International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Securing Cloud Using Decoy: A Review

Reega Maria[1]

[1,] *Department of Computer Sci. & Engg, Thejus Engineering College, Vellarakkad, Thrissur, Kerala, India*

Abstract - *Cloud computing provides ubiquitous, convenient, on-demand access to a shared pool of computing resources with minimal management effort. A large amount of personal and organizational data is stored in the cloud which needs to be protected from data theft and tampering attacks, especially insider attacks. Security is a major factor which needs to be focused on. Here proposing a different method to secure data stored in the cloud using User Behavior Profiling and Decoy Technology. Here detecting abnormal data access patterns and monitor data access in the cloud. If an unauthorized user activity is suspected and verified by using various security questions, deploying a disinformation attack by returning decoy information to the attacker. It ensures the security of the user's real data.*

***Key Words*: User Behavior Profiling, Decoy Technology.**

1. INTRODUCTION

Cloud storage is a strategical approach of networked enterprise storage where the data is stored in virtualized pools of storage with minimal management effort. For the business enterprise outsourcing data and storing in Cloud plays an important role. Storing data on the cloud contains many drawbacks which cannot be ignored. It includes delay, no location awareness, data theft, data tampering, bandwidth delay, etc. Data theft is considered as one of the top threats to cloud computing by the Cloud Security Alliance. Masqueraders act as legitimate users after obtaining the credentials of authorized users when they try to gain access to Cloud. When the masqueraders log in with the stolen credentials, he acts as the legitimate user with the same access rights as the real user. For avoiding data theft and tampering use concept of decoy and user behavior profiling along with the concept of fog computing. Fog computing act as an intermediator between cloud and edge devices. It solves issues of bandwidth, delay, location awareness problems. User profiling is well known for how, when, and how much a user accesses their information in the Cloud. Such 'normal user' behavior can be continuously checked to determine whether unauthorized access to a user's information is occurring. Decoy information, such as decoy documents, honey files, honeypots, and various other bogus information can be generated on demand and serve as a means of detecting unauthorized access to information for a confusing attacker. the decoy must be believable, enticing enough to attract, conspicuous and differentiable. That means it must be confusing to the attacker Masquerader, who is not familiar with the file system and its contents, is likely to access these decoy files. If he or she is an authorized user, gets bait information embedded in these decoy files. This decoy technology may be integrated with user behavior profiling technology to secure a user's information in the Cloud. Whenever unauthorized access to a cloud is noticed, decoy information may be returned. It appears completely legitimate and normal. Otherwise, it provides original data.

2. LITERATURE REVIEW

[1] Explain about authentication and integrity issues in the cloud, mainly focusing on the healthcare domain. Describes 2 major techniques such as data coloring based watermarking for making decoy documents and user behavior monitored by cusum algorithm. Cusum algorithm is used in which average fluctuations in user behavior calculated. Data coloring based watermarking helps to find data tampering. Here placed decoy documents along with original documents and access original documents/decoy documents with the help of Hmac.

[2] Many private and public organization implements firewalls, router access to control list, antivirus, intrusion detection system. But they are failed to prevent data due to various hacking tools. Using decoy system also named as deception system or honeypots or tar pits detect unauthorized access on networks and sends bogus information

[3] Explains about securing data in the cloud using offensive decoy technology. It also monitors normal data access and abnormal data access in the cloud. Here unauthorized access is verified by asking questions. It protects data from unauthenticated users

[4] Explains about securing healthcare data such as X-ray,CT Scan, MRI reports, etc protect from malicious insiders by bilinear pairing cryptography. It generates a session key among participant and communicates towards them securely. Here private healthcare data are accessed securely by implementing decoy technique.

[5] Explains about honey files to detect insider attacks by exfiltrating information. Honey files are bait files that reside on file server and server sends an alarm when honey files are accessed. These are tested by honeynet.

[6]Here tells about an offensive decoy technology to protect data from malicious insiders The anomaly detector used here to access decoy. It validates the local file and monitors access to the original file or decoy files by profiling the behavior of users.

