CP2414 Assignment 2
Cryptography and Network Security Applications

WARNING: This is not a group project. Each student must individually complete all parts of their submission.

Students must start with a new document, and they must not have another person's file in their possession at any time. Students may discuss the task with each other, but each student must write their assignment independently and not show their work to other students.

Introduction:

This assignment has been divided into four (4) parts. You are to prepare a report for the CEO of *MEDASIA* with regard to:

1. The User authentication
2. Cloud Computing and blockchain for handling the Company's data
3. Network Diagram
4. Citation and Referencing

Deliverables:

1. A single Word document (.docx) – containing all parts.
2. Font - Calibri 11, Line Spacing 1.5
3. Word limit for this report - must not exceed 4000 words.
4. Use IEEE referencing, see https://libguides.jcu.edu.au/IEEE

NOTE: The assignment template can be found at the end of this assignment sheets.

Scenario:

Your client, *MEDASIA*, was satisfied with the advice you provided them with last time. They have decided to hire you again. Having accrued a vast amount of valuable data, and with the intent to licence the company's data to others, the CEO has begun to take security more seriously.

Note: You may only use information concerning *MEDASIA* in this assignment if it has been provided within this document. Company information must not be carried over from the previous assignment.

About the company:

MEDASIA is a growing medical research company consisting of six branches: Thailand (main) branch, the Philippines and Indonesia branch. Each branch has six departments and there are approximately 40 employees per department. The Thailand branch has 2 mail servers, 3 web servers, and 3 database servers. The Indonesia branch is a smaller branch, so it has only 1 mail server and 1 database server.

All branches have high-speed networks; however, weekday traffic can be quite heavy. This is especially true for the Thailand branch.

Part I Kerberos and User Authentication

As the company grows, the CEO fears legitimate users may be impersonated to access company network resources. You, as a consultant, know that Kerberos would be the answer to CEO's requirement regarding user authentication.

Your task for this part is to explain how Kerberos cryptography can be used for user authentication purpose. The following aspects may be explained:

- Why Kerberos should be chosen for this purpose?
- Does Kerberos use symmetric or asymmetric cryptography? Explain.
- How does Kerberos authenticate each client? You may discuss Kerberos Ticket-Granting Server (TGS) and Ticket Granting Ticket (TGT).
- How does Kerberos tackle the problem of replay attacks?

You must also:

- Recommend a commercial software program for user authentication; and
- Explain and justify your recommendation clearly.

Part II Cloud Computing and Blockchain for Handling the Company's Data

As you were already informed, the CEO wants to keep her company's valuable data secure. She told you that she has heard about Cloud Computing and blockchain, and as a result, she wants to know if they could be used to keep the company's data secure. For this part, you are required to:

- Explain the possibility of employing Cloud Computing (CC) for the company to protect valuable data.
- You must recommend a kind/s of CC service/s to be used for the company's data as well as how data may be sent to an authorised partner securely using the Cloud. You will have to justify why you recommend such CC service/s over the other services.
- Explain blockchain in detail to the CEO. Furthermore, list and describe any drawbacks andadvantages of employing blockchain in general.
- You are to advise the possibility of using Blockchain to keep the company's data secure and whether blockchain is suitable for this purpose. Explain any drawbacks and advantages of employing blockchain within the company.
- You will have to explicitly make a recommendation and justification on employing blockchain for storing the company's data.

Part III Network Diagram employing Kerberos and Cloud Computing for Thailand Branch

Employing Kerberos for user authentication and Cloud Computing can be an effective means of protecting the company's valuable data. As such, you are required to design a network diagram for the Thailand branch of the company. To do this, you will need to consider the existing devices (see "About the company" – **Thailand branch ONLY**), the user authentication software you recommended in Part I, and Cloud Computing service/s you recommended in Part II.

You are required to:

1. Draw your proposed network diagram, including:
    a. User authentication software
    b. Cloud Computing service integrated into the Thailand branch network
    c. Existing devices (e.g. servers, workstations, routers, switches)

Continue on Next Page

2. Explain and justify the proposed network diagram with respect to the placement and purpose of each piece of hardware/software, user authentication software and CC service.

Part IV. References

- Use correct IEEE referencing style, see https://libguides.jcu.edu.au/IEEE

Assignment Guide/Template:

To get the highest marks possible, you should **READ THE RUBRIC** and follow the template below:

Part I User authentication

- Make a recommendation on Kerberos cryptography
  - Explain all aspects asked about Kerberos.
  - Recommendation and justification on a software off the shelf for user authentication.

Part II Cloud Computing and Blockchain for Handling the Company's Data

- Explain the possibility of employing CC for the company's valuable data.
  - Provide recommendations and justification on employing CC (which model you've recommended and why).
- Explain the possibility of employing Blockchain for the company's valuable data.
  - Explain blockchain, list and describe any advantages and disadvantages of using blockchain in general (with any other applications).
  - Explain any drawbacks and advantages of employing Blockchain within the company
  - Provide recommendations and justification for employing blockchain for storing the company's data.

Part III Network Diagram employing Kerberos and Cloud Computing for Thailand Branch

- Diagram
- Explanation and justification of the proposed configuration.

Part IV Use Correct IEEE Referencing Style

- includes in-text citation
- References at the end of the document using IEEE referencing Style

---

End of Assignment 2

See rubric on the next pages

CP2414 Assignment 2 Cryptography and Network Security Applications Rubric

Part	Criteria	Exemplary (9, 10)	Good (7, 8)	Satisfactory (5, 6)	Limited (2, 3, 4)	Limited (0, 1)	Weighting
Part I Kerberos and User Authentication	**Kerberos and User Authentication**	1. Kerberos is extremely well-explained. The explanation contains the following: a. Why Kerberos should be chosen for this purpose? b. Does Kerberos use symmetric or asymmetric cryptography? Explain. c. How does Kerberos authenticate each client? You may discuss Kerberos Ticket-Granting Server (TGS) and Ticket Granting Ticket (TGT). d. How does Kerberos tackle the problem of replay attacks?	Exhibits aspects of exemplary (left) and satisfactory (right)	1. Kerberos is reasonably explained. The explanation contains the following a. Why Kerberos should be chosen for this purpose? b. Does Kerberos use symmetric or asymmetric cryptography? Explain. c. How does Kerberos authenticate each client? You may discuss Kerberos Ticket-Granting Server (TGS) and Ticket Granting Ticket (TGT). d. How does Kerberos tackle the problem of replay attacks?	Exhibits aspects of satisfactory (left) and very limited (right)	Negligible attempt, nonsensical, or not done.	**10%**
Part II Cloud Computing and Blockchain for Handling the Company's Data	**Secure Cloud Computing**	1. Extremely well-explained the following: a. Explain the possibility of employing Cloud Computing (CC) for the company's valuable data. b. What Cloud Computing service/s can be used for the data? And how?		1. Reasonably explained the following: a. Explain the possibility of employing Cloud Computing (CC) for the company's valuable data. b. What Cloud Computing service/s can be used for the data? And how?			**15%**
	Cloud Computing Recommendation	1. State clearly whether Cloud Computing is recommended to be used with the company's valuable data. **IF** it is recommended, what kind CC service/s is recommended 2. Your recommendation is extremely well-justified.		1. State whether Cloud Computing is recommended to be used with the company's valuable data. **IF** it is recommended, what kind CC service/s is recommended 2 Your recommendation is reasonably justified.			**15%**

See Next Page

CP2414 Assignment 2 Cryptography and Network Security Applications Rubric (continue)

Part	Criteria	Exemplary (9, 10)	Good (7, 8)	Satisfactory (5, 6)	Limited (2, 3, 4)	Limited (0, 1)	Weighting
Part II Cloud Computing and Blockchain for Handling the Company's Data	**Business and Blockchain Integration**	1. Blockchain is extremely well-explained. 2. How Blockchain can be used for storing the company securely is extremely well-explained. 3. Advantages and disadvantages of employing Blockchain in general and with the company's data are extremely well-explained. 4. Recommendation and justification on employing blockchain for storing the company's data is extremely well-discussed.	Exhibits aspects of exemplary (left) and satisfactory (right)	1. Blockchain is reasonably-explained. 2. How Blockchain can be used for storing the company securely is reasonably-explained. 3. Advantages and disadvantages of employing Blockchain in general and with the company's data are reasonably-explained. 4. Recommendation and justification on employing blockchain for storing the company's data is reasonably-discussed.	Exhibits aspects of satisfactory (left) and very limited (right)	Negligible attempt, nonsensical, or not done.	**20%**
Part III Network Diagram employing Kerberos and Cloud Computing for Thailand Branch	**Kerberos, CC service and other devices Diagram and Labels**	Diagram is accurate and includes: 1. Kerberos 2. CC service 3. all relevant devices 4. lines 5. labels		Diagram is considered accurate and at least half of the following are satisfactory: 1. Kerberos 2. CC service 3. all relevant devices 4. lines 5. labels			**15%**
	Analysis and Recommendation - Kerberos, CC service and other devices	Clear and accurate explanation to the following questions: 1. Why each of the devices/Software/CC is placed where it is placed in the diagram? 2. What are the purposes and advantages of placing it there?		Sufficiently clear and accurate explanation to the following questions: 1. Why each of the devices/Software/CC is placed where it is placed in the diagram? 2. What are the purposes and advantages of placing it there?			**20%**
Part IV Citation	**Citation and referencing**	Excellent citing and excellent use of IEEE style		Correct citing and correct use of IEEE style.			**5%**