**JAMES COOK UNIVERSITY**

Cryptography and Network Security Applications

**Student ID**

**Date YYYY**

**UNIT LEADER**

Contents

[1.0 Introduction 3](#_Toc124431925)

[2.0 PART (I) The User authentication 4](#_Toc124431926)

[3.0 PART (II) Cloud Computing and blockchain for handling the Company's data 6](#_Toc124431927)

[3.1 Cloud computing 6](#_Toc124431928)

[3.2 Blockchain 7](#_Toc124431929)

[4.0 PART (III) Cloud Computing and blockchain for handling the Company's data 8](#_Toc124431930)

[4.1 Proposed Network Diagram 9](#_Toc124431931)

[4.2 Kerberos-Based User Authentication System 11](#_Toc124431932)

[4.3 Cloud Computing Service 11](#_Toc124431933)

[4.4 Existing Devices 12](#_Toc124431934)

[5.0 Conclusion 12](#_Toc124431935)

[References 14](#_Toc124431936)

[Figure 1 Network Diagram for Thailand Branch 9](#_Toc124431912)

# 1.0 Introduction

The ever-evolving digital landscape presents organizations with a host of challenges, particularly those relating to the security of their data and resources [1]. Data security is of paramount importance to any business, and The Thailand branch of MEDASIA is no exception. The MEDASIA is a leading global company in the manufacturing industry, with a presence in Thailand, China, and the United States [2]. As a result, it is essential that MEDASIA’s data is secure and accessible.

In order to ensure the security of their data and resources, organizations must have the right security measures in place. This includes a robust user authentication system, an effective cloud computing service, and secure existing devices [1]. MEDASIA has proposed a network diagram that integrates a Kerberos-based user authentication system, a cloud computing service, and the existing devices into a secure, efficient network. Kerberos is an authentication protocol that uses tickets to authenticate users and grant them access to resources [3]. It is widely used in network and computer security applications and is the default authentication system used in Windows operating systems. The Kerberos-based user authentication system is the cornerstone of the proposed network. It is designed to ensure that only authenticated users are able to access MEDASIA’s data and systems.

The proposed network also includes a cloud computing service. Cloud computing is a form of distributed computing that allows users to access applications and data stored on remote servers [1]. This allows MEDASIA to reduce the cost of computing power by leveraging the resources of multiple machines. The cloud computing service is designed to provide high levels of availability and scalability. The existing devices in the Thailand branch include two mail servers, three web servers, and three database servers [2]. All of these devices are connected to the network via routers and switches, which are used to manage traffic and ensure that the data is securely transmitted. The routers and switches are responsible for routing traffic between the different devices in the network. The routers are also responsible for providing access to the internet. Finally, the existing devices are connected to the network via routers and switches, which are responsible for routing traffic and providing access to the internet. By integrating these systems, MEDASIA can be confident that their data is secure and accessible.

This paper will discuss the proposed network diagram in detail, including the Kerberos-based user authentication system, the Cloud Computing service, and the existing devices. It will also discuss the advantages and disadvantages of using the proposed network diagram and how it can provide a secure and efficient way to manage the company’s data and resources.

# 2.0 PART (I) The User authentication

Kerberos is an authentication protocol that can be used to verify the identity of users and services on an open network [4]. Kerberos allows client/server applications to securely identify themselves to one another. It is a secure and reliable way of authenticating users in a distributed environment such as a corporate network [5]. It provides a secure point of access to the network, allowing users to access resources and services on the network by providing a cryptographically secure method of authentication [6]. Kerberos is a widely used and highly recommended security protocol that should be utilized for user authentication purposes [7].

The main reason why Kerberos should be chosen for user authentication purposes is that it is a secure protocol that achieves mutual authentication of users and services on the network [8]. It makes use of symmetric cryptography, which is a type of encryption that uses the same key for both encryption and decryption. In the case of Kerberos, the secret key is shared between the user/client and the authentication server, which is used to both encrypt and decrypt data when sent over the network [9]. This means that all data is encoded and decrypted using the same key, making it secure and reliable.

Kerberos authentication involves three different components: the Kerberos server, the Ticket-Granting Server (TGS), and the application server [10]. The Kerberos server is responsible for authenticating the user and issuing a Ticket-Granting Ticket (TGT) to the user [11]. The TGT is a cryptographically secure token which is generated by the TGS and is used to identify the user [12]. The TGT is sent to the user when they request access to a resource on the network. When the user attempts to access the resource, the TGT is sent to the TGS, which then verifies the user’s identity and grants or denies access to the requested resource. The TGS is a trusted third-party server that authenticates the user and grants access to the application server. The application server is the server where the user is trying to gain access to.

The Kerberos protocol works by authenticating the user and granting them access to the application server. The process starts when the user sends a request to the Kerberos server [12]. The Kerberos server then authenticates the user and issues a Ticket-Granting Ticket (TGT) to the user [13]. The TGT contains information about the user, such as their username and password. The user then sends the TGT to the TGS, which authenticates the user and grants them access to the application server.

Kerberos also tackles the problem of replay attacks by using timestamps [14]. Timestamps are used to ensure that the TGT is only valid for a certain period of time. This helps to prevent attackers from re-using the TGT and allows the authentication process to be more secure and reliable. A timestamp is a numerical value that is used to verify the authenticity of a request. Each time a user sends a request to the Kerberos server, the server assigns a timestamp to the request [15]. This timestamp must be included in the request when it is sent to the TGS. The TGS will check the timestamp and if it is not valid or if it is older than a certain amount of time, the request will be rejected. This prevents attackers from replaying old requests and gaining access to the application server.

For MEDASIA, I recommend the use of Symantec Advanced Authentication (SAA) for user authentication [16]. SAA is a commercial software program that provides multi-factor authentication for users. It makes use of a variety of authentication methods, such as passwords, one-time passwords, biometric authentication, and two-factor authentication [16]. It is also easy to use and can be easily integrated into existing systems. Symantec’s Endpoint Protection Enterprise Edition is an ideal choice for MEDASIA’s user authentication requirements as it is a reliable and secure security solution [16]. It also provides a comprehensive set of features that can help to protect the company’s network resources from malicious threats [16]. Additionally, the software is easy to install and manage, making it a great choice for IT administrators [16]. This software provides a comprehensive suite of security solutions, including Kerberos authentication [16]. Endpoint Protection Enterprise Edition also offers a variety of other security features such as antivirus, anti-malware, and personal firewall protection [30]. It is also equipped with advanced technologies such as reputation-based protection and application control, which helps to protect critical network resources from malicious threats [16].

Generally, Kerberos is a secure and reliable way of authenticating users in a distributed environment. It makes use of symmetric cryptography, which is a secure type of encryption that uses the same key for both encryption and decryption. It also provides a way to tackle the problem of replay attacks by using timestamps. For MEDASIA, I recommend the use of Symantec Advanced Authentication (SAA) for user authentication. SAA is a commercial software program that provides multi-factor authentication for users and can be easily integrated into existing systems.

# 3.0 PART (II) Cloud Computing and blockchain for handling the Company's data

## 3.1 Cloud computing

Cloud computing is an increasingly popular way to store and access data [17]. It provides the user with a virtual environment in which to store and access data and applications. The user is not required to own any hardware or software, instead they gain access to the data and applications they need over the internet. Cloud computing can provide a number of advantages to companies looking to store and access data securely and efficiently [18].

The main advantage of cloud computing is that it is more cost effective than traditional hosting solutions. Companies no longer have to purchase and maintain expensive hardware and software, as they can access the resources they need over the internet. This means that companies can save money on capital expenditure and operational costs. Furthermore, cloud computing is more reliable than traditional hosting solutions as the cloud provider can manage the resources and ensure that the data is always available.

Cloud computing also provides greater flexibility for companies. Companies no longer have to maintain their own hosting infrastructure and can access the resources they need on demand. This means that companies can scale up or down their computing resources as needed and only pay for what they use. Cloud computing also provides greater security as the cloud provider can manage the security of the data and ensure that it is not compromised.

In terms of using cloud computing for MEDASIA, there are a number of services that can be used [19]. One of the most popular services is Infrastructure-as-a-Service (IaaS). This is a type of cloud computing service in which the user is provided with the hardware and software they need in the form of virtual machines. This means that MEDASIA can access the computing resources they need without having to purchase and maintain their own hardware and software. This is a great option for MEDASIA as it can provide cost savings and greater flexibility.

Another service that can be used is Platform-as-a-Service (PaaS). This is a type of cloud computing service in which the user is provided with a platform upon which to develop and deploy applications. This means that MEDASIA can develop and deploy applications to the cloud without having to worry about maintaining their own hardware and software. This is a great option for MEDASIA as it can provide cost savings and greater flexibility. MEDASIA can use Software-as-a-Service (SaaS). This is a type of cloud computing service in which the user is provided with the software they need in the form of applications. This means that MEDASIA can access the applications they need without having to purchase and maintain their own software. This is a great option for MEDASIA as it can provide cost savings and greater flexibility.

In terms of sending data securely to an authorized partner using the cloud, MEDASIA can use a number of different services. One of the most popular services is Virtual Private Networks (VPNs). A VPN is a type of network in which the user is provided with a secure connection to the cloud provider. This means that the user can securely send data over the internet without having to worry about it being intercepted. Furthermore, MEDASIA can use encryption to ensure that the data is secure while it is in transit.

Another service that can be used is Secure File Transfer Protocol (SFTP). This is a type of file transfer protocol in which the user is provided with a secure connection to the cloud provider. This means that the user can securely send files to the cloud provider without having to worry about them being intercepted. Furthermore, MEDASIA can use encryption to ensure that the files are secure while they are in transit. Cloud computing can provide a number of advantages to MEDASIA. It can provide cost savings and greater flexibility, as well as greater security. Furthermore, MEDASIA can use a number of different services to securely send data to an authorized partner using the cloud.

## 3.2 Blockchain

Blockchain is an increasingly popular technology that is being used to store and access data securely [20]. It is a distributed database in which records are stored in blocks that are linked together using cryptographic techniques. This means that the data is secure and cannot be changed or deleted. It is also transparent as the records are publicly visible.

There are a number of advantages to using blockchain. Firstly, it is secure as the data is stored in a distributed database that is secure and cannot be changed or deleted. This means that the data is safe from hackers and other malicious actors. Furthermore, it is transparent as the records are publicly visible. This means that anyone can view the records and verify the accuracy of the data. In addition, blockchain is also efficient as it does not require a central authority to facilitate transactions. This means that transactions can be completed quicker and more efficiently. Furthermore, blockchain is also cost effective as it does not require any additional hardware or software to be purchased.

There are also a number of drawbacks to using blockchain. Firstly, it is slow as it is a distributed database and requires a consensus from all participants in order to validate a transaction. This means that transactions can take a long time to complete. Furthermore, blockchain is also expensive as a large amount of computing power is required to run a blockchain network.

In terms of using blockchain for MEDASIA, it is possible to use blockchain to store and access data securely [20]. MEDASIA can use a number of different technologies such as Hyperledger Fabric or Ethereum to create a blockchain network that is secure and transparent. This means that MEDASIA can store and access data securely and efficiently.

However, there are a number of drawbacks to using blockchain. Firstly, it can be slow as it requires a consensus from all participants in order to validate a transaction. This means that transactions can take a long time to complete. Furthermore, blockchain is also expensive as a large amount of computing power is required to run a blockchain network.

Blockchain can provide a number of advantages to MEDASIA. It is secure, transparent, efficient and cost effective. However, there are a number of drawbacks to using blockchain, such as its slow speed and high cost. Therefore, it is important for MEDASIA to weigh up the pros and cons of using blockchain before making a decision.

Based on the information provided, it is possible for MEDASIA to use cloud computing and blockchain to store and access data securely. Cloud computing can provide cost savings and greater flexibility, as well as greater security. Furthermore, MEDASIA can use a number of different services to securely send data to an authorized partner using the cloud.

In terms of blockchain, it is possible to use blockchain to store and access data securely. MEDASIA can use a number of different technologies such as Hyperledger Fabric or Ethereum to create a blockchain network that is secure and transparent. However, there are a number of drawbacks to using blockchain, such as its slow speed and high cost. Therefore, it is important for MEDASIA to weigh up the pros and cons of using blockchain before making a decision.

Both cloud computing and blockchain can provide a number of advantages to MEDASIA. Therefore, MEDASIA should consider using both technologies in order to ensure the security of their data.

# 4.0 PART (III) Cloud Computing and blockchain for handling the Company's data

The proposed network diagram is designed to provide a secure and efficient way to manage the company’s data and resources. The combination of the Kerberos authentication system and the user authentication software ensures that only authenticated users are granted access to resources. The Cloud Computing service is designed to provide a secure, scalable, and cost-effective way to manage and store data. The existing devices are used to store the data and resources and to provide access to them. The router and switch are used to manage traffic and ensure that the data is securely transmitted.

## 4.1 Proposed Network Diagram

The proposed network diagram of the Thailand branch of MEDASIA incorporates Kerberos for user authentication and Cloud Computing services. The diagram is divided into three main sections: the user authentication section, the Cloud Computing section, and the existing devices into a secure, efficient network. The diagram is shown below.

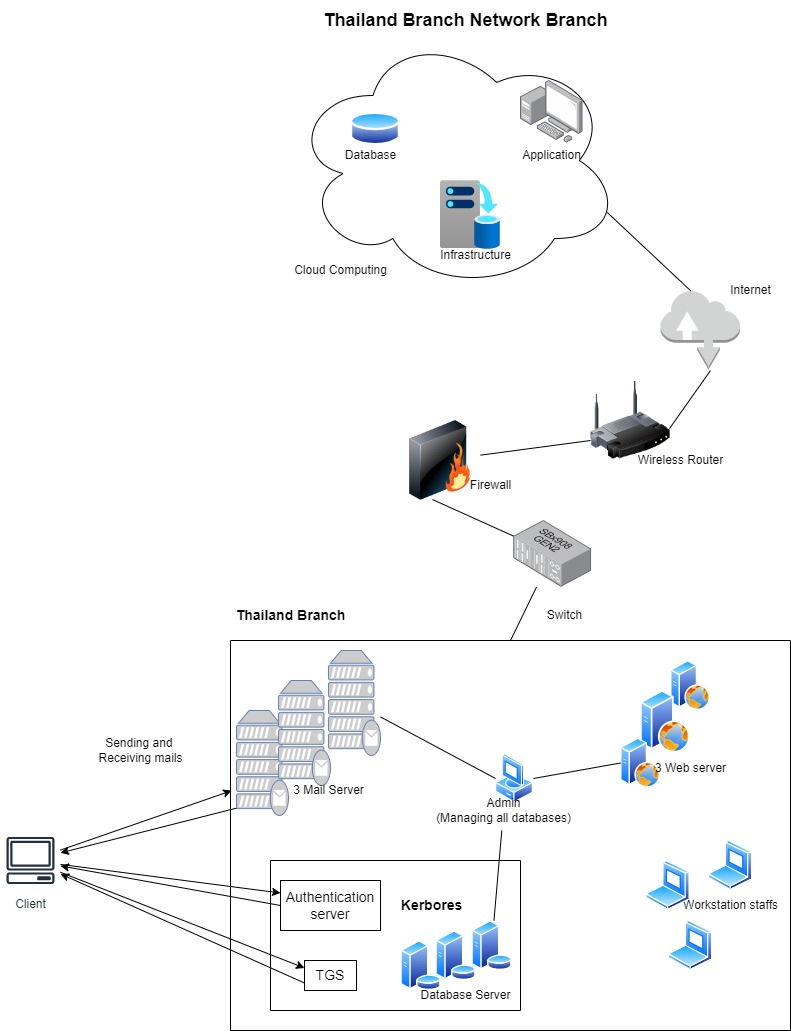


Figure Network Diagram for Thailand Branch

## 4.2 Kerberos-Based User Authentication System

Kerberos is an authentication protocol that uses tickets to authenticate users and grant them access to resources. It is widely used in network and computer security applications, and is the default authentication system used in Windows operating systems. The Kerberos-based user authentication system is the cornerstone of the proposed network. It is designed to ensure that only authenticated users are able to access MEDASIA’s data and systems. The Kerberos system is based on the concept of a trusted third-party authentication server (KDC). The KDC is responsible for verifying the identity of users and issuing tickets that are used to gain access to the network. The KDC is also responsible for maintaining a secure key distribution center (KDC) that stores the private keys used in authentication.

The authentication process begins when a user attempts to gain access to the network. The user first authenticates with the KDC, which verifies the user’s identity. If the user is successfully authenticated, the KDC issues a ticket that is used to gain access to the network. The ticket is encrypted and contains a session key that is used to encrypt the data that is exchanged between the user and the network.

The Kerberos system is also designed to be highly secure. All of the communications between the user and the KDC are encrypted using a secure key exchange protocol. Furthermore, the Kerberos system is designed to be resistant to replay attacks, meaning that an attacker cannot simply replay an authentication request and gain access to the network.

## 4.3 Cloud Computing Service

The proposed network also includes a cloud computing service. Cloud computing is a form of distributed computing that allows users to access applications and data stored on remote servers. This allows MEDASIA to reduce the cost of computing power by leveraging the resources of multiple machines.

The cloud computing service is designed to provide high levels of availability and scalability. The service is designed to provide redundancy so that if one server fails, the remaining servers can still provide access to the applications and data. Furthermore, the service can be scaled up or down as needed to meet the changing needs of the business.

The cloud computing service is also designed to be secure. All of the data stored on the cloud is encrypted and access is restricted to only authorized users. Furthermore, the service is designed to be resistant to attacks such as denial of service (DoS) attacks.

The Cloud Computing section of the diagram consists of the Cloud Computing service integrated into the Thailand branch network. The Cloud Computing service is responsible for managing the company’s data and resources, as well as for providing secure access to them. The Cloud Computing service is designed to provide a secure, scalable, and cost-effective way to manage and store data.

## 4.4 Existing Devices

The existing devices in the Thailand branch include two mail servers, three web servers, and three database servers. The mail servers are responsible for sending and receiving emails. The web servers are responsible for hosting the company’s web applications, while the database servers are responsible for storing and retrieving the company’s data. All of these devices are connected to the network via routers and switches, which are used to manage traffic and ensure that the data is securely transmitted.

The routers and switches are responsible for routing traffic between the different devices in the network. The routers are also responsible for providing access to the internet. The switches are responsible for connecting the different devices in the network, allowing them to communicate with each other.

The proposed network diagram for the Thailand branch of MEDASIA integrates a Kerberos-based user authentication system, a cloud computing service, and the existing devices into a secure, efficient network. The Kerberos system is designed to ensure that only authenticated users are able to access MEDASIA’s data and systems. The cloud computing service is designed to provide high levels of availability and scalability, while also being secure and resistant to attacks. Finally, the existing devices are connected to the network via routers and switches, which are responsible for routing traffic and providing access to the internet. By integrating these systems, MEDASIA can be confident that their data is secure and accessible.

# 5.0 Conclusion

In conclusion, the proposed network diagram for MEDASIA’s Thailand branch is designed to provide a secure and efficient way to manage the company’s data and resources. The combination of the Kerberos authentication system, the user authentication software, and the Cloud Computing service ensures that only authenticated users are granted access to resources. The Cloud Computing service is designed to provide a secure, scalable, and cost-effective way to manage and store data. The existing devices are used to store the data and resources and to provide access to them. The router and switch are used to manage traffic and ensure that the data is securely transmitted.