[7] The author explains an application for securing data in the cloud using decoy techniques. To identify user profile activity logs use a naïve Bayes classification method to identify whether the user is real or not. But the usage of naïve Bayes classifier it provides low accuracy and theoretically infeasible information. The system also challenges real user by asking a one-time password(OTP) for verifying identity. Based on user profiling provide real/decoy data to users. The system maintains the integrity by providing the SHA-1 algorithm.

[8] Explains the creation of bait information aim to expose malicious insiders. For this use decoy documents. They are automatically generated and stored in file system D^3. Also, embed stealthy beacons in documents. It creates a signal that emitted to the server when decoy documents were opened.

[9] The author tells about software-based decoy system aims to deceive malicious insiders. Bogus software is generated iteratively side code obfuscation technique. It transforms a program by inserting new code or modifying existing code Beacons are also injected to bogus software to understand if the decoy software is modified or not.

[10]Tells about a novel approach to securing personal and business data in the cloud using fog. Here profiling user search behavior by developing models trained with one class modeling technique called support vector machines. It builds a classifier without to share data from distinct users. But it has high algorithm complexity and requires extensive memory. Based on user profiling decoy documents ate provided. Decoy documents are stored along with user's real data. It also calculates keyed hashed authentication code(Hmac) for checking whether it is a decoy or not for further usage.

[11] Explains about decoy traffic n Tor networks with help of decoy Internet message access protocol(IMAP) and simple mail access protocol(SMAP) servers.

[12]The author explains about a hybrid protocol such as selective encryption with data cleaning, enhanced neural network based user profiling and decoy technology to secure cloud from insider threats. It also uses the concept of fog computing. Selective encryption indicates only selected information provides maximum security. After that encrypted key deleted from the system. Using selective encryption when an authorized user decrypts data it would be stored in the physical memory of a volatile machine. A malicious insider can steal this decrypted data. Data cleaning prevents planned/unplanned access to volatile memory until data has been deleted or overwritten. User search behavior is profiled here by using neural networks to understand whether the authenticated user or not. But it computationally requires a large number of training data and very expensive been deleted or overwritten. User search behavior is profiled here by using neural networks to understand whether the authenticated user or not. But it computationally requires a large number of training data and very expensive been deleted or overwritten. User search behavior is profiled here by using neural networks to understand whether the authenticated user or not. But it computationally requires a large number of training data and very expensive

3. COMPARISON TABLE

Paper title	Techniques	Advantages
Data-Driven Techniques For Neutralizing Authentication And Integrity Issues In Cloud	1.Data coloring based watermarking for making decoy documents. 2.User behavior – CUSUM algorithm	1.protect shared data objects and ensures the security level in the cloud.
Decoy Systems: A New Player in Network Security and Computer Incident Response	1.Honeypots	1. Reduce false positive. 2.Cost-effective 3.Simplicity 4. Avoid data theft 5. Avoid data tampering
Secured Cloud Computing With Decoy Documents	1.Decoy technology 2.Asking a questionnaire for user behavior profiling	
Security Model For Preserving The Privacy Of Medical Big Data In Health CareCloud Using A Fog Computing Facility With Pairing-Based Cryptography	1.Decoy technology 2.Bilinear pairing cryptography	1. Avoid data theft 2. Avoid data tampering. 3.Provide integrity of data
Honey Files: Deceptive Files For Intrusion Detection	1.Honeyfiles 2.Honeynet	1. Reduce false positive. 2.Cost-effective 3.Simplicity 4. Avoid data theft 5. Avoid data tampering
Alleviating Malicious Insider In Cloud Through Offensive Decoy Technology	1.User behavior profiling 2.Decoy technology	1. Avoid data theft 2. Avoid data tampering.

Data Security System In Cloud By Using Fog Computing And Data Mining	1.User behavior profiling-naïve Bayes classifier 2.OTP 3.SHA-1-Integrity checking	1.Simple 2.Easy to implement. 3. Provide integrity of data. 4. Avoid data theft and tampering.
Baiting inside attackers using decoy documents	1.Decoy technology 2. Stealthy beacons embed –User behavior profiling.	1. Avoid data theft 2. