012	abc	9923659856	abc@gmail.com	sdasd	K2GDxryn	NULL
7	8	test	9892369017	test@gmail.com	Kandivali westsss	y86hPcR6	NULL
8	1009	shubham	9956536598	kamblishubham1@gmail.com	SDASDAS	XFud8JVq	NULL
9	1013	testing	9999999999	testing@gmail.com	sdasdasdas	GtP5LzFO	NULL
10	1014	asdas	9989653656	das32da@gmail.com	sdasd	nNLp9xNn	NULL
11	1020	sadasd	9986598569	dasdasdda@gmail.com	sadas	3DzZsY9R	pkGHNplNBoJjzN3XpCl45gNUu9gkHK5Vzo+4q70L/K9rfH9o...
12	1015	weqe	9989653656	sagarwarchavan28@gmail.com	sdasdas	sagar	zx3H9Nyy/6hf5zh5/DeRreLdij6uSV6S0ySbIbA8PMEdRwwVY...
13	1016	cp	9986598569	cp@gmail.com	dfsdfasdfs	qh8SDbzn	nx4GUIwAOLxEOwv5KcoJClvx+bF9Zomi44fmACMvMyOuiHs...
14	1017	sada	9986598569	dawwsda@gmail.com	sdasd	f71erOii	vu589LguFzWJKMjH/SxStgXtPwMy+9raa3m2vBehRloy83Z1...
15	1019	asda	9986598569	dasda@gmail.com	asdasd	T5rg4b99	nSdfcnycfttfIJrn25ONloyIzz/ou1TADdvzYtRrgsgR/Cg2e9zmjb...
16	1018	asdas	9986598569	sagarwarchavan438@gmail.com	asdasd	ARSNchoM	zny7HA9sxtisiNUyQ5pWeYiK47Fal9sL3IXR7RNx3jRjPSGP7r...
17	1021	sasdas	9989653656	sagarwasdaarchavan438@gmail...	sdasd	0PZkzs1p	pb+vF57A+319cfIhcb9GL6IXA81+HdCl4IbnQeS3OvRYOE7...
18	1022	sadas	9986598569	sagarwarchadasvan438@gmail	sdasd	qMBTLI8r.I	sEOY7VMLOrDqSEuxbKZQudGs40WsXmtNNH9/ZssuKurZG

Figure 6: User Table

100 %

Results | Messages

	share_id	file_name	username	cloud_id	fid
1	1	Jellyfish.jpg	project@projectideas.co.in	clouuud	1
2	2	architecture.PNG	maryneethu.devassy4@gmail.com	clouuud	2
3	3	architecture.PNG	maryneethu.devassy4@gmail.com	clouuud	2
4	4	decription.PNG	antonymary970@gmail.com	clouuud	4
5	5	Proposed Architecture.PNG	antonymary970@gmail.com	clouuud	5
6	1001	1.jpg	maryneethu.devassy4@gmail.com	clouuud	1001
7	1002	NCI_Logo_colour.jpg	ann@gmail.com	clouuud	1002
8	1006	20220906_190211.jpg	antonymary970@gmail.com	clouuud	1006
9	1008	image4.png	maryneethu.devassy4@gmail.com	clouuud	1008
10	2001	2.png	maryneethu.devassy4@gmail.com	clouuud	2001
11	2002	google.png	maryneethu.devassy4@gmail.com	clouuud	2002
12	2003	Architecture_FogComputing.PNG	maryneethu.devassy4@gmail.com	clouuud	2003

Query executed successfully. (localdb)\MSSQLLocalDB (15....

Figure 6: Table for Data Sharing

5 Implementation of PGP Technique

To implement the PGP approach, symmetric and asymmetric algorithms were combined. The produced secret key is encrypted using an asymmetric algorithm (RSA) while the data is encrypted using a symmetric algorithm (AES). Prior to decrypting the data, it is crucial to decrypt the secret key. The user receives the secret key through mail, encrypted.