Kerberos is an authentication protocol that uses tickets to authenticate users and grant them access to resources. It is widely used in network and computer security applications, and is the default authentication system used in Windows operating systems. The Kerberos-based user authentication system is the cornerstone of the proposed network. It is designed to ensure that only authenticated users are able to access MEDASIA’s data and systems. The Kerberos system is based on the concept of a trusted third-party authentication server (KDC). The KDC is responsible for verifying the identity of users and issuing tickets that are used to gain access to the network. The Cloud Computing service is designed to provide a secure, scalable, and cost-effective way to manage and store data. The service is designed to provide redundancy so that if one server fails, the remaining servers can still provide access to the applications and data. Furthermore, the service can be scaled up or down as needed to meet the changing needs of the business. The cloud computing service is also designed to be secure. All of the data stored on the cloud is encrypted and access is restricted to only authorized users. Furthermore, the service is designed to be resistant to attacks such as denial of service (DoS) attacks. The existing devices in the Thailand branch include two mail servers, three web servers, and three database servers. The mail servers are responsible for sending and receiving emails. The web servers are responsible for hosting the company’s web applications, while the database servers are responsible for storing and retrieving the company’s data. All of these devices are connected to the network via routers and switches, which are used to manage traffic and ensure that the data is securely transmitted.

In summary, the proposed network diagram for MEDASIA’s Thailand branch provides a secure and efficient way to manage the company’s data and resources. The combination of the Kerberos authentication system, the user authentication software, the Cloud Computing service, and the existing devices create a secure, efficient network. This network ensures that MEDASIA’s data is secure and accessible, while also providing cost savings and greater flexibility.

# References

|  |  |
| --- | --- |
| [1] | A. Lal, M. Parekh and A. Sheth, "Security Measures in Cloud Computing.," *International Journal of Computer Applications, 186(7), ,* pp. 1-8., 2020. |
| [2] | MEDASIA., 2021. [Online]. Available: https://www.medasia.co/th/about-us. |
| [3] | J. Feng, "Overview of Kerberos Authentication.," 2020. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview. |
| [4] | B. Clifford Neuman. and Theodore Ts'o, "Kerberos: An Authentication Service for Open Network Systems,", USENIX Conference Proceedings, 1993. |
| [5] | T. B. Jansen., "Securing Computer Networks: An Introduction to cryptography and network security,", John Wiley & Sons, 2008. |
| [6] | M. P. Robshaw, "Cryptography and Network Security: Principles and Practice,", Pearson Education, 2003. |
| [7] | D. R. Stinson., "Cryptography: Theory and Practice, CRC Press, 2006. |
| [8] | M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Management,", 1994. |
| [9] | R. L. Rivest, A. Shamir and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,", Communications of the ACM, 1998. |
| [10] | M. B. Greenwald, "The Kerberos Authentication System," in Network and Distributed System Security Symposium, 1995. |
| [11] | S. J. Murdoch, M. R. Anderson and B. D. Payne, "The Kerberos Network Authentication Protocol Version 5,", Internet Draft, RFC , 1992. |
| [12] | M. B. Greenwald, "The Kerberos Authentication System," in Network and Distributed System Security Symposium, 1995. |
| [13] | S. J. Murdoch, M. R. Anderson and B. D. Payne, "The Kerberos Network Authentication Protocol Version 5,", Internet Draft, RFC , 1992. |
| [14] | W. Diffie and M. E. Hellman, "New Directions in Cryptography,", 1976. |
| [15] | S. J. Murdoch, M. R. Anderson and B. D. Payne, The Kerberos Network Authentication Protocol Version 5,", Internet Draft, RFC , 1992. |
| [16] | Symantec, "“Advanced Authentication: Multi-factor Authentication Solutions,”," 2018. [Online]. Available: https://www.symantec.com/products/endpoint-protection/advanced-authentication.. |
| [17] | X. L. J. Meng, X. Wang and Y. Liang, The research of cloud computing security: A survey. Computers & Security, 2020. |
| [18] | P. S. Raju, P. Raju and S. Raju, "An overview of cloud computing: Benefits, challenges, and security.," *International Journal of Computer Applications,* 2018. |
| [19] | V. Raghunath, A. Balasubramani and D. S. Shetty, "Cloud computing: introduction, benefits, types, challenges, and security issues.," *International Journal of Computer Applications, 150(20), ,* pp. 8-14., 2017. |
| [20] | Lam, W. W. Y., R. W. C. Law and S. Y. Yiu, "Blockchain technology and applications: a systematic literature review of papers and frameworks.," *International Journal of Information Management, 38(2),,* pp. 121-136., 2018. |