Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 149 – 156

Procedia Computer Science

2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Big data security issues based on quantum cryptography and privacy with authentication for mobile data center

Vijey Thayananthan* and Aiiad Albeshri*

Department of Computer Science, FCIT, KAU, Jeddah 21589, KSA

Abstract

Enhancement of security and privacy in mobile data centers is challengeable with efficient security key management. In order to solve this problem, data centers need efficient quantum cryptography using Grover's algorithm and authentication technique which are appropriate approaches to enhance the security and privacy with less complexity. In this research, quantum cryptography with the PairHand protocol seems to be a better approach. In future, light which has same quantum properties will be the best approach because people can see only the light not the data. So, light based on quantum cryptography and PairHand protocols will be the best for this research.

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Keywords: Big data security and privacy; Quantum cryptography; PairHand protocol; Key management; Data center

1. Introduction

There are many solutions which are available for solving data security in data centers but implementing strong security for which big data (size > 1Terra Byte) being approached to the data center is one of the interesting topics. According to Couch and Robins [1], big data based on digital information has been doubling every 2 years since 2011. Based on the recent research, estimate also suggested that 2.5 zettabytes (2.5×10^{21} bytes) of information

* Corresponding author: Vijey Thayananthan. Tel.:+0966 6952000; fax:+0966 6952000.
E-mail address: vthayanathan@kau.edu.sa

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)
doi:10.1016/j.procs.2015.04.077

handled in 2012. Keeping privacy is another big issue in mobile data center which handles the data using proper management techniques. Goorden et al. [2] explained that Quantum cryptography (QC) supported to generate the authenticated key which provides security through the key management between the authentication server and users involved in the mobile data center. It includes efficient key searching and generating different size of keys with less complexity as big data security issues. Authentication supports privacy through the verifications and validations of entities which are authentication servers and mobile users. Thus, we can control the security and the privacy of big data which may be either sensitive or secret information. Here, proper authentication protocol which reduces the computation complexity when data centers handle the big data may be useful because the complexity prevents from creating the dynamic security solutions. Further, this complexity increases the traffic; delay and storage problems seem to be a quick chance of pilfering the data. This situation needs to be addressed using efficient authentication protocols to control the security and privacy dynamically. There is a trade-off between the complexity and big data security with traffic which is unavoidable during the data handling in the mobile data center.

According to Thayananthan et al. [3], QC is designed with Grover's algorithm (GA), which has simple and quick procedure to optimize the searching operations in the key management (KM). In this research, block cipher used as conventional algorithm can be implemented with QC which allows us to handle the big data and its key for the security and privacy. The GA is very attracted to big data when quantum information is used as a big data and quantum processing of big data helps to carry secure messages between the mobile users and data centers that hold the authentication server. All quantum techniques in QC need quick and efficient processing steps to avoid the unnecessary attacks during the big data transmission. Size of the big data is the growing but it should be limited to make efficient key development and management. Further, QC generate the key dynamically and control the necessary security issues appeared during the transmission.

Key handling and management provide necessary support to big data security issues because dynamic key generation for the big data is not simple when we use existing cryptographic techniques. In this mobile environment, mobile users and data centers can be anywhere in the land, space or under the sea. This is like a wireless sensor network which needs specific key management to look at the data and to secure the channel used for the data transmission between the nodes. Thayananthan and Alzahrani [4] mentioned that key management in wireless sensor network can be used in this research.

In the existing work, security protocols and other privacy issues based on authentication protocols use only bitwise operations but these operations are not suitable for big data. In this research, quantum bits (qbits) operations seem that mobile data centers get big data security and privacy very quickly and efficiently. When multiple authentication and re-authentications are used in the data center, passive attacks will be increasing. Security issues which affect the big data are defendable using QC with efficient protocols that minimize the searching steps and operations.

In this research, we have considered three contributions that provide necessary data security and privacy for future data centers that may be either fixed or mobile. Firstly, general information about big data security and privacy being collected from recent researches is that we try and understand the concept of big data, necessary security and privacy, and specific security in the mobile data center located in all environments. Secondly, big data security in mobile data center seems that users from all sectors expect to use strong keys with key management and authentication between the mobile user nodes and the authentication server. Here, we have considered to employing the quantum cryptography which supports to generate strong keys with less complexity and PairHand protocol that provides the necessary security based on handover authentication that is applicable in mobile environments. Finally, privacy is another issue related to human nature and behavior that means that confidential information must be protected from the public including the authorized staffs who work in the data center. Although maximum protection is established in all diplomatic organizations, privacy issues of big data used in government and diplomatic organization are still in unsafe. So, in this research, we investigate the general solution of big data privacy considered in a large organization such as hospitals and academic institutions. We hope these contributions will be better to establish big data security protocols or platforms with all necessary credentials in future data centers.

The rest of the paper is organized as follows. Section 2 explains the related work which is useful for the big data security issues such as key management. In section 3, proposed research which uses the QC with a specific algorithm and PairHand protocol is considered. Section 4 provides the necessary results and discussions that

organize the key management for the big data security in future data centers. In section 5, overall conclusions are written based on the theoretical analysis and results.

2. Related work and useful background

Big data security and privacy is the one of the expected solutions in large organizations where they can establish the maximum protection controlled by the data center that is either fixed or mobile. Quantum cryptography provides not only the maximum security to which big data exchanges between the data center and users but also it reduces the key search operations which are part of security issues organized in the key management of the data center. Some protocols are easy to design when applications use different architectures which not only depend on the data size but also data traffic.

2.1. Quantum cryptography for big data security

In this research, quantum cryptography provides maximum protection with less complexity that increases the storage capacity and security strength of the big data. In this section, we need to remember the use of symmetric key with a block cipher which is suitable to control the big data security because the design of the block cipher for the big data is very simple. Complexity always increases when we use large blocks but we can minimize the processing steps dynamically. Here, block cipher using GA which provides efficient key search is one of the best QC approaches in big data security procedures. Through this algorithm, secure communications between the mobile users and authentication server can be established.

In symmetric key developments, block ciphers designed with GA are very powerful to make an efficient key management scheme for future data centers. Assume any block cipher of key size is n. So, following the equation (1) reduces the steps and complexity when secret key is established in the attack.

$$complexity = O\left(\sqrt{2^n}\right) \tag{1}$$

In the conventional key management scheme, equation (1) had to use for many passive attacks, which require more steps than equation (2).

$$complexity = O\left(2^n\right) \tag{2}$$

2.2. Handover authentication for mobile data center

According to Lin at el. [5-7], authentication in wireless application is studied to investigate the wireless security and privacy involved in the mobile channels. In mobile data center, users should be able to send their big data from any location that is nearest to the mobile data center. When users send their big data to mobile data center, handover problems occur as big data security issues which need proper mechanism to control the security of the big data transmitted between the authentication server located in the data center and users. In this research, we consider the PairHand authentication protocol which supports to control the security issues and privacy in mobile data centers.

2.3. PairHand authentication protocol

Handover authentication procedures use many different protocols which take more than two handshakes and increase the computations as in He et al. [8-9]. In this research, handover authentication procedure is given in Cao et al. [10] is also analyzed to design the theoretical model. PairHand protocol has four procedures that are available in recent articles applied for different scenarios of mobile communications and networks. They are system initiation,

handover authentication, batch authentication, and DoS attack resistance respectively. It uses only two handshakes during the operations of which authentications are being established between the users and mobile data centers. Following four steps are briefly outlined to propose our design implemented within the theoretical model.

Firstly as in, the mobile user U_i computes the signature S_i as (3). Here, H_1 and H_2 are hash functions and k is used for calculating the private key.

$$S_i = H_2(U_i) k H_1(uid_i) \tag{3}$$

Where $U_i = uid_i \| ID_{APy} \| ts$, uid_i is pseudo-ID was chosen by authentication server (AS) located in the data center, ID_{APy} is the identity of the APy and ts is the timestamp. Using this signature, the U_i makes one-to-one connection to APy for the access request message. After that, U_i computes the shared symmetric key as (4)

$$K_{i-y} = \hat{e}(kH_1(uid_i), H_1(ID_{APy})) \tag{4}$$

Secondly, APy verifies the timestamp and check the signature S_i. If they are valid APy computes value as (5), sets the authentication code and sends all details (uid_i, ID_{APy}, Auth) to U_i.

$$K_{y-i} = \hat{e}(H_1(uid_i), kH_1(ID_{APy})) \tag{5}$$

Thirdly, U_i generates the verification code which ensures the identity of connection. To compare the authorization code sent by APy, verification code is given as (6)

$$Ver = H_2(K_{i-y} \| uid_i \| ID_{APy}) \tag{6}$$

Ui compares ($Ver \stackrel{?}{=} Aut$) and if they are same, U_i creates a secure connection with authentication between the mobile user and AS in data center.

Finally, APy establishes the secure connection to transmit the message with the signature to AS located in mobile data center. Re-authentication as in Pack and Choi [11] which causes the long latency may affect big data security during the handover procedure.

Hash function can be used in this research because it is powerful to handle any size of big data and it produces fixed length output with many properties.

2.4. Privacy for big data in mobile data centers

The big data which we receive from any mobile users needs some privacy controls because staff dealing with this specific big data should be honest and trustable person. Some cases, single big data reaches final storage of mobile data center through many procedures and operations. When more than one staffs deal with specific big data, managing privacy controls is very difficult. In spite of strong privacy controls in all data centers, many confidential data which belong to diplomat organization leak through the unnecessary procedures. In order to implement the strong privacy, attack "Man in the middle" may be reduced or removed using QC and PairHand protocol. Privacy Policies are many:

Shairing data with official identifications
Downloading policies
Canceling procedures of required services

3. Proposed model

Authentication key which is highly desirable to establish the secure link between the mobile user and authentication server as mentioned in Chang and Tsai [12] and Chen et al. [13] can be developed for big data. In this research, we have proposed PairHand authentication protocol which is attractive to mobile applications because it takes only two handshakes. This model ensures that big data security and privacy is valid with KM organized within the mobile data center where authentication server expects quick and efficient authentication. This proposed model shows that the design of mobile data center with the PairHand protocol reduces the computations and increases the efficiency of the handover authentication.

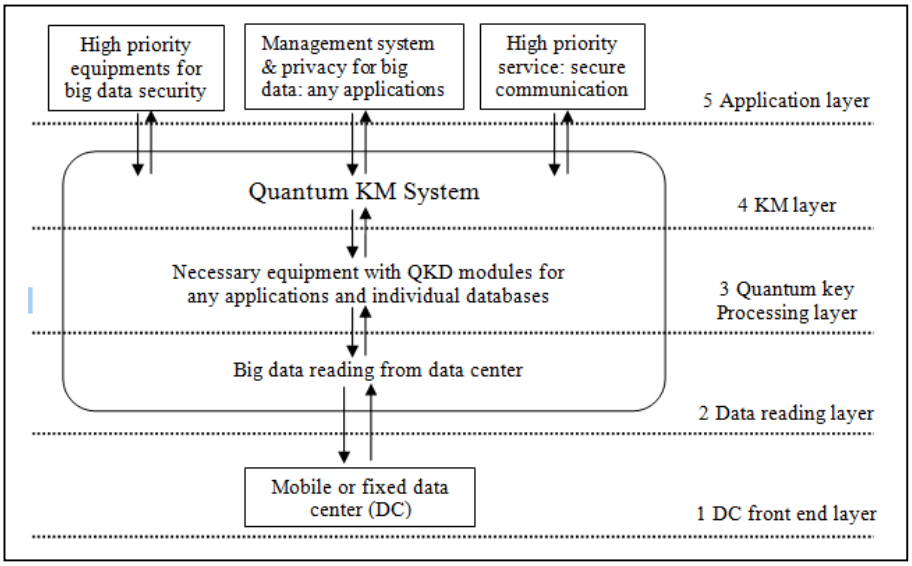

Fig. 1. Theoretical model of the quantum KM system for data center

As shown in the Fig. 2, we have designed the theoretical model which includes many layers, necessary operations for the key management and interfaces. In this model, following layers provide necessary operations which help to manage the big data security issues and privacy problems when big data sent by mobile user is approaching the nearest mobile data center.

Layer 1: Data center front end

We assume that big data transmission takes place between the DC and theoretical model that provides the KM for the big data security. When mobile users send big data contained with TB (10^{12} bytes) to ZB (10^{21} bytes) to any data center, the theoretical model should be able to read the data properly and quickly. This theoretical model read the verifications and identifications of the mobile user and big data using QC and authentication protocols we mentioned in the previous section. The big data such as confidential data and sensitivity are quickly recorded and stored according to the size of the data.

Layer 2: Data reading interface

In this layer, interface between the data center and the mobile users must be a wireless channel where many interferences including security attacks are considered. When big data enter into this theoretical model, many interfaces handle the big data within this model during the KM processing. In each operation of the interface, GA

provides the best performance to minimize the complexity throughout KM processing expected to use in future data cenetrs.

Layer 3: Quantum key processing layer

According to Zeng et al. [14], quantum key processing rely on number of factors which are quantum key distribution (QKD) based on QC, size of the big data and level of the security which depend on the types of the data. Li et al. [15] indicates that DC should be able to take multiple data through the ports which enhance the quantum key processing.

Layer 4: KM layer

According to the size of the big data and traffic problems, KM handles the security key generations which are the main operations in this model designed for mobile data center. Here, KM protocols based on QC are employed.

Layer 5: *Application Layer*

Security issues of big data depend on the applications which big data may be secured according to organization policy that deals with different level of the security and privacy.

4. Results and discussion

In this research, we have proposed QC with PairHand authentication protocol, which is attractive to mobile applications. It seems that big data security and privacy of the mobile data center expect quick and efficient action dynamically when data traffic is high. This proposed model shows that the design of mobile data center with the PairHand protocol reduces the computations and increases the efficiency of the handover authentication.

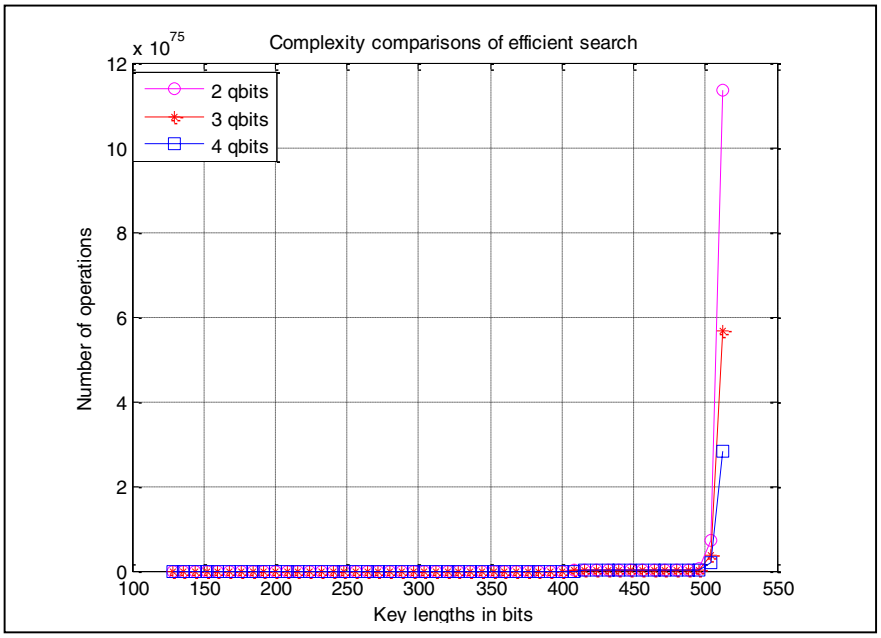

Fig. 2. Complexity of key used in big data security

As shown in Fig. 2, security issues of big data are compared using KM technique which uses the GA, QC and PairHand protocols. Basically, we applied the big data using our theoretical model which has efficient KM processing with all necessary algorithms. In this result, three different qbits are compared for which key sizes of big data are between 128 and 512 bits. When qbits are increased as shown in Fig. 2, not only complexity of searching operations needed for the big data is reduced but also traffic, delay and cost of the data center for making security keys are reduced. When lengthy keys are used for long distance with high speed, data center will be efficient. Further, we can use the light to hide the big data because we can see the light only not the data during the big data transmission.

Table 1 illustrates the GA approach for the KM processing with reasonable data size which may be used for current data centers. Also, it provided details of the original and optimized searching steps data for some selected key lengths. As shown in table I, block cipher for big data can be designed with different values of n, which is representing block of bits used in the block cipher. Here, N and M are a number of searches and number of steps in GA respectively.

Table 1. Details of key lengths and optimized M used in big data security.

Key size (n)	N	Original M	Optimized M
40	1099511627776	341772.6958	341774
48	281474976710656	5468369.3578	5468370
56	72057594037927936	87493915.9503	87493917
64	18446744073709552000	1399902661.4292	1399902662

All types of attacks can be eliminated using appropriate KM which deals with algorithm and protocols mentioned in section 2. As in (7), ciphertexts can be generated for big data handled in mobile data centers where authentication server can be implemented with the theoretical model. In simple attack, specific secret key k is used for breaking the encrypted text.

$$C = E(P, k) \tag{7}$$

In the equation (7), P, E and C are plaintext, encryption and ciphertext respectively. Using GA, secret key can be obtained. Following details provide verification of the QC with GA.

1) Blocks of big data are converted to cipher text with the conditions defined in F.

$$F(k_i) = \begin{cases} 1 & if \quad E(P, k_i) = C \\ 0 & if \quad E(P, k_i) \neq C \end{cases}$$

2) Optimization based on GA depends on QC and size of the key. For instance, if the key length n is 64 bit $O\left(\sqrt{2^{32}}\right)$ steps are enough to solve when F(k) = 1.

5. Conclusions

We have studied about the big data security and privacy using QC, GA and PairHand protocols for mobile data center which deals with TB, EB and ZB data traffic.

Specific case of big data security depends on the number of factors that are the size of the data, traffic, and delay when mobile data centers handle the big data between the authentication server and mobile users. These factors help us to create the novel design which is the theoretical model of efficient KM using QC and GA.

In future, hybrid approach using QC algorithms and PairHand protocol can be developed and implemented to control the both big data security and privacy simultaneously.

Acknowledgements

This paper was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No (23-611-D1432). The authors, therefore, acknowledge with thanks DSR technical and financial support.

References

[1]. Couch N and Robins B, Big Data for Defence and Security, report, Royal United Services Institute (RUSI), 2013; pp. 2 -36

[2]. Goorden S A, Horstmann M, Mosk A P, Škori B, and Pinkse P W H, "Quantum-Secure Authentication Of A Physical Unclonable Key", Optica, Vol. 1, No. 6 / December 2014

[3]. Thayananthan V, Alzahrani A and Qureshi M S. Efficient techniques of key management and quantum cryptography in RFID networks", SECURITY AND COMMUNICATION NETWORKS, USA, 2014 (Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1005)

[4]. Thayananthan V and Alzahrani A. Analysis of Key Management and Quantum Cryptography in Wireless Sensors Networks", *IJCA Special Issue on "Network Security and Cryptograph. (NSC 2011),* International Journal of Computer Applications (IJCA), USA, Dec. 2011; pp. 45-49.

[5]. Lin, S.-H., Chiu, J.-H. and Lee, G.-R. A Fast Iterative Localized Re-authentication Protocol for Heterogeneous Mobile Networks. *IEEE Transaction on Consumer Electronic*, **56**, 2010; 2267-2276. http://dx.doi.org/10.1109/TCE.2010.5681099

[6]. Lin, S.H., Chiu, J.H. and Shen, S.S. Performance Evaluation of the Fast Authentication Schemes in GSMWLAN Heterogeneous Networks. *Journal of Networks*, **5**, 2010; 956-963. http://dx.doi.org/10.4304/jnw.5.8.956-963

[7]. Lin, S.-H., Chiu, J.-H. and Shen, S.-S. The Performance Evaluation of Fast Iterative Localized Re-Authentication for 3G/UMTS-WLAN Interworking Networks. *Journal of Ambient Intelligence and Humanized Computing*, **4**, 2011; 209-221

[8]. He D, Ma M, Zhang Y, Chen C and Bu J. A Strong User Authentication Scheme with Smart Cards for Wireless Communications. Computer Comm., vol. 34, no. 3, 2011; pp. 367-374.

[9]. He D, Jiajun Bu, Sammy Chan and Chun Chen. Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks. IEEE Transactions on Computers, VOL. 62, NO. 3, MARCH 2013.

[10]. Cao, J., Li, H., Ma, M., *et al.* A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks. *Journal Computer Networks*: *The International Journal of Computer and Telecommunications Networking*, **56**, 2012; 2119-2131.

[11]. Pack S and Choi Y. Fast Handoff Scheme Based on Mobility Prediction in Public Wireless LAN Systems. Proc. IEE Comm., vol. 151, no. 5, Oct. 2004; pp. 489-495.

[12]. Chang C C and Tsai H C. An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks. IEEE Trans. Wireless Comm., vol. 9, no. 11, Nov. 2010; pp. 3346-3353.

[13]. Chen C, He D, Chan S, Bu J, Gao Y and Fan R. Lightweight and Provably Secure User Authentication with Anonymity for the Global Mobility Network. Int'l J. Comm. Systems, vol. 24, no. 3, 2011; pp. 347-362.

[14]. Zeng K, Govindan K, and Mohapatra P. Non-Cryptographic Authentication and Identification in Wireless Networks. IEEE Wireless Comm., vol. 17, no. 5, Oct. 2010; pp. 56-62.

[15]. Li D, Guo C, Wu H, et al. "Scalable and Cost-effective Interconnection of Data-center Servers using Dual Server Ports", *IEEE/ACM Transactions on Networking*, 19(1): 2011; 102-114.