School of Computing Technologies

**INTE2401/2402/2691 Cloud Security**

Assignment 3

|  |  |
| --- | --- |
| RMIT_icon_Industry_connections_Red_RGB.png | **Assessment Type:** Individual assignment; no group work. Submit online via Canvas→Assignments→Assignment 3.  Marks awarded for meeting requirements as closely as possible. Clarifications/updates may be made via announcements/relevant discussion forums. |
| RMIT_icon_add_an_event_Red_RGB.png | **Due date:** **Week 12, Sunday the 1nd June 2024 11:59pm**  As this is a major assignment in which you demonstrate your understanding, a university standard late penalty of 10% per each working day applies for up to 5 working days late, unless special consideration has been granted. |
|  | **Weighting**: **35 marks (Contributes 35% of the total Grade)** |

1. **Overview**

The objective of Assignment 3 is evaluating your knowledge on the topics covered mainly from Lecture 9 to 11. Topics include Data Privacy Protection Techniques, AWS Identity Management and Database Security, and AWS VPN and Firewall Practices. However, topics covered from Lecture 1 to 8 are required as prerequisite. Assignment 3 will focus on developing your abilities in application of knowledge, critical analysis, decision making and using AWS security services. Assignment 3 contains several problems related to the topics mentioned above. You are required to prepare your answers and programming codes, videos and upload them as a single zip file in CANVAS.

In this assignment, there are **4 (four**) questions in total.

Question Q1 is about how to protect cloud data privacy with **Homomorphic Encryption**. To protect our data privacy in cloud and meanwhile allow the cloud server to process our data, the best solution is using homomorphic encryption scheme, e.g., Paillier encryption scheme, to protect our data in the cloud. In this question, you are expected to understand how homormphic encrytion technique can be used to protect your data privacy in Cloud and analyse data privacy.

Question Q2 is about **Key Recovery with Shamir Secret Sharing**. In Question Q1, the decryption key of homomorphic encryption is required when decrypting the ciphertexts downloaded from the cloud. If you lost your decryption key, you would lose all of your date stored in the cloud. In this question, you are expected to use Shamir’s secret sharing scheme to recover your decryption key of homomorphic encryption.

Question 3 is about **Secure Data Management via Amazon S3.** Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. In this question, you are expected to demonstrate your understanding of how to create three secure buckets in Amazon S3 to keep the data from the three departments of a company, respectively.

Question Q4 is about **AWS Virtual Private Network (AWS VPN)**. AWS Client VPN is a managed client-based VPN service that enables you to securely access your AWS resources in your on-premises network. With Client VPN, you can access your resources from any location using an OpenVPN-based VPN client. Client VPN offers the following features and functionality: secure connections, authentication, granular control, ease of use and etc. In this question, you are expected to demonstrate your understanding of how to create an AWS VPN server for a company and allow the staff of the company to get access to the AWS VPN server and then AWS VPC.

Develop this assignment in an iterative fashion (as opposed to completing it in one sitting). You should be able to start preparing your answers immediately after Lecture 9 (in Week 9). At the end of each week starting from Week 9 to Week 11, you should be able to solve at least one question.

If there are questions, you may ask via the relevant Canvas discussion forums in a general manner.

1. **Learning Outcomes**

This assessment is relevant to the following Learning Outcomes:

* Demonstrate knowledge of cloud security principles and mechanisms
* Demonstrate computer programming and configuration skills required to develop a cloud security infrastructure
* Identify cloud security weaknesses by recognising and discovering threats and vulnerabilities to cloud computing
* Problem solve how to fix cloud security weaknesses and mitigate security threats to cloud computing
* Demonstrate knowledge and skills to prepare for industry cloud security certificate exams, e.g. CCSK, CCSP.
* Communicate clearly and effectively using the technical language of the field correctly.

1. **Submission**

You must follow the following special instructions:

* You must use the values provided in the questions.
* Hand-written answers are not allowed and will not be assessed. Compose your answers using any word processing software (e.g. MS Word).
* You are required to show all of the steps and intermediate results for each question.
* For Questions 3 and 4, use screen shots to show clearly the outcome of each step you took to arrive at your answers. And, also include videos to demonstrate your configurations.
* Upload your answers together with programming codes and videos as a single zip file in CANVAS.

This assessment will determine your ability to:

* Follow requirements provided in this document and in the lessons.
* Independently solve a problem by using security concepts, principles and mechanisms taught over the course.
* Meeting deadlines.

After the due date, you will have 5 business days to submit your assignment as a late submission. Late submissions will incur a penalty of 10% per day. After these five days, Canvas will be closed and you will lose ALL the assignment marks.

1. **Assessment details**

Please ensure that you have read **Section 1** to **3** of this document before going further. Assessment details (i.e. question Q1 to Q4) are provided in the **next page**.

**Q1. Data Privacy Protection with Homomorphic Encryption (Marks: 2+2+2+2+2=10)**

|  |
| --- |
| In cloud computing, you may store your data in cloud.  *ISSUE*  Although the cloud server is able to protect your data against various attacks from the outside, it cannot guarrantee your data privacy if your data is not encrypted by youself. The cloud data administrator may be able to get access to your plain data stored in cloud and reveal the privacy of your data.  *SOLUTION*  To protect your data privacy in cloud and meanwhile allow the cloud server to process your data, the best solution is using **homomorphic encryption scheme,** e.g., Paillier encryption scheme, to protect your data in the cloud as shown in **Figure 1.**  A picture containing drawing  Description automatically generated  **Figure 1. Homomorphic Encryption**  Assume that you want to store your monthly incomes in the first quarter in the cloud and decide to use the Paillier encryption scheme to encrypt the incomes and upload them to the cloud.   1. Use the tool <https://www.mobilefish.com/services/rsa_key_generation/rsa_key_generation.php> to **generate your public key** for Paillier encryption and **determine your private** key for Paillier decryption. The size of the modulo**(n)** is required to be **1024 bits.**   -**Get P** and **Q, (512 bits)**  **N = p\*q**  **G,** Generator is n+1  **Modular = n^2**  Public key (n, g)  Private key (p,q)  N/ p = Q. So in my case I can use 1 value eulers.    (p-1)(q-1) = Eulers my   * Eulers us used for decryption later.   ~~- These value are used to derive the private key, (Lambda).~~  **~~-Ask: Is our public exponent the same (I.e. student number)~~**   1. Use your public key to encrypt your monthly incomes from January to March and upload the ciphertexts to the cloud. Assume that your monthly income is MD5(your student ID||the month) (**mod 10000).** What are the three ciphertexts?   **Use this:**  <https://emn178.github.io/online-tools/md5_checksum.html>  <https://www.boxentriq.com/code-breaking/modular-exponentiation>  Random value can be anything.   1. How does the cloud server compute the encryption of the sum of your monthly salaries for these 3 months (assume that the cloud server returns one encrypted result to you)? ***What is the ciphertext computed by the cloud server?***   Look at Week 9 slide 18.  Multiply 3 ciphertexts   1. How do you decrypt the encrypted result to get the sum of your monthly salaries for these 3 months? Show the steps in detail. 2. **Implement Paillier encryption algorithm** (submit your code) and verify your encryption results in (2).   -Assignment 2, Q3. Fi nd the generator ^plaintext \*randompower^n mod nsquare |
|  |

