Token Based Authentication & Data Encryption Approach for Micro Data Center Architecture

Vijender Kumar
University Institute Engineering and Technology, India.

Naresh Kumar
University Institute Engineering and Technology, India.

Abstract – Mobile cloud computing is composed of two things: mobile computing and cloud computing which provides space to the mobile user to offload heavy task on the cloud which can help performing mobile device operations in the cloud. By using MCC mobile user loses its physical control. So it needs security, there is already a lot of security concern but no protocol has been found for the micro data center architecture. The micro data center is resource rich which is connected to the internet and easily available for nearby devices. In this paper, we propose an authentication protocol for a micro data center architecture, our authentication protocol protects the data from any unauthorized user and secure it. Basically, two approaches are used in the whole process one of them is data encryption approach and another one is token based authentication approach.

Index Terms – mobile Cloud computing, micro data center, Distributed denial of services.

1. INTRODUCTION

The mobile computing makes it possible to "access information anytime, anywhere" in another words Accessing information at any time and any place, [1] In recent years, mobile applications have seamlessly integrated with real-time data and web applications, This results in the growth of application in various categories such as entertainment, health , games, business, social networking, travel and news. To avail these devices have limited resources like battery life, storage capacity and processing power as compare to fixed devices. Cloud computing provides solution to these problems by offering on-demand, scalable and reliable services to the mobile users which leads to the development of the mobile cloud computing (MCC). Cloud computing Gardens blog on 5 March 2010 record [2] as "the availability of cloud computing services in a mobile environment. In recent years, applications developed for mobile devices have become plentiful including applications of various types such as fitness, news, amusement, commercial, Social networking Cloud computing allows devices to avoid these constraints by letting more resource intensive tasks be performed on systems without these constraints and having the results sent to the device. Thus, cloud computing for mobile devices is a highly appealing and potentially lucrative trend. [3]

2. RELATED WORK

L. Guan et al. [7] provides survey of recent research accomplishments in the MCC. They also give the detail of application partiioning, technology, offloading and context – aware services in the mobile cloud computing paradigm

Lee et al. [8] proposed authentication scheme for cloud computing based on the public key infrastructure (PKI). However, the credentials such as PW, ID, and PKI are transmitted without encryption which can be easily interrupted by the malicious users. Moreover, the given scheme does not consider data integrity, confidentiality and users cannot change their password therefor, this scheme does not fit into the real-time cloud computing environment. Chow et al. [9] proposed an authentication framework known as implicit authentication. The proposed scheme is flexible enough to provision different, cloud-oriented authentication methods. In this given scheme, the mobile user has to perform hashing of frequently produced information. This frequent hash functions on client side result in energy loss and communication delay

Yoo et al. [10] The proposed scheme is energy efficient and is used for performing multi-user authentication in the cloud computing environment. In the proposed scheme, the concept of one-time password (OTP) is used to securely perform the authentication process. However, the seed is sent without encryption from the authentication server to the user.

M.Felemban et al. [15] proposed a micro data center architecture which is resource rich and well connected to the internet. Mobile user not able to perform a difficult task on the mobile processor because some program used the huge memory and ram that's why the user is bound to use cloud services which are resource-rich and give result fast.

3. ISSUES AND CHALLENGES

M.Felemabn et al. proposed a micro data center architecture which is placed the edge of the internet because of well connected to the internet. mobile user uses it for computational work because of the mobile user not able to process this programs due to lack of memory and ram

problem[15]. micro data center lies between cloud and mobile user so security is important in this case and a lot of attacks occurs:

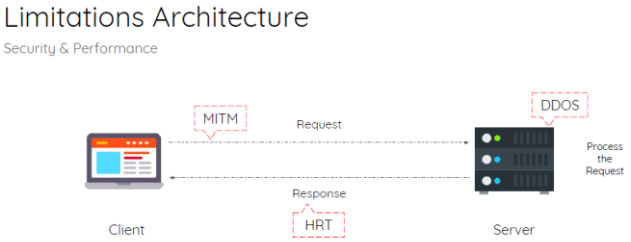

Figure 1 Traditional Architecture

i. MITM attacks: Intruder lies between the mobile user and the micro data center. Intruder easily intercepts the messages because messages are not encrypted

ii. Non-repudiation attacks: owner can't deny what owner said. There is no way taking it back

iii. Phishing attacks: Intruder can act as an authorized user and can gain access to the cloud resources and services.

iv. Credential security: data user credentials such as user id and password or email id are stored in the micro data center and malicious user gain access data owner credential are to be at risk.

v. Password security: password is sent to the micro data center which is not secure

4. TOKEN BASED AUTHENTICATION APPROACH

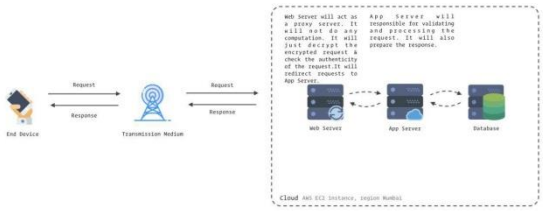

Figure 2 Token Based Authentication Approach

In this proposed approach to communicating with web server registration is a must. After registering a token is generated. The token is used for communication between mobile device and web server. Steps of token based authentication approach:

1. The client generates a request to the web server
2. The web server will receive the request and send the public key in the response.
3. The client will encrypt the request with received public key and resend to the web server.
4. The web server will authenticate the request if authentication results in success go to 5 else go to 1.
5. The web server will pass the request to the application server
6. The application server will store the information (username and password etc.) and generate a token.
7. The application server will process the request and ready the response which includes the generated token.
8. The application server sends the response back to the web server.
9. The web server will send the response (token) back to the client.

The client will save this token in local storage and use this for future transmission.

5. DATA ENCRYPTION APPROACH

In this proposed approach client is used PKE to encrypt the username and password and then sends to the web server. Web server verifies the client through token and after this process client easily communicates with the application server. Steps of data encryption approach

Figure 3 Data Encryption Approach

1. Client generate are request to the web server
2. The web server will receive the request and send the public key in the response.
3. The client will encrypt the request with the received public key and resend to the web server.
4. The web server will authenticate the request; if authentication results in success go to 5 else go to 1.
5. The web server will pass that request to the application server.
6. The application server will validate the token if valid then go to 7 else reject.

7. The application server will process the request and ready the response.
8. The application server sends the response back to the web server.
9. The web server will send the response back to the client.

6. NEW DESIGNED ARCHITECTURE

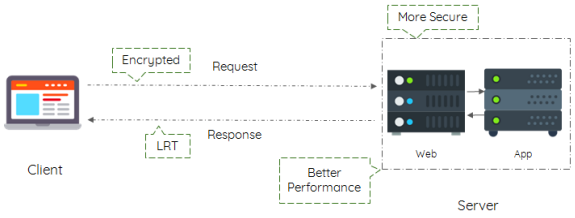

Figure 4 New Designed Architecture

Proposed architecture is different from traditional architecture because it has app server is used which is taking filter users information from web server and according to request send response to the client and work is divided between them that's why low response time is used and security is also there.

7. PROGRAMMING LANGUAGE USED

JSON Web Token is a way for securely transmitting information between two devices over a network as a JSON object. This information can be authenticated because it is digitally signed. JWTs can be signed using HMAC or RSA algorithm

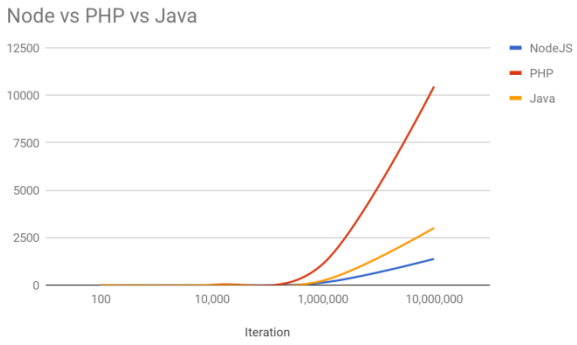

Figure 5 Comparison Nodes, PHP, JAVA

8. CONCLUSION

In this paper, we discuss the lot of work about mobile cloud computing which offloads the heavy task on the cloud and performs computational work and gives the results to the mobile user. But it used to cost more time and money and battery usage. Hence, the micro data centre is vital to deal with this problem. mDC presents all the time of the corner of the internet for a good connectivity and mobile user. Token based authentication approach and data encryption approach is used to secure credential and safe from different type of attack which is occur during communication with the web server and app server low response time is given by proposed architecture.

REFERENCES

[1]. N. Mimura Gonzalez, M. Torrez Rojas, M. Maciel da Silva, F. Redigolo, T. Melo de Brito Carvalho, C. Miers, M. Naslund, and A. Ahmed, "A framework for authentication and authorization credentials in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 509–516, July 2013.

[2]. R. Banyal, P. Jain, and V. Jain, "Multi-factor authentication framework for cloud computing," in Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on, pp. 105–110, Sept 2013.

[3]. R. Lomotey and R. Deters, "Saas authentication middleware for mobile consumers of iaas cloud," in Services (SERVICES), 2013 IEEE Ninth World Congress on, pp. 448–455, June 2013.

[4]. H. Kim and S. Timm, "X.509 authentication and authorization in fermi cloud," in Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, pp. 732–737, Dec 2014.

[5]. B. Tang, R. Sandhu, and Q. Li, "Multi-tenancy authorization models for collaborative cloud services," in Collaboration Technologies and Systems (CTS), 2013 International Conference on, pp. 132–138, May 2013.

[6]. L. Zhou, V. Varadharajan, and M. Hitchens, "Integrating trust with cryptographic role-based access control for secure cloud data storage," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 560–569, July 2013.

[7]. J. Sendor, Y. Lehmann, G. Serme, and A. Santana de Oliveira, "Platform level support for authorization in cloud services with oauth 2," in Proceedings of the 2014 IEEE International Conference on Cloud Engineering, IC2E '14, (Washington, DC, USA), pp. 458–465, IEEE Computer Society, 2014.

[8]. S. Ahmed and A. Abdullah, "E-healthcare and data management services in a cloud," 8th International Conference on High-capacity Optical Networks and Emerging Technologies, pp. 248–252, 2011.

[9]. V. G.r and A. R. M. Reddy, "An Efficient Security Model in Cloud Computing based on Soft computing Techniques," International Journal of Computer Applications, vol. 60, no. 14, pp. 18–23, 2012.

[10]. K. Mali and S. Bhattacharya, "Soft Computing on Medical-Data (SCOM) for a Countrywide Medical System using Data Mining and Cloud Computing Features ," Global Journal of Computer Science and Technology Cloud and Distributed , vol. 13, no. 3, pp. 6–13, 2013.

[11]. H. V. Tran, "Data Management Challenges in Cloud Computing," 2013 13th International Conference on Computational Science and Its Applications, pp. 19–27, 2013.

[12]. W. Zhao, Z. Ye, M. Wang, L. Ma, and W. Liu, "An image threholding approach based on cuckoo search algorithm and 2D maximum entropy," 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 1, pp. 303–308, 2015

[13]. E. B. George, G. J. Rosline, and D. G. Rajesh, "Brain tumor segmentation using Cuckoo Search optimization for Magnetic Resonance Images," 2015 IEEE 8th GCC Conference & Exhibition, pp. 1–6, 2015.

[14]. R. Banyal, V. Jain, and P. Jain, "Data Management System to Improve Security and Availability in Cloud Storage," 2015 International Conference on Computational Intelligence and Networks, pp. 124–129, 2015.

[15]. N. Ambika and M. Sujaritha , "A Survey on Data Security and Integrity in Cloud Computing ," International Journal of Advanced Research in Computer Science , vol. 7, no. 4, pp. 57–63, 2016.

[16]. W.-F. Hsien, C.-C. Yang, and M.-S. Hwang, "A Survey of Public Auditing for Secure Data Storage in Cloud Computing," International Journal of Network Security, vol. 18, no. 1, pp. 133–142, 2016.
[17]. M. Mishra and U. Bellur, "De-Fragmenting the Cloud," 2016 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 511–520, 2016.
[18]. N. Islam and S. Xaviers , "Region Based Image Segmentation using Cuckoo Search Algorithm," Journal of Chemical and Pharmaceutical Sciences , vol. 9, no. 2, pp. 884–888, 2016.
[19]. V. Dubey and P. Agrawal, "Cloud computing and data management," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), pp. 1–6, 2016.
[20]. M. Akbari and H. Rashidi, "A multi-objectives scheduling algorithm based on cuckoo optimization for task allocation problem at compile time in heterogeneous systems," Expert Systems with Applications, vol. 60, pp. 234–248, 2016.
[21]. A.Alsirhani, P. Bodorik, and S. Sampalli, "Improving Database Security in Cloud Computing by Fragmentation of Data," 2017 International Conference on Computer and Applications (ICCA), pp. 43–49, 2017.
[22]. A.Chandran and C. K. Shyamala, "Data management issues in cloud integrated computing: A big picture," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1–8, 2017.
[23]. A.Esposito, A. Castiglione, C.-A. Tudorica, and F. Pop, "Security and privacy for cloud-based data management in the health network service chain: a microservice approach," IEEE Communications Magazine, vol. 55, no. 9, pp. 102–108, 2017.
[24]. K. Kapusta, G. Memmi, and H. Noura , "An Efficient Keyless Fragmentation Algorithm for Data Protection," Cornell University Library, 2017.
[25]. "Cloud Computing," Computer Communications and Networks, pp. 1–353, 2017.