Chapter 6

CONCLUSION AND SCOPE FOR FUTURE WORK

This chapter presents the conclusion of the thesis. This chapter is organized in two sections. Section 6.1 presents concluding remarks and section 6.2 discusses the possible scope for future works.

6.1. Concluding Remarks

The research contributions of this thesis are as follows:

In Chapter 1, the concepts of cloud computing, especially service models and implementation models were presented with relevant examples. The motivation for the work is described, and the objectives of this thesis were also presented in this chapter. The last section of this chapter lists a thesis plan describing the coverage in the chapters.

In Chapter 2, we discussed the basic concepts associated with the problems and tasks of cloud computing security. This chapter also discusses a bibliographic study related to the problems and tasks of cloud computing, mainly for security reasons. Cloud computing provides benefits that include resource sharing, location independence, profitability, but there are many practical problems that need to be addressed. In addition, the control of infrastructure security is somewhat beyond the control of the client. The client can still encrypt data on the way to the cloud. In the near future, it will be necessary to provide security as a service as the sole responsibility of the CSP, since the administration of data security in the cloud will present complexity and risks of data loss. Customers also need to consider SLA (Service Level Agreements) with CSP and eliminate potential problems related to the protection of liability and data.

Chapter 3 introduces an integrated authentication model for the security and privacy of cloud computing based on Kerberos and Pretty Good Privacy. In this chapter, we present an integrated model that guarantees the security and privacy of the user and provider of cloud services. To provide detailed security in the cloud, there are several methods and mechanisms, and ideas are offered and presented. In this regard, we propose a framework that uses Pretty Good Privacy (PGP) and security based on Kerberos in cloud computing. Kerberos demonstrates the identity of users across networks and ensures the integrity and confidentiality of data. Kerberos performs a secure verification of users and services based on the concept of a trusted third party (KDC). But one of the weaknesses of Kerberos is that it can not provide the characteristics of rejection of communication, therefore we improve this function of refusing rejection of our proposed work using the Pretty Good Privacy program, we know that PGP uses digital signature functions in communication. PGP provides skills to people to take their personal lives in their hands.

In Chapter 4, a general algorithm for the OTP algorithm for remote authentication was proposed. This document presents an authentication scheme in which a one-time password is created on the user's mobile phone. OTP algorithms on the client and server side use the number of attempts and user credentials to create OTP. The client-side attempt number is the number of times the user generates OTP on the mobile device. And the server-side attempt number is the user's attempt to log on to the website. The server then checks the user according to the entered OTP. This method does not require synchronization between the mobile device and the server or sending SMS-based OTP to users. This method is more secure, because strict passwords are generated using strong hash functions

In Chapter 5 in this chapter, we report that the level of authentication used by the cloud service provider should match the risks associated with these products and services. The cloud service provider must conduct risk assessments to determine the types and levels of risk associated with their Internet banking applications. Here, risk assessments indicate that the use of one-factor authentication is inadequate, financial institutions need to implement multifactor authentication, tiered protection, or other management tools that are reasonably designed to mitigate these risks. Agencies believe that the authentication of one factor, as the only control mechanism, is insufficient in the case of transactions with a high level of risk associated with access to customer information or movement of funds to other parties.

Multifactor authentication for access control has become the most important requirement for cloud computing to achieve the goals of secrecy, integrity and confidentiality. It is important to more closely integrate computer and network security to develop a true security discipline in the cloud. We use multi-factor access mechanisms to authenticate an individual.

6.2. Scope for Future Work

The research work presented in this thesis can be deepened in different directions, which are described in detail below:

In the future, we strive and try to improve the technique of collecting biometric data. This will greatly improve the user identification process, which uses a common biometric recognition system. Thus, this will lead us to another step towards a cloud-based and secure cloud computing network.

There are several limitations that can be difficult with the correct implementation of user authentication through multifactor mechanisms. The effectiveness of the proposed structure depends on several factors, such as the lack of availability of the mobile network, which can cause a delay in obtaining the TNA and the expiration of the session. Future work can be to reduce the delay in receiving OTP. The system also depends on the FRR (false deflection rate) of the biometric device, so in the future the FFR will be improved.