**Q2. Key Recovery with Secret Sharing (Marks: 2+2+2+2+2=10)**

|  |
| --- |
| In Question Q1, the decryption key of homomorphic encryption is required when decrypting the ciphertexts downloaded from the cloud. If you lost your decryption key, you would lose all of your date stored in the cloud.  In order to be able to recover your decryption key, suppose that you decide to use **Shamir’s secret sharing scheme.** Shamir's Secret Sharing is an approach to share secret, where a secret is divided into parts, giving each participant its own unique part. To reconstruct the original secret, a minimum number of parts is required.  Following Shamir’s secret sharing scheme, suppose that you divide your decryption key into 4 parts, storing 4 parts in four different clouds as shown in **Figure 2.** If you lost your decryption key, you should be able to recover it with any 3 parts.    Clouds  A close up of a sign  Description automatically generated A close up of a sign  Description automatically generated A close up of a sign  Description automatically generated A close up of a sign  Description automatically generated    Share 4  Share 3  Share 2  Share 1  A picture containing computer, desk, mouse, keyboard  Description automatically generated  **Figure 2. Key recovery with Shamir’s scheme**     1. Select a **suitable polynomial** (using your **student ID** as one of the coefficient and determining what Paillier key parameter in Question 1 should be considered as the secret);  * Secret value from question 1 we use. Phi(n) is the secret s. * Or N= P\*Q => N/P =Q. We assume everyone know N~~.~~ *We treat P or Q as secret key.* P and Q is 512 bits. (1.1 – key generation). Use **q** as it is a smaller value. * A = polynomial as example. This is a random value * B = student ID * Formula = f(x) = a \* x^2 \* b x^1 + s  1. Divide your Paillier key parameter **into 4 shares** (assume uploading them onto 4 different clouds, respectively);  * Compute f(1)… f(4): This represents each share. * Record shares as (x0,y0) (x1,y1), (x2, y2)… (x3,y3) * We substitute into x into the polynomial formula. * Can calculate manually with <https://www.boxentriq.com/code-breaking/big-number-calculator> to do validation.  1. Recover your Paillier key parameter with any **3 of 4 shares** (show the steps in detail);   Refer to Week 9.    P1 = 1, y1  P2 = 2, y2  P3 = 3, t3  F(0) = y1 \* (x2 / (x2 – x1) \* x3 / x(x3 – x1)) + y2 \* ( x1 / (x1 - x2) \* x3 / (x3 /x2)) + y3 \* ( …  **Below is not fully correct and incomplete**  First Part = y1 \* (x2 / (x2 -x1) \* x3 / (x3 -x1))  X2 / (x2 – x1) = 2 / (2 -1) = 2  X3 / (x3 – x1) = 3 / ( 3 -1) = 3/2  Second Part = y2 \* (x1 / (x1 -x2) \* x3 / (x3 -x2))  X1 / (x2 – x2) = 1 / (2 -1) = 2  X3 / (x3 – x2) = 3 / ( 3 -1) = 3/2  3rd part = y3 \* (x1 / (x1 -x2) \* x3 / (x3 -x2))  S = first part + second part + third part   1. **Implement (1)-(3) with JavaScript** (submit your codes);   -Choose suitable parameters.  <https://titan.csit.rmit.edu.au/~e31435/2024/lab9/shamir.html>  (Week 9 tutorial)  Note: You have to add another term in polynomial.   1. Analyse the security of your Paillier key parameter in the case of 2 of the 4 clouds collude to derive your decryption key.   *Tutorial 3*  **Will the server notice your Pallier key parameters.**  **Secret sharing has perfect secrurity.**  **Nothing is known to servers.**  **Since you need 3 to decrypt, but only need 2 servers you are secure.**    This is the formula to recover secret (Week 9).  Yi is range of possible values. |
|  |

**Q3. Secure Data Management via Amazon S3 (Marks: 2+2+2+2+2=10)**

|  |
| --- |
| **Overview**  “Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements”.   * AWS S3 Developer Guide   This task requires you to demonstrate your knowledge of cloud security principles by creating secure buckets in Amazon S3.  **Task**  Suppose that you are an IT manager for a company with three departments – **marketing, sales and services**. The CEO of the company decides to move all company data to Amazon Simple Storage Service (Amazon S3).  For this purpose, you are required to create three buckets in Amazon S3 to keep the data from the three departments, respectively, as shown in **Figure 3.**  A picture containing game  Description automatically generated  **Figure 3. AWS S3**  **Questions**  Assume that Alice, Bob are two staff in the marketing department, Smith and Turdy are two staff in the sales department, and Charlie is a staff in the service department.  3.1. In order for the five staff to upload and download data to and from Amazon S3, **create user accounts** for them (please name the user with your **student ID + a, b, c, d, or e, e.g., s1234567a**).    3.2. In order to protect data privacy between departments, different department buckets should be encrypted by different secret keys. Generate the **marketing key, the sales key, and the services key, respectively**.  - Screenshot all departments  3.3 Allow Alice and Bob to access the marketing key, Smith and Trudy to access the sales key, and Charlie to access the services key.  - Step 4 key users screenshot.  3.4 **Create three buckets** in S3 for the marketing, sales and services departments, respectively.  3.5 **Encryp**t the marketing, sales and services department buckets with the marketing key, the sales key, and the services key, respectively.  - You cannot change the key once the bucket is created.  -   * For Question 3.1 to 3.5, use screen shots with a video to show clearly the outcome of each step you took to arrive at your response.   Your responses will be assessed for clarity, completeness and correctness. |

**Q4. Create AWS Client Virtual Private Network (Marks: 1+1+1+1+1=5)**

|  |
| --- |
| **Overview**  “AWS Client VPN is a managed client-based VPN service that enables you to securely access your AWS resources and resources in your on-premises network. With Client VPN, you can access your resources from any location using an OpenVPN-based VPN client.”   * AWS Client VPN Guide   This task requires you to demonstrate your knowledge of cloud security principles by setting up and configuring a VPN Server using AWS Client VPN.  **Task**  Suppose that you are the IT Manager for ABC Bookshop PTY LTD. ABC Bookshop has decided to move all services including its web server and databases to Amazon Virtual Private Cloud (VPC). As the IT Manager, your job is to set up an AWS VPN Server. You are then required to configure this server so that staff are able to access the server and then the Virtual Private Cloud (VPC). Please see Figure 4 for the AWS architecture diagram representing the final solution.  A screenshot of a cell phone  Description automatically generated  **Figure 4. AWS VPN (IP addresses here are used for example only)**  **Questions**   * 1. Create an AWS VPN Server in AWS.   - A server is called an instance  4.2 Configure the AWS VPN Server connection.  4.3 Setup a password for your staff to get access to the AWS VPN Server. The password should be your **student ID.**  4.4. Demonstrate admin login and client login to the AWS VPN Server.  4.5 Jane, the CEO of Bookshop PTY LTD is concerned about the security of the VPN solution. Explain to Jane how secure your solution is.   * For Question 4.1 to 4.4, use screen shots with a video to show clearly the outcome of each step you took to arrive at your response.   Your responses will be assessed for clarity, completeness and correctness. |

1. **Academic integrity and plagiarism (standard warning)**

Academic integrity is about honest presentation of your academic work. It means acknowledging the work of others while developing your own insights, knowledge and ideas. You should take extreme care that you have:

* Acknowledged words, data, diagrams, models, frameworks and/or ideas of others you have quoted (i.e. directly copied), summarized, paraphrased, discussed or mentioned in your assessment through the appropriate referencing methods.
* Provided a reference list of the publication details so your reader can locate the source if necessary. This includes material taken from Internet sites.

If you do not acknowledge the sources of your material, you may be accused of plagiarism because you have passed off the work and ideas of another person without appropriate referencing, as if they were your own.

RMIT University treats plagiarism as a very serious offence constituting misconduct. Plagiarism covers a variety of inappropriate behaviors, including:

* Failure to properly document a source
* Copyright material from the internet or databases
* Collusion between students

For further information on our policies and procedures, please refer to the [University website.](https://www.rmit.edu.au/students/student-essentials/rights-and-responsibilities/academic-integrity)

1. **Assessment declaration**

When you submit work electronically, you agree to the [assessment declaration.](https://www.rmit.edu.au/students/student-essentials/assessment-and-exams/assessment/assessment-declaration)

1. **Rubric/assessment criteria for marking**

All of the computations must be correct and only provided values must be used. Instructions must be followed.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Criteria**  The characteristic or outcome that is being judged. |  | | | | | | | **Total** |
| **Question 1**  Data Privacy Protection with Homomorphic Encryption | **Questions (1)-(5) are answered correctly.**  **Step-by-step processes are shown with detail computations and implementations.**  **All of the computations, implementation are shown correctly in detail.** | Any 4 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations and implementations.  The computations, implementations in 4 questions are shown correctly in detail. | Any 3 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations and implementations.  The computations, implementations in 3 questions are shown correctly in detail. | Any 2 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations and implementations.  The computations, implementations in 2 questions are shown correctly in detail. | Any 1 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations or implementations.  The computations, implementations in 1 question are shown correctly in detail. | Answer is not correct  Or  Not answered | 10 Marks | | |
| **10 Marks** | 8 Marks | 6 Marks | 4 Mark | 2 Mark | 0 Marks |  | | |
|  |  |  |  |  |  |  |  | | |
| **Question 2**  Key Recovery with Secret Sharing | **Questions (1)-(5) are answered correctly.**  **Step-by-step processes are shown with detail computations, implementations.**  **All of the computations, implementation and security analysis are shown correctly in detail.** | Any 4 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations and implementations.  The computations, implementations and/or security analysis in 4 questions are shown correctly in detail. | Any 3 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations and implementations.  The computations, implementations and/or security analysis in 3 questions are shown correctly in detail. | Any 2 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations and implementations.  The computations, implementations and/or security analysis in 2 questions are shown correctly in detail. | Any 1 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations or implementations.  The computations, implementations, or security analysis in 1 question are shown correctly in detail. | Answer is not correct  Or  Not answered | 10 Marks | | |
| **10 Marks** | 8 Marks | 6 Marks | 4 Mark | 2 Mark | 0 Marks |  | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Question 3**  Secure Data Management via Amazon S3 | **Questions (1)-(5) are answered correctly.**  **Step-by-step processes are shown with detail implementations.**  **All of the implementations are shown correctly in detail.** | Any 4 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail implementations.  The implementations in 4 questions are shown correctly in detail. | Any 3 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail implementations.  The implementations in 3 questions are shown correctly in detail. | Any 2 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail implementations.  The implementations in 2 questions are shown correctly in detail. | Any one of questions (1)-(5) is answered correctly.  Step-by-step processes are shown with detail implementations.  The implementations in 1 question are shown correctly in detail. | Answer is not correct  Or  Not answered | 10 Marks |
| **10 Marks** | 8 Marks | 6 Marks | 4 Mark | 2 Mark | 0 Marks |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Question 4**  Create AWS Client Virtual Private Network | **Questions (1)-(5) are answered correctly.**  **Step-by-step processes are shown with detail implementations.**  **All of the implementations and security analysis are shown correctly in detail.** | Any 4 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail implementations.  The implementations and/or security analysis in 4 questions are shown correctly in detail. | Any 3 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail implementations.  The implementations and/or security analysis in 3 questions are shown correctly in detail. | Any 2 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail implementations.  The implementations and/or security analysis in 2 questions are shown correctly in detail. | Any one of questions (1)-(5) is answered correctly.  Step-by-step processes are shown with detail implementations.  The implementation or security analysis in 1 question is shown correctly in detail. | Answer is not correct  Or  Not answered | 5 Marks |
| **5 Marks** | 4 Marks | 3 Marks | 2 Mark | 1 Mark | 0 Marks |  |