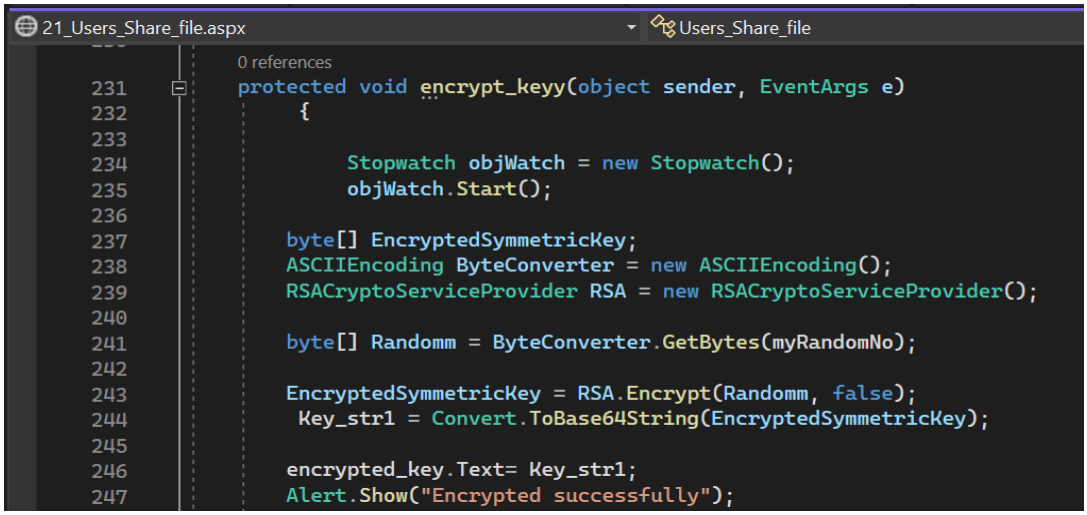

Figure 7: Code for Key encryption

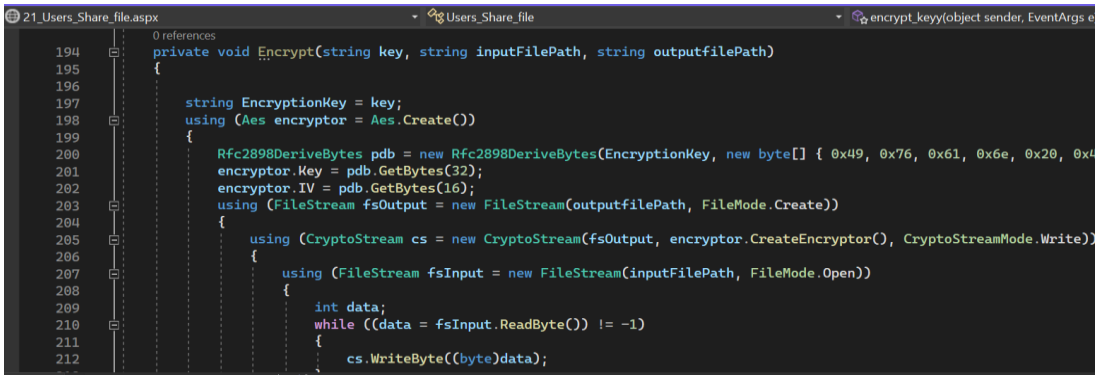

Figure 7: Code for Data encryption

The code for sending encrypted files and data to an authenticated email address can be seen in the screenshot below.

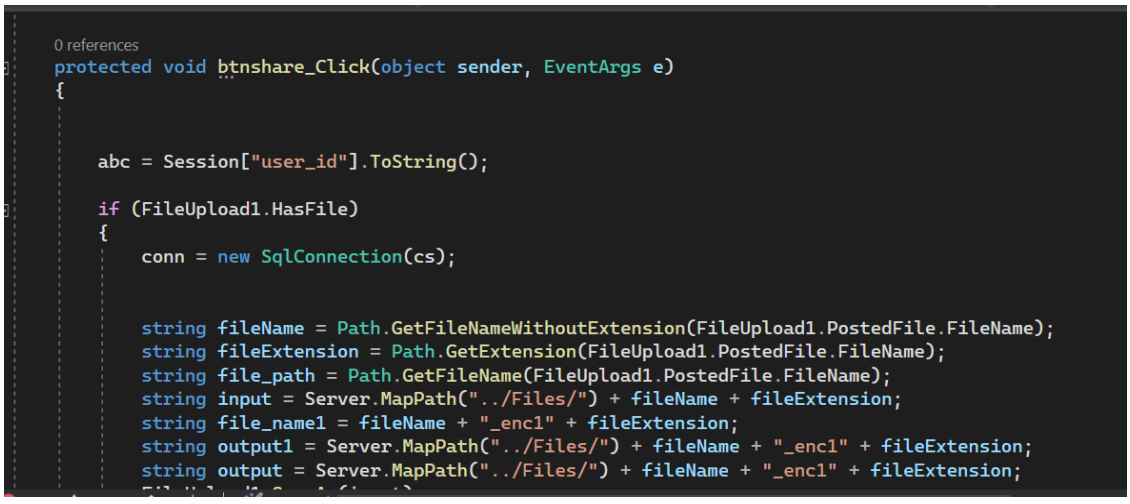

Figure 8: Code for Share encrypted file

The application connects to local and cloud databases using a web.cofig file.

```
<?xml version="1.0" encoding="utf-8"?>

<!-- For more information on using web.config transformation visit http://go.microsoft.com/fwlink/?LinkId=125889 -

<configuration xmlns:xdt="http://schemas.microsoft.com/XML-Document-Transform">
  <!--
    In the example below, the "SetAttributes" transform will change the value of
    "connectionString" to use "ReleaseSQLServer" only when the "Match" locator
    finds an attribute "name" that has a value of "MyDB".

    <connectionStrings>
      <add name="MyDB"
        connectionString="Data Source=ReleaseSQLServer;Initial Catalog=MyReleaseDB;Integrated Security=True"
        xdt:Transform="SetAttributes" xdt:Locator="Match(name)"/>
    </connectionStrings>
  -->
  <system.web>
    <compilation xdt:Transform="RemoveAttributes(debug)" />
    <!--
      In the example below, the "Replace" transform will replace the entire
      <customErrors> section of your web.config file.
      Note that because there is only one customErrors section under the
```

Figure 8: Configuration File for Database Connection

6 Cloud Deployment

6.1 New Application Creation

The entire application is deployed into the cloud. Windows Azure projects can be developed in almost any language and include cloud-based public services. This application using Windows Azure cloud service.

Login to the cloud environment first. Then select App service to develop a new application in the Azure cloud. Once a program is released, a cloud access URL is provided.

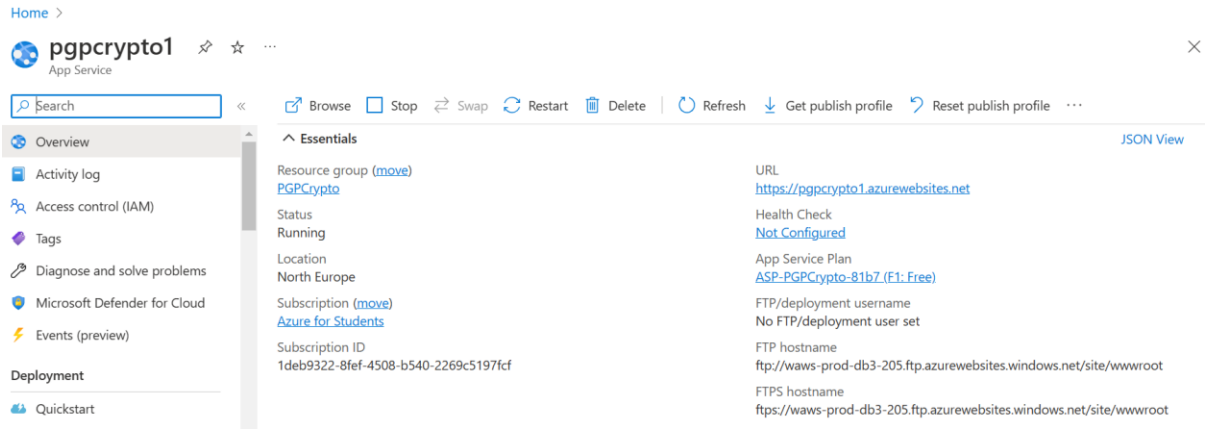

Figure 8: Application Deployment in Cloud

6.2 Create Cloud Database

Below screenshot shows the option to create Database in Azure Cloud. The database connection details are different in cloud platform.

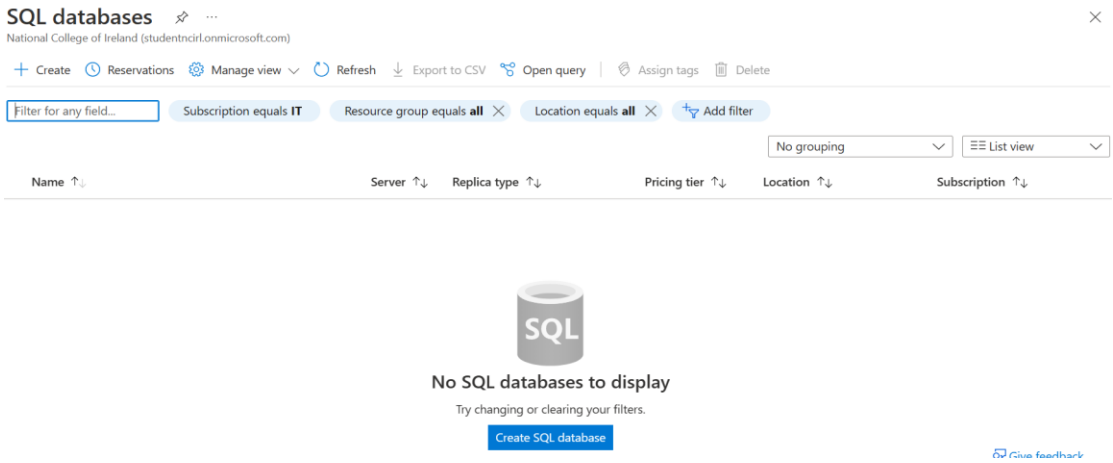

Figure 9: Create Cloud Database

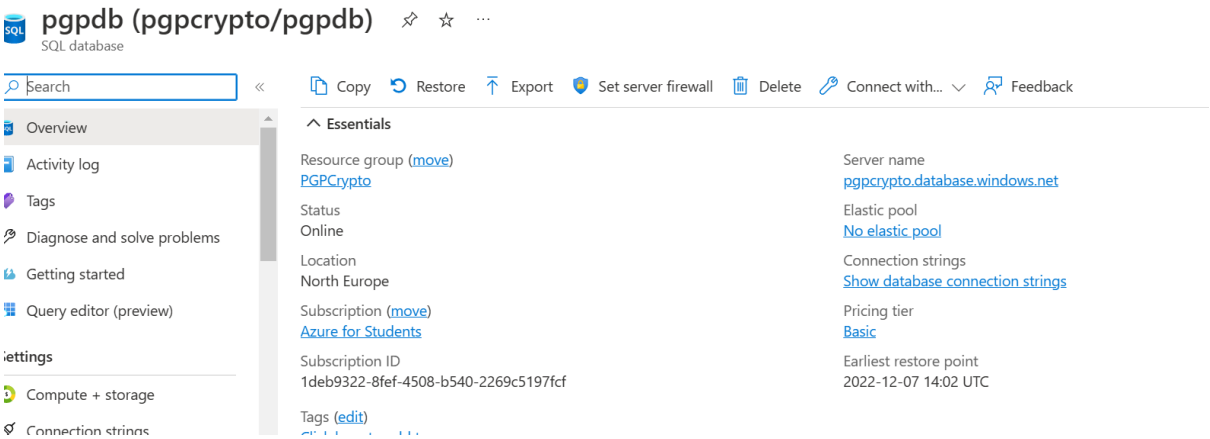

Figure 10: Database created for Application in Cloud

6.3 Publish Updated details in Cloud Environment

The same should be published in the cloud if there is an update to the current code base. It is possible to update local changes in a cloud environment. The below Fig:10 shows an option to publishes changes from local machine to cloud environment.

