Zuriati Ahmad Zukarnain, J Inform Tech Soft Engg 2015, 5:2
http://dx.doi.org/10.4172/2165-7866.S1.002

QKD communication protocol for authentication mechanism of cloud network

Zuriati Ahmad Zukarnain
University Putra Malaysia, Malaysia

Quantum Key Distribution (QKD) protocol is a unique communication protocol for authentication mechanism of cloud network in replacing the key distribution technique based on public key infra-structure to achieve unconditional security in cloud. Cloud infrastructure provides many benefits in terms of low cost and accessibility of data. Ensuring the security aspect is a major factor in the cloud infrastructure. Currently, there are certain issues pertaining on Public Key Infrastructure (PKI) in cloud systems. It is obviously shown that there is no sufficient secured procedure to move private keys between clouds' clients. At the same time, there is no certificate authority separation. Thus, it does not provide a secure authentication and authorization of cloud network. This QKD protocol is believed to detect any eaves-dropping activities and provide an effective security. The Quantum Key Distribution (QKD) protocol used the concept of multi-party QKD (MQKD) which allows the same key, distributed to different parties based on quantum mechanism. A quantum key server generates a secret key that may strengthen the security aspects. A quantum key distribution key scheme is imposed in the cloud network to secure the top-secret message or information and capture the eaves-dropper. The existence of quantum key storage between the cloud provider and cloud client may guarantee the integrity of communication process that ensure the party is authenticated and the communication cannot be intercepted. To achieve the practical feasibility and simplicity in MQKD, a standard cryptographic like authentication scheme is designed. The simulation results show that our proposed protocol provides authentication of the clients is acceptable response to error rate and time. In addition, our results show that the proposed scheme could reduce amount of information leak.

Biography

Zuriati Ahmad Zukarnain is an Associate Professor at the Faculty of Computer Science and Information Technology, University Putra Malaysia. She is the Head for high performance computing section at Institute for Mathematics and Research (INSPEM), University Putra Malaysia. She received her PhD from the University of Bradford, UK. Her research interests include efficient multiparty QKD protocol for classical network and cloud, load balancing in the wireless ad hoc network, quantum processor unit for quantum computer, authentication time of IEEE with multiple-key protocol, intra-domain mobility handling scheme for wireless networks, efficiency and fairness for new AIMD algorithms and a kernel model to improve the computation speed-up and work-load performance. She has published more than 100 papers in reputed journals and has been actively involved as a Member of the Editorial Board for some international peer-reviewed and cited journals. She is currently undertaking some national funded projects on QKD protocol for cloud environment as well as routing and load balancing in the wireless ad hoc network.

zuriati@upm.edu.my

Notes: