IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10407

IMPLEMENTATION OF CLOUD DECOY FILE USING SASSY INTRUSION DETECTION ALGORITHM

P.Prithiv Siva[1,] B.S.Tharani[2], S.VenkateshPrasad[3,] Mr.S.Vivekanandan, M.E.,[4]

Final year B.E, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode, Tamilnadu, India[1, 2, 3]

Assistant Professor, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode, Tamilnadu, India.[4]

Abstract: Data security in this digital age of human era is the important motivation behind this research work. As the utilization the online application becomes high, Trails of digital data's are always available to track a human behaviour, like his/her birthday, school of study and profile pic etc. It is unavoidable to be in online maximum of time, so strong fool proof data security mechanism without a large hardware trade-off is much needed..

I. INTRODUCTION

Cloud computing consists of a shared pool of resources shared among users per subscription basis. The way computer-stored information and personal data can cause new data security challenges. Cloud storage sectors are becoming the largest successful application interface for many online solutions, to avoid unauthorized cloud data access, Existing method proposes various cryptographic solutions, behavioral profiling of original user etc. but these mechanisms requires huge computational and storage resources to per . This paper proposes a simple yet power solution for intrusion detection cloud environment. A decoy file management service will be developed using JavaScript in which user can manually develop decoy intrusion trigger files. Original user only knows which files are decoy in nature, when the decoy files are accessed from a achieved through a preventive disinformation attack person other than user it will immediately alert the original user's mobile number through notification and will shut down the cloud access for current session. Cloud access will be regained once OTP based password verification is done through original users registered mobile number or mail.

2. LITERATURE REVIEW

Salvatore J.Stolfo, Malek Ben Salem, Angelos D.Keromytis.

The basic idea that they limited the damage of stolen data if decreased the value of stolen information to the attacker this achieved through a preventive disinformation attack. The cloud services can be implemented through two security features: User behavior profiling, decoy technology. They proposed approach to securing the cloud using decoy information technology called fog computing to launch disinformation attack against malicious insider, preventing from the real customer data from f ake worthless data by cloud service customers.

Keke Gai, Kim-Kwang Raymond choo, Liehuang Zhu.

Block chains, a decentralized storage technique, have many applications, including in reengineering cloud datacenters. This article proposes a conceptual mode for fusing bock chains and cloud computing for addition a value creation. The proposed model comprises three deployment modes: cloud over Block chain(CoB),Block chain over cloud(BoC),and Mixed Blockchain(MBC). The article also highlights the potential benefits of such a fusion and outlines a number of future research directions.

Priya dhir,Sushi Garg

Cloud computing is a technology, which providers low cost, scalable computation capacity and services to enterprises on demand for expansion. Although, cloud computing is facilitation the Information technology industry, the research and development in this arena is yet to be satisfactory. Cloud computing resources offered service on an as- needed basis, and delivered by IP–Based connectivity, providing highly scalable, reliable on-demand services with agile management capabilities. That are a lot of developments in the cloud computing, security of the data in the cloud has become the one of major aspects in the cloud computing is nothing but the sharing of thee resources is a open environment which leads to the security problems. This paper aim is to provide different modes od cloud computing and data masking techniques for providing security

Ganesh,Asha.

For web based cloud computing services we introduced fine grained two factor access control.

The basic concept behind the fine grained two factor access control is getting the permission from two parties in this case we consider two parties as user secret key and light weight device. In two factor access control system an attribute based control mechanism is implemented from the help of user secret key and lightweight security device.User must satisfy with this two for getting access to system.If anyone fails user can't get access to the system. The access control system denies the access of the user to the system if multiple user have same attribute set value.

Rishav Chatterjee, Sharmistha Roy

Cloud computing is an internet-based computing model which provides several resources through cloud service provider(CSP) to cloud users (cu) on demand basis without buying the underlying infrastructure and follows pay-per-use basis. It supports virtualization of physical resources in order to improve efficiency and accomplishment of multiple tasks at the same time. Cloud computing environment (CCE) provides several deployment models to represent several categories of cloud owned by organization or institutes.

However, CCE provider resources to cloud users through several services like pass, sass and Iaas. Cloud computing is a notion based on the concept of summing up physical resources and displaying them as an unacknowledged resource. It is a model for producing resources, for sorting out application, and for manifesto-independent user accesses to services. In this paper, we will focus upon the reviewing and understanding cloud security issues by proposing crypto algorithm and effective measures so as to ensure the data security in cloud. Along with this, we will elucidate a bit more about some security aspects of cryptography by showcasing some privacy issues of current cloud computing surroundings.

Christian Esposito , Aiello Castiglione, Florin pop, Kim – Kwang Raymond Cho

A given sensor network consists of tiny sensing devices deployed within an area of interest, such as forest , within a building or alone a motor way, to measure certain environmental factors, such as temperature, humidity, vibrations, pollution and so on. Such devices are typically only capable of computing simple task on the collected data, such as simple aggregation and filtering operation, and sending the collected information to base stations using short-range wireless communication. These base stations are more powerful devices, with a rechargeable battery and a stable wired connection to a centralized remote server in charge of collecting all data, performing complex analytics and presenting the result using visualization.

Barbara Russo, Laura valle

Disclosing personal data for a purpose not known by data subject is a practice that the 2018 European Union general data production regulation (GDPR) is supposed to prevent. This article gives an overview of the major aspects of GDPR related to provision, use, and maintenance of cloud services and technology.

Mu Yang,Andrea Margheri, Rushan Hu, and Vadimiro Sassone

Cloud federation is emergent cloud–computing paradigms that allow service from different cloud system to be aggregated in a single pool. To support secure data sharing in a cloud federation, anonymization services that obfuscate sensitive datasets under differential privacy have been recently proposed. However, by outsourcing data protection to the cloud, data owner lose control over their data, raising privacy concerns. This is even more compelling in multi-query scenarios in which maintaining privacy amounts to controlling the allocation of the so-called privacy budget. In this paper, we propose a blockchain- based approach that enables data owners to control the anonymization process and that enhances the security of the services. Our approach relies on blockchain to validate the usage of the privacy budget and adaptively changes its allocation through smart contracts, depending on the privacy requirements provided by data owners. Prototype implementation with the hyper ledger permissioned blockchain validates our approach with respect to privacy guarantee and practicality.

Shankar Gadhve , Deveshree Naidu

In cloud storage we store personal data which contain banking details such as account number, password, valuable notes, and other such information that can be misused by hackers. These data are copied and cached by cloud service providers, often without user's authentication and control. Securing the user valuable data's privacy. All the information and their copies become destructed. In this paper, we present a system that meets this challenge through integration of active storage techniques. We implemented self-destructive system through the different functionality and different security properties evaluations of this system. In addition to this the data privacy can be given to the system by encryption the data.

Sokratis K.Katsikas,Coasts Lambrinoudakis.

One of the new computing paradigms that has gained tremendous momentum in the past few years is cloud computing. This is due, at least to some extent, to the fact that IT cost reduction is achieved by offloading data and computations as an economic model has found versatile ground and is attracting a lot of investment, many are still reluctant to use cloud services because of several security, privacy and trust issues that have emerged. In answer to these concerns, the security and privacy in cloud computing (SEPRICC) special session within cloud computing 2017,held in Athens, Greece will provide an international forum for researchers and practitioners to exchange information regarding advancements in the state of the art and practice of security, privacy and trust in cloud computing

3. MODULES

A. *CLOUD WEB SERVICE DESIGN*

Using JavaScript as client side programming, a Web Service for uploading and downloading user documents will be developed. To store the user documents in cloud storage a PHP based server script will be developed. Users can able to sign up and sign in into our cloud web service for free. User data validation will be done on client side programming. User can be provided with Read, Edit and share options for their uploaded documents.

B. *USER DECOY FILE TRIGGERS*

User can create a folder and rename it with important names to lure the intruders. Users can select any folders in their personal cloud storage and change it status as decoy files. Once the decoy files are clicked by the intruder it will provide a trigger mechanism to the server side PHP programming Server side PHP scripting will imitate the auto password changing procedure immediately.

4. EXISTING SYSTEM

There are many algorithms on user behavior profiling and decoy technology but no one addresses the problem of efficiently delivering the decoy file in such a way the intruder not able to recognize the difference between the genuine and decoy file, once the anonymous behavior of the user identified. The existing system was not worked on anonymous behavior. The data stored on cloud need security for stored data, the way computer-stored information and personal data can cause new data security challenges.

5. PROPOSED SYSTEM

This project work proposes a simple power solution for intrusion detection cloud environment. A decoy file management service will be developed using JavaScript in which user can manually develop decoy intrusion trigger files. Original user only knows which files are decoy in nature, when the decoy files are accessed from a person other than user it will immediately alert the original user’s mobile number through notification and will shut down the cloud access for current session. Cloud access will be regained once a OTP based password verification is done through original users registered mobile number.

6. CONCLUSION

A successful design and implementation of the proposed secured cloud server is developed and deployed in online server. Static website content is developed using HTML styling and graphic designing of the page is designed using Cascaded style sheets. Form validation and user responses are processed using client side java scripting. Dynamic web page with Database management and cloud directory management is developed by PHP server. Multilevel security is achieved from the beginning of the user account creation. For account verification a 6 digit alpha numeric OTP will be generated randomly and sent to the user registered mail id. Second level of security will be provided when user attempt to login the user activity will be again sent to the registered mail id. Text will be displayed in Green on successful login and will be displayed in red when a user repeatedly enter wrong password. After successful login user can create virtual directories in their own allocated cloud space and dynamic menus will be created when user click a directory. User can select any directory as decoy folder, which multi folder the security of the directory and used for intrusion detection.

REFERENCES

[1] Francesco Palmieri, Gianni D’Angelo, Massimo Ficco, and. Malware detection in mobile environments based on auto encoders and api-images. Journal of Parallel and Distributed Computing, 137:26–33, 2020.

[2] AxelKüpper, FelixBeierle, IwailoDenisow, SebastianZickau. Dynamic location information in attribute-based encryption schemes. In 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, pages 240–247. IEEE, 2015.

[3] Jiguo Li, Ningyu Chen, and Yichen Zhang. Extended file hierarchy access control scheme with attribute based encryption in cloud computing. IEEE.Transactions on Emerging Topics in Computing, 2019

[4] Halil Murat Unver, Khaled Bakour and. Visdroid: Android malware classification based on local and global image features, bag of visual words and machine learning techniques. Neural Computing and Applications,pages 1–21, 2020.

[5] Adria Salvador Palau, Ajith Kumar Parlikad, Bhupesh Kumar Lad, Kushite Bakliwal, Maharshi Harshadbhai Dhada. And A multi agent system architecture to implement collaborative learning for social industrial assets. IFAC-PapersOnLine, 51(11):1237–1242, 2018.

[6] FRichard Yu, Mehdi Sookhak, Muhammad Khurram Khan, Rajkumar Buyya and Yang Xiang. Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. Future Generation Computer Systems, 72:273–287, 2017.

[7] George Q Huang , Gangyan Xu, Ming Li, and Peng Lin. Cloud-based ubiquitous object sharing platform for heterogeneous logistics system integration. Advanced Engineering Informatics, 38:343–356, 2018.

[8] Neha Agrawal and Shashikala Tapaswi. A trustworthy agent Based encrypted access control method for mobile Cloud computing environment.Pervasive Mobile Computing, 52:13–28, 2019.

[9] BG Kirankumar, Prakash H Unki and Suvarna L Kattimani. Cp-abe based mobile cloud computing application for secure data sharing. In International Conference on Intelligent Data Communication Technologies Internet of Things, pages 561–568. Springer, 2019.

DOI 10.17148/IJARCCE.2021.10407

[10] Praveen Kumar, PJA Alphonse, et al. Attribute based encryption in cloud computing A survey, gap analysis, and future directions. Journal of Network and Computer Applications,108:37–52, 2018. [11] Rahim Taheri, Reza Javidan, and Zahra Pooranian. Adversarial android malware detection for mobile multimedia applications in iot environments. Multimedia Tools and Applications, pages 1–17, 2020.

[12] Hissam Tawfik, Ismaeel Al Ridhawi, Moayad Aloqaily, Thar Baker, Yaser Jararweh, and Yehia Kotb. Cloud-based multi-agent cooperation for iot devices using workflow-nets. Journal of Grid Computing, 17(4):625–650, 2019.

[13] Dong Zheng, Jianfei Sun, Qi Li, Robert H Deng, Shengmin Xu, and Yinghui Zhang. Attribute-based encryption for cloud computing access control: A survey. ACM Computing Surveys (CSUR), 53(4):1–41, 2020.