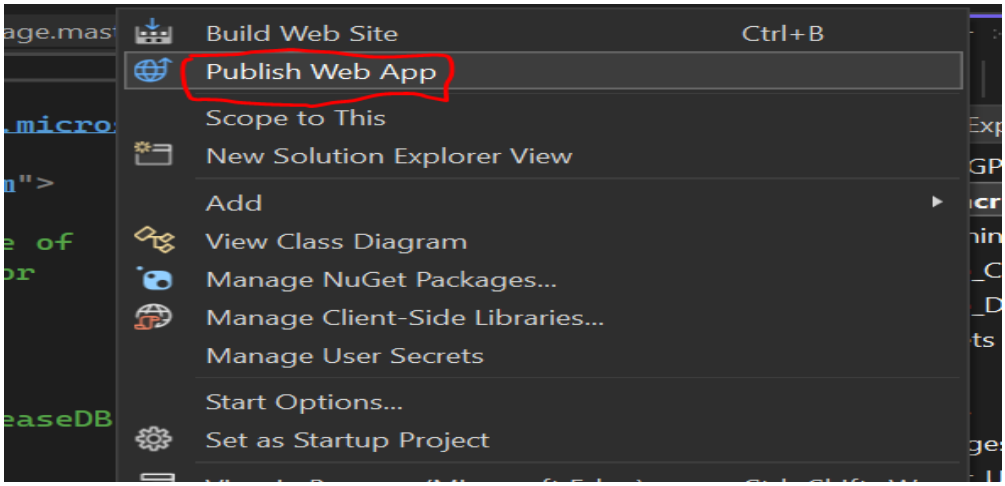

Figure 10: Publish Code Changes in Cloud

Fig:11 shows an option to get the changes from local machine to cloud platform.

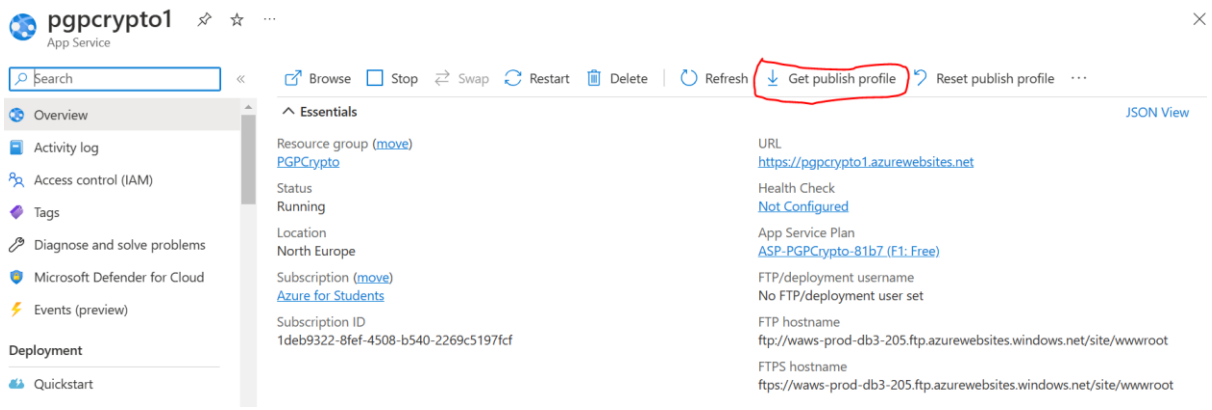

Figure 10: Get Published Code Changes in Cloud