IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Cryptographic Methods to Securing Big-Data Analytics in Cloud using Parallel Computing

Adi Maheswara Reddy G[1], Dr K Venkata Rao[2], Dr JVR Murthy[3]

Research Scholar, Department of CSE, JNTUK, Kakinada, AP, India[1]

Department of CSE, Vignan Institute of Information Technology, Visakhapatnam, AP, India[2]

Department of CSE, JNTUK College of Engineering, Kakinada, AP, India[3]

Abstract: Evaluating the efficacy of several methods. Key managing predominantly uses up the power of battery in two ways: one way using the algorithm computations accomplished by the core processor and the other way is the extra communications energy expanded to communicate and to collect information related to key management. From the time when the quantity of energy utilized by various processors and the systems involved for the communications differs extensively, providing privacy and security in data centres for mobile is very challengeable as we need effective security for the managing the keys. Here we have analysed numerous standard parallel programming techniques to effectively use the processors and do the jobs in parallel with less time complexity.

Keywords: Security, Big Data, Cloud, Parallel Programming.

I. INTRODUCTION

Big-data handling in these days should be effective as today's world is data-centric and analytics have become critical to most enterprise and government applications. Thus, there is a need for an appropriate big data infrastructure that supports storage and processing on a huge scale.
Considering the cost, wider access of network, resistance, pooling of assets and measured check, due to this the cloud computing is the optimal for the big data handling and analytics [1].

Key Management afford essential provision to big data issues related to security because generating key dynamically for the today's world big data will be ineffective when we design solutions using existing cryptographic methodologies, In the environment of mobiles, users of mobile and data centres can be anyplace in the land, space. This is similar to a network which is wireless sensor in nature and which requires specific key handling mechanisms to take care at the data and secure the channel used for the data transmission between the nodes. Thayananthan and Alzahrani [2] mentioned that key management in wireless sensor network can be used in this research.
Protocols related to security and other issues related to privacy based on authentication protocols use only operations in bitwise but bitwise actions not suites the big data. In this investigation, quantum bits (qbits) operations appear that mobile data centers get big data security and privacy rapidly and proficiently. When many verification and re-verification 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 [13] using the parallel computing.

II. RELATED WORK AND USEFUL BACKGROUND

For large organizations one of the expected solutions is the security and the confidentiality of big data. Where they can create the extreme security organized by the data centre which can be mobile or fixed. Quantum cryptography (QC) delivers not only the extreme security for the big data which will have interactions among the users and the data centres but also it minimizes the key lookup actions which are part of issues related to security controlled in the key handling of the data centre. Few protocols are easy to implement when applications use different designs which are not only hang on the size of data but also traffic for the data.
According to Thayananthan et al. [3], Quantum Cryptography (QC) is well-thought-out with Grover's algorithm (GA), which has simple and rapid process to enhance the searching actions in the key management (KM).

A. Big data Security with Quantum cryptography

In this investigation, quantum cryptography delivers extreme security with less complexity that increases the storage capacity and security strength of the big data. Here, we need to use the symmetric key with a block cipher which is proper to control the big data security because it is very simple to architecture the block cipher for big data. GA

DOI10.17148/IJARCCE.2017.6857

delivers effective key lookup is one of the best available QC methods in the techniques related to security of big data. This algorithm provides protected interactions between the users of mobile and the authentication server (AS).

B. Mobile data centre- Handover authentication

According to Lin at el. [4-6], to explore the wireless privacy and security for mobile channels, in wireless application authentication is studied; users in mobile data centres should be capable of sending the big data to the mobile data centre from any of the location. In this study, we explored the protocol which provisions to handle the issues related to the privacy and security in mobile data centres which is called as PairHand authentication.

C. PairHand authentication protocol

Authentication for Handover actions uses several different procedures which will use handshakes more than two and increase [13] the overall calculations as in He et al. [7-8], in this study, procedure used for handover authentication is mentioned in Cao et al. [9] is also investigated to architect the abstract prototype. There are four methods available in PairHand protocol which is suitable for mobile networks and communications. They are batch authentication, system initiation, Dos attack and handover authentication. It uses two handshakes between the mobile data and users for the authentication operations.

D. Mobile data centres – big data privacy

From any users of mobile when big data is received then users require privacy controls for the staff operating with this data which is big in size should be authentic as well as trustable individual. In few cases, the big data reach the storing of data centre for mobile using many methods and operations. For Specific big data when more than single staff dealing handling privacy is tough. Controlling privacy in all the centres of data, secure data belongs to organization may outflow with the redundant methods. So for implementing the privacy, “Man in the middle” attack may be reduced by implementing PairHand and QC procedures.

E. Why Parallel Processing

Traditional computers are not able to meet high-performance
Requirements for many applications:

- Simulation of large complex systems in physics, economy, biology...
- Distributed data base with search function.
- Computer-aided design.
- Visualization and multimedia.
- Multi-tasking and multi-user systems (e.g., super computers).

Such applications are categorized by a very huge volume of Mathematical calculations and/or a high number of input data. In order to provide enough performance for such applications, we can have many processors in a single computer.

III.PROPOSED MODEL

To create the secure connection between authentication server and mobile user for big data the authentication key needs to be extremely necessary and can be developed as stated in Tsai and Chang [10] and Chen et al. [11] . In this study, we have proposed we can use PairHand as the authentication protocol because it is very optimal for the mobile applications because the handshakes used by this are only two. This approach guarantees that the security for big data and the privacy are effective with Key Management effectively organized with in the data centres of mobile because authentication server anticipates very fast and effective authentication and it will be more effective with incorporating the parallel computing capabilities here. The model proposed here indicates that the design of PairHand protocol and the data centres for mobile decreases the calculations and increases the effectiveness of the authentication for handover

A. Amdahl Law

As per Amdahl Law, even we use ideal system which is parallel; it is difficult to get the speedup rate equivalent with the processors number as for each of the programs, with respect to executing time can have a portion α which cannot be run using concept of parallelism and that portion should be run consecutively using single processor. And the remaining portion of (1 - α) can be run in parallel.
In these scenarios the speedup and the parallel execution times can be calculated:

$$T_p = T_s \cdot \alpha + T_s \cdot (1-\alpha)/p$$

$$S = \frac{T_s}{T_p} = \frac{T_s}{T_s \cdot \alpha + T_s \cdot (1-\alpha)/p} = \frac{1}{\alpha + (1-\alpha)/p} = \frac{p}{\alpha \cdot (p-1)+1}$$

DOI10.17148/IJARCCE.2017.6857

Here if p ∞, then the speedup become:

$$\lim_{p\to\infty} S = \frac{1}{\alpha}$$

B. Computations involved in Authentication Protocol and PairHand

For user of mobile U_i used for computing the S_i as signature as (1), where k is private key and H1 and H2 are hash functions.

$$S_i = kH1\ (ui\ d_i)\ H2(U_i) \qquad (1)$$

Here U_i is equal to ui d_i || IDAPy ||ts

Where (ui d_i) considered to be Pseudo-ID for AS (authentication server) used for the data centres ts represents the timestamp IDAPy represents the identity of the APy

$$Ki\text{-}y = \hat{e}(H1(IDAPy\ ),kH1(uidi\ )) \qquad (2)$$

$$Ky\text{-}i = \hat{e}\ (kH1(IDAPy\ ),H1(uidi\ )) \qquad (3)$$

$$Ver = H2\ (uidi\ \ \|\ Ki\text{-}y\ \|IDAPy\ ) \qquad (4)$$

The above (1), (2), (3) and (4) can used to Signature computation (1), symmetric key computation (2), securely sending all the details and the authentication key (3) and finally certification of identify of the connection (4) respectively.

C. Parallel Computing

In the above step there many computations in each step (1), (2), (3) and (4). So for each for big data applications the computations are sequential and we can make them independent computations as parallel and we can gain lot of performance gain as the requests coming for the big data applications will be very huge.

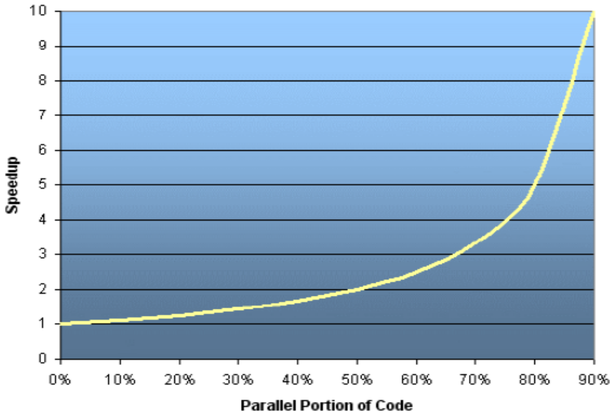

Fig. 1 The Graph represents the performance gain obtain as per Amdahl Law – Speed vs Parallel Portion of Code

As per the Gustafson's, the represent of the speed up is as follows:

$$Speedup\ (N) = S + N\ (1\text{-}S)$$

Here "N" represents the number of processor cores used "S" represents the Serial percentage of unscaled workload expressed as a decimal in the range of 0 to 1.

TABLE I

# cores	Computation	Speedup	Efficiency (speedup / # cores)
2	0.1 + 2 (1 -0 .1)	1.9x	95.00%
4	0.1 + 4 (1 -0 .1)	3.7x	92.50%
32	0.1 + 32 (1 -0 .1)	28.9x	90.31%
1024	0.1 + 1024 (1 -0 .1)	921.7x	90.01%

The above table represents how the performance result is scaled up when more processors are used along with the parallel computation when we use Gustafson's represent of speedup.

IV. CONCLUSIONS

In this investigation we have explored about the PairHand, GA and Quantum Cryptography protocols for mobile data center for big data privacy and security which deals data movement with ZB, EB and TB with efficient usage of parallel computation for key management. Particular case of security for the big data hangs on delay, traffic and the data size when data centers handles mobile users and authentication for big data. For the abstract model of innovative design the GA, QC, KM and parallel computing help us.

In future, using the PairHand protocol, QC procedures and parallel computing, hybrid methods can be designed and executed for the privacy and security of big data.

REFERENCES

[1] P. Mell and T. Grace, “The NIST definition of cloud computing,” NIST Special Publication 800-145, 2011.

[2] 2. 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.

[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] 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

[5] 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

[6] 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

[7] 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.

[8] 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

[9] 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.

[10] 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.

[11] 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

[12] Juby Mathew, Dr.R Vijayakumar,The Performance of Parallel Algorithms by Amdahl's Law, Gustafson's Trend, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2796-2799

[13] Thayananthan, Vijey, and Aiiad Albeshri. "Big Data Security Issues Based on Quantum Cryptography and Privacy with Authentication for Mobile Data Center", Procedia Computer Science 50, (2015) 149 – 156