Securing the Cloud

D. Asir Antony Gnana Singh
Department of Computer Science and Engineering,
Anna University, BIT Campus, Tiruchirappalli, India
asirantony@gmail.com

R. Priyadharshini
Department of Computer Science and Engineering,
Anna University, BIT Campus, Tiruchirappalli, India
dharshinipriya245@gmail.com

E. Jebamalar Leavline
Department of Electronics and Communication Engineering,
Anna University, BIT Campus, Tiruchirappalli, India
jebilee@gmail.com

Abstract—**Data acquisition increases tremendously through various data acquisition devices from various sectors in the recent past. Hence, larger storage and computing units are necessary to store and process these data to take data-driven decisions. Therefore, cloud environment is employed to store and process these data to make data-driven decision. The cloud can be categorized into three types such as public, private and hybrid cloud based on the data being stored and computed. Public cloud contains the public data and services rendered to the public based on their own demand. Private cloud contains private data concerned to an individual organization or a company and such data can be processed for the individual organization. The hybrid cloud combines the characteristics of both public and private cloud. Securing the cloud is a challenging task. Hence, many researchers conducted their research with the focuses on securing the cloud. This paper presents study on various measures reported by the researchers for securing the cloud**

Keywords-cloud computing; private cloud; cipher text policy; security in private cloud;

I. Introduction

The cloud consists of set of sharable and configurable computing resources. These resources are provisioned by the cloud service provides (CSP) based on the requirement of the users and that are accessed by the users through internet in on-demand basis. The cloud environment provides infrastructures and services to store, share, and compute the data. The cloud services include infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), and development-as-a-service (DaaS). In IaaS, infrastructures or hardware entities such as servers, networks, storage units, etc. are rented by the individual, organization, or an institution to store and carryout the computations through internet. In PaaS, the platforms such as operating system, application development frameworks, etc. are rented by the cloud. The developer can develop their application and run their application using the platform such as particular development framework or operating system. In SaaS, the application software is provided to the users that are run in the cloud environment through internet. In DaaS, the cloud provides the development tools to the user to develop application such as web applications, mobile application, etc. Thus, the cloud provides various services. The cloud is classified into three types such as public, private and hybrid cloud based on the data being stored and computed. The public cloud contains the public data and services rendered to the public based on their own demand. The private cloud contains the private data concerned to an individual organization or the company and the data can be processed for the individual organization. The hybrid cloud combines the characteristics of both public and private cloud.

Securing the cloud is a challenging task. Moreover, the cloud environment consists of data communication elements, data storage elements, computing elements, and policy making for resources sharing. Hence, the cloud security can be classified into four categories such as security in data communication, security in data storage, security in computing, and security in resource sharing policy making. This paper comprehends various aspects of security mechanisms adopted in the cloud environment. The following section presents a detailed review of security issues and mechanisms in cloud environment and Section 3 presents the conclusion.

II. Cloud Security

This section presents the security issues in the cloud computing. Figure 1 shows the participation of a cloud user in cloud computing. In general, the cloud environment consists of data centers that contain many virtual machines that are run to serve the client's request. The cloud environment is designed based on the services that are provided to the cloud user. Hence, the cloud environment contains platforms, infrastructure or application in order to provide the services that are discussed in Section 1. The cloud environment is connected with the internet through the network. Hence, the network needs to be protected for the seamless services that are carried out through the network. Therefore, the network security is of major concern to ensure cloud security.

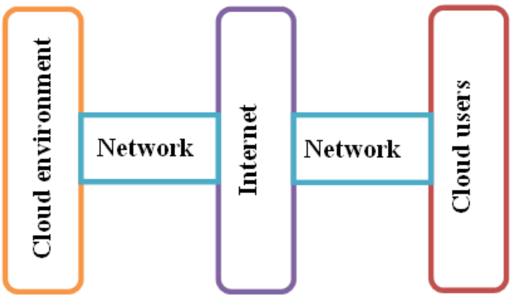

Figure 1. Schematic view of user participation in cloud computing

A. *Network and Data Storage Security for Cloud*

The network plays a significant role in providing the cloud services to the cloud users. The network connects the cloud environment with the internet and connects the internet with the end cloud user to access the service from the cloud. The data is moved around the network to render cloud services. Moreover, the data are stored in the databases at the data centers to render the cloud services to the cloud users. Hence, it is essential to secure the network and data to secure the cloud. Securing the network and the data storage can be performed by the security mechanisms and techniques such as cryptography, firewall, intrusion detection system, etc. Furthermore, many researchers conducted the research on improving the security in networks and communication systems for cloud services.

Z. Chen presented a network security scheme for the data center that is rented to many users [1]. J. Ullrich et al. conducted a survey on the secret communication in the cloud [2]. T. Wang discussed the data center networking in different aspects [3]. H. Yao et al. presented a scheme to prevent information leakage in the cloud [4]. Q. Yan conducted a survey of issues and challenges in addressing the denial of services attack in cloud environment [5]. M. Zhang presented a metric to prevent the zero-day attacks [6]. S. Han et al. presented a privacy preserving scheme for the cloud-assisted wireless body area networks (WBANs) [7].

B. *Cryptography*

Cryptography is a type of security mechanism that converts the data into cipher data or coded data to avoid intrusion. The cipher or coded data cannot be understood by the intruders. The encryption and decryption are the two major processes of the cryptography. The encryption is a process that coverts the plain data or original data into the cipher data or coded data. Decryption is the process that converts the cipher data into the plain data. Many researchers conducted research on cryptography to provide security in cloud. Moreover, W. Pan et al. presented a cryptography scheme to secure the data transmission [8]. The cloud computing is carried out for various applications such as medical, education, engineering, commercial, mobile application, etc. Therefore, many researches focuses on improving the cryptography mechanism for different applications in cloud computing. H. Huang designed a framework of health care system with an encryption scheme to ensure the privacy in data transmission [9]. J. J. Hwang presented a cryptography technique for the business model that is employed in cloud computing to provide secured services [10]. Somani, U et al. presented a digital signature with Ron Rivest, Adi Shamir and Leonard Adleman (RSA) algorithm for data security [11]. Tysowski also presented a cryptography-based security mechanism to provide security in mobile application in cloud computing [12].

C. *Firewall*

Firewall is a security system that restricts the unwanted incoming/outgoing packets or data based on the predefined rules that are set by the network administrators pertaining to the organizational policy. Several research works attempted to improving the performance of the firewall for cloud computing. G. Liyanage et al. presented a firewall model to improve the security in cloud computing [13]. Z. Yang presented a firewall to enhance the security in the cloud environment [14].

D. Intrusion Detection System

Intrusion detection system (IDS) is one of the network security mechanisms that are used to secure the cloud. The intrusion detection system receives the data packets that are passed through it and detects the data packets whether the data packet comes from the intruders or not. If the data packet comes from the intruders, it intimates the network administrator to take preventive measures. The intrusion detection system is classified into two types based on the location where the IDS is placed namely host-based IDS and network-based IDS. The host-based IDS is placed in the host that is available in the data center. The network-based IDS placed in the network. On the other hand, the IDS is classified into two based on the working principle namely signature-based and anomaly-based IDS. The signature-based IDS has the matching algorithm that matches the data packet with the existing stored signatures or rules, if any deviation found on the data packet, that is identified as intruder packet. Moreover, the signature-based intrusion detection system has high accuracy rate in detecting the data packets, but it fails to detect the data packets when their signatures are not present in the stored database. The anomaly-based intrusion IDS detects the data packets that are unknown, but the false positive rate is high. Hence, many researches focus on IDS to improve their performance to provide cloud security. K. Salah conducted an analysis on cloud security on the overlay network that provides some securities such as intrusion detection system, antivirus system, etc. [15]. Massimo Ficco et al. presented the intrusion detection system for the cloud security [16]. Vieira. K et al. presented an intrusion detection system to secure cloud computing [17].

E. Security the Data Storage

The data in the cloud is placed in host systems that are present in the cloud data centers [18]. The stored data need to be secured; hence many researchers conducted the research on securing the data storage. Wang Q presented scheme to secure the data storage in cloud [19]. Kaufman et al. presented the concepts of the data security in cloud computing [20]. Deyan Chen et al. presented an analysis on the issues in data security in cloud and their solutions [21]. Cong Wang and Kui Ren discussed the concepts of the secured cloud data storage services [22]. Kan Yang presented auditing protocol and privacy preserving auditing protocol for securing the data storage in cloud computing [23]. Wassim Itani et al. explored privacy-as-a-service (PaaS) to provide security in data storage [24]. Feng, D.G et al. presented the framework for securing cloud computing [25]. Moreover, some researchers use the cryptographic techniques [26] for securing the data storage. Seny Kamara et al. presented a study on cryptography technologies available for the cloud data storage [27].

III. Conclusion

The cloud environment consists of a set of sharable and configurable computing resources. These resources are provisioned by the cloud service provides (CSP) based on the requirement of the users and they are accessed by the users through internet in an on-demand basis. The cloud provides infrastructures and the services to store, share, and compute the data. The cloud services include infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), and development-as-a-service (DaaS), etc. This paper presented a study on the security in the cloud computing. Moreover, the literatures on security in cloud computing are reviewed. The cloud security can be achieved using various security mechanisms and techniques such as cryptography, firewall, and intrusion detection system.

References

[1] Z. Chen, W. Dong, H. Li, P. Zhang, X. Chen and J. Cao, "Collaborative network security in multi-tenant data center for cloud computing," in Tsinghua Science and Technology, vol. 19, no. 1, pp. 82-94, Feb. 2014.

[2] J. Ullrich, T. Zseby, J. Fabini and E. Weippl, "Network-Based Secret Communication in Clouds: A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1112-1144, Second quarter 2017.

[3] T. Wang, Z. Su, Y. Xia and M. Hamdi, "Rethinking the Data Center Networking: Architecture, Network Protocols, and Resource Sharing," in IEEE Access, vol. 2, no. , pp. 1481-1496, 2014.

[4] H. Yao, N. Xing, J. Zhou and Z. Xia, "Secure Index for Resource-Constraint Mobile Devices in Cloud Computing," in IEEE Access, vol. 4, no. , pp. 9119-9128, 2016.

[5] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602-622, 2016.

[6] M. Zhang, L. Wang, S. Jajodia, A. Singhal and M. Albanese, "Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero-Day Attacks," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 1071-1086, May 2016.

[7] S. Han, S. Zhao, Q. Li, C. H. Ju and W. Zhou, "PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation With Fault Tolerance," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1940-1955, Sept. 2016.

[8] W. Pan, F. Zheng, Y. Zhao, W. T. Zhu and J. Jing, "An Efficient Elliptic Curve Cryptography Signature Server With GPU Acceleration," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 111-122, Jan. 2017.

[9] H. Huang, T. Gong, N. Ye, R. Wang and Y. Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System," in IEEE Transactions on Industrial Informatics, vol. 13, no. 3, pp. 1227-1237, June 2017.

[10] J. J. Hwang, H. K. Chuang, Y. C. Hsu and C. H. Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," 2011 International Conference on Information Science and Applications, Jeju Island, 2011, pp. 1-7.

[11] Somani, U., Lakhani, K. and Mundra, M., 2010, October. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on (pp. 211-216). IEEE.

[12] Tysowski, Piotr K., and M. Anwarul Hasan. "Hybrid attribute-and re-encryption-based key management for secure and scalable mobile applications in clouds." IEEE Transactions on Cloud Computing 1.2 (2013): 172-186.

[13] G. Liyanage and S. Fernando, "Firewall model for cloud computing," 2013 IEEE 8th International Conference on Industrial and Information Systems, Peradeniya, 2013, pp. 86-91.

[14] Z. Yang, L. Qiao, C. Liu, C. Yang and G. Wan, "A collaborative trust model of firewall-through based on Cloud Computing," The 2010 14th International Conference on Computer Supported Cooperative Work in Design, Shanghai, China, 2010, pp. 329-334.

[15] K. Salah, J. M. Alcaraz Calero, S. Zeadally, S. Al-Mulla and M. Alzaabi, "Using Cloud Computing to Implement a Security Overlay Network," in IEEE Security & Privacy, vol. 11, no. 1, pp. 44-53, Jan.-Feb. 2013

[16] Ficco, M., Tasquier, L. and Aversa, R., 2013, October. Intrusion detection in cloud computing. In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on (pp. 276-283). IEEE.

[17] Vieira, K., Schulter, A., Westphall, C. and Westphall, C., 2010. Intrusion detection techniques in grid and cloud computing environment. IT Professional, IEEE Computer Society, 12(4), pp.38-43.

[18] D. Asir Antony Gnana Singh, B. Tamizhpoonguil,E. Jebamalar Leavline, "A Survey on Big Data and Cloud Computing", International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 4, no. 7, pp. 273 -277, July 2016.

[19] Wang, Q., Wang, C., Li, J., Ren, K. and Lou, W., 2009, September. Enabling public verifiability and data dynamics for storage security in cloud computing. In European symposium on research in computer security (pp. 355-370). Springer Berlin Heidelberg.

[20] Kaufman, Lori M. "Data security in the world of cloud computing." IEEE Security & Privacy 7, no. 4 (2009).

[21] Chen, D. and Zhao, H., 2012, March. Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647-651). IEEE.

[22] Wang, C., Ren, K., Lou, W. and Li, J., 2010. Toward publicly auditable secure cloud data storage services. IEEE network, 24(4).

[23] Yang, Kan, and Xiaohua Jia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing." IEEE transactions on parallel and distributed systems 24.9 (2013): 1717-1726.

[24] Itani, W., Kayssi, A. and Chehab, A., 2009, December. Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures. In Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on (pp. 711-716). IEEE.

[25] Feng, D.G., Zhang, M., Zhang, Y. and Xu, Z., 2011. Study on cloud computing security. Journal of software, 22(1), pp.71-83.

[26] D. Asir Antontony Gnana Singh, R.Priyadharshini,"Performance Analysis of Data Encryption Algorithms for Secure Data Transmission", International Journal for Science and Advance Research In Technology,Vol.2, no. 12, December 2016.

[27] Kamara, S. and Lauter, K., 2010, January. Cryptographic cloud storage. In International Conference on Financial Cryptography and Data Security (pp. 136-149). Springer Berlin Heidelberg.