ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

Survey on Recent Research in Cyber Security in Cloud

Jaitee A. Bankar[1], Aishwarya S. Chavan [2]

Assistant Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, Pune, India[1]

Assistant Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, Pune, India[2]

ABSTRACT: The Cloud Computing technology has improved the usage and management of the IT infrastructure. Cloud computing is divided by on-demand services, pooling of resources, ubiquitous network accesses, and elasticity. These features of Cloud Computing make cloud computing an outstanding technology for individual users and organizations. One of the vital aspects is data security amongst those eliminating the extensive implementation of Cloud Computing. Cloud security issues could arise from the implementation of core technology, cloud services and from cloud features. Prevalent concern in Cloud is about data and its security. Cyber security comprises of each and every domain that ought to be protected including Internet of Things (IoT), Cloud, Artificial Intelligence, Machine Learning. Cloud security is a component of Cyber Security that includes all the security requirements that are required for securing Cloud environment. The main emphasis of this paper is on the recent researches carried out in the field of Cyber Security in Cloud environment.

KEYWORDS: Cloud security, IoT, Cyber Security, Service Models, DDoS.

I. INTRODUCTION

Cloud computing is a technique that uses remote servers instead of local server that are hosted on Internet for storing and processing data. Cyber security comprises of various technologies and methods that are used for securing networks, devices and records from attack or unauthorized access. Cloud security is a component of Cyber Security that includes all the security requirements that are required for securing Cloud environment. Features of Cloud Computing are: on demand service, resource pooling, measured services and elasticity. The Service Models of Cloud are Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Most of the organizations and institutes are adopting the Cloud Computing technology. The protection of data is most important concern. After switching to the cloud, their security needs are handled by the providers, allowing them to concentrate more on their business. Although some of the most delicate data legislative departments have data saved in the cloud. The cloud allows for them to preserve their agreement requirements with simplicity. Startups make use of the cloud as it scales with the business. In the fast-paced startup environment, organizations don't have to decide among growing and staying secure.

Now-a-days everyone benefits from highly developed cyber defense programs. At user level, cyber security attack may result into identity theft, fraud or damage of significant data. Everybody relies on decisive infrastructure such as hospitals and financial service companies. Securing these organizations is necessary to keeping society functioning. One must understand that in the digital era, private information is more susceptible than ever before. Companies and organizations are regularly functioning to defend themselves with growing security measures.

Cloud computing improves the computation representation by offering elastic computation and storage to the users. Users can send information to the Cloud server and can access data from other devices. The client can demand cloud server to carry out several computations over the outsourced data. These benefits lead to huge success of cloud computing, but they also increase privacy and security concerns with respect to the client's outsourced data. The concerns come from the fact that the cloud service providers cannot be fully trusted.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

In this paper, we have surveyed on cyber security and cloud security. Section 2 of this paper deals with Literature Survey and Section 3 concludes this paper.

II. LITERATURE SURVEY

A comprehensive literature survey is performed in the support of cyber security and cloud security. In literature, several techniques have been presented for securing the data saved in the Cloud servers. The data outsourced to a public cloud must be secured. Unauthorized data access by new users and processes must be prevented. Cloud security is a bit similar to security in data centers without the expenses of maintaining services and hardware. In the cloud, it is not necessary to deal with physical servers or storage devices. As an alternative, software based security tools can be used for monitoring and protecting the information flowing into and out of resources. A number of techniques have been introduced in order to solve the complexity observed in the cloud security. Providing security to the data stored in cloud still remains difficult task.

Division and replication of data in the Cloud for optimal performance and security (DROPS) method has been proposed in [1] that jointly solves the performance and security issues. The proposed methodology divides data file into multiple fragments. Then, that fragmented data file is replicated on the cloud nodes. Each cloud node stores just a sole fragment of a data file so as to ensure that even a successful attack occurs, no information will be revealed by the attacker. Furthermore, the cloud nodes that are storing fragments are divided with some distance using graph T-coloring method to exclude attacker from guessing locations of the fragment. Besides, the proposed methodology does not use any conventional cryptographic method for the data protection. Thus, this relieves the system from computationally expensive methodologies. It has been shown that the likelihood to find and negotiate all of the cloud nodes have the fragments of a particular file is exceptionally low.

A lightweight data sharing (LDSS) scheme in favor of mobile cloud computing has been developed in [2]. This scheme uses Ciphertext Policy- Attribute based Encryption (CP-ABE) which is an access control method that has been used in cloud. But the structure of access control tree has been changed in order to formulate an appropriate access control method for mobile cloud environments. This scheme moves a huge segment of the computationally complex access control tree conversion in CP-ABE from mobile devices to exterior proxy servers. Additionally, for reducing the user revocation expenditure, attribute description fields has been introduced for implementing lazy revocation. LDSS efficiently reduces operating cost of the mobile device during data sharing by users in mobile cloud environment.

A completely secure white-box CP-ABE system has been developed in [3] for cloud storage service with a binding key. The proposed system permits data owners to describe access policies for data which is to be stored on cloud and authorized users will be assigned access credentials related to the attributes held by the users. For illegitimate leakage of access, the proposed system can outline the owner of the data whose access credentials have been leaked. In [4], a safe and fault-tolerant key agreement for group data sharing for cloud storage has been proposed. The proposed approach is based group signature and generates a common conference key proficiently that is used to defend data on cloud and maintain secure group data sharing in the cloud.

Scale Inside out approach has been developed in [5] which throughout attacks, reduces resource utilization factor to a negligible value. This enables quick absorption of the Distributed Denial of Service (DDoS) attack. During DDoS attacks, the system resources are used greatly. The genuine traffic approaching the victim service is not serviced all through the downtime. Additionally, damages due to the increased resource usage there are delays to the mitigation process. The traffic flow during these attacks is huge which cannot be absorbed by the victim system having the restricted resources. The victim service is reconfigured to have less resource consumption per request throughout the attack.

The cloud access control and the data owner end CP-ABE access control has been combined in [6]. The proposed scheme resolves the security problems in preserving privacy of cloud storage. This method can avoid the Economic Denial of Sustainability (EDoS) attacks provided that the cloud server with can check whether the user is allowed in CP-ABE based system. The ciphertexts are related to the access policy with the particular file. For an incoming data user, the cloud server asks user to decrypt arbitrarily selected challenge ciphertext. If the user shows a correct result, that means user is authorized and can download the file.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

A combined approach to cyber insurance provisioning and security for Cloud has been presented in [7]. Using random optimization, a method of optimally provisioning both services has been presented in spite of uncertainty concerning future pricing and cyber attacks. Since the optimization involves solving programming problem, the partial Lagrange multiplier method has been proposed that employs the entire modularity property that assures integer solutions, though soothing the difficulty of linear programming problem. This difficulty is solved using a sub gradient method, that has been proved converge to the optimal result in polynomial time. Using the result formed by the proposed algorithm, an analytical sensitivity analysis approach has been applied that provides specific sensitivity values for different parameters. A specific association between cyber insurance provisioning and security has been presented where the insurance provides an incentive for provisioning security, which reduces the expenses from packet damages.

III. CONCLUSION

In this paper, we have surveyed the different concepts of security issues which can occur in Cloud environment. The concept of DROPS (Division and replication of data in the Cloud for optimal performance and security), white-box CP-ABE system, absorption of the Distributed Denial of Service (DDoS) attack techniques and implementation are studied for reducing attacks on cloud security and cyber security.

REFERENCES

[1] M. Ali, K. Bilal, S. Khan, B. Veeravalli, K. Li, and A. Zomaya, "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security," *IEEE Transactions On Cloud Computing*, Vol. 6 , No. 2 , pp. 303- 315, June 2018.

[2] Ruixuan Li, Chenglin Shen, Heng He, Xiwu Gu, Zhiyong Xu, and Cheng-Zhong Xu, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing", *IEEE Transactions On Cloud Computing*, Vol. 6 , No. 2 , pp. 344 - 357, 2018.

[3] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and Lifei Wei, "White-Box Traceable CP-ABE for Cloud Storage Service: How to Catch People Leaking Their Access Credentials Effectively", *IEEE Transactions on Dependable and Secure Computing*, Vol. 15 , No. 5 , 2018.

[4] Jian Shen, Tianqi Zhou, Xiaofeng Chen, Jin Li, and Willy Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing", *IEEE* Transactions on Information Forensics and Security, Vol. 13 , No. 4, 2018.

[5] G. Somani, M. Gaur, D. Sanghi, M. Conti, and M. Rajarajan, "Scale Inside-out: Rapid Mitigation of Cloud DDoS Attacks", *IEEE Transactions on Dependable and Secure Computing*, Vol. 15 , No. 6, 2018.

[6] Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong and Peilin Hong, "Combining Data Owner Side and Cloud Access Control for Encrypted Cloud Storage," IEEE Transactions on Information Forensics and Security, Vol. 13 , No. 8, 2018.

[7] Jonathan Chase, Dusit Niyato, Ping Wang, Sivadon Chaisiri, Ryan Ko, "A Scalable Approach to Joint Cyber Insurance and Security-as-a-Service Provisioning in Cloud Computing," *IEEE Transactions on Dependable and Secure Computing*, Vol. 13 , No. 8, 2018.

[8] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, "Quantitative comparisons of the state of the art data center architectures," Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp. 1771-1783.

[9] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.

[10] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446-451.

[11] B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.

[12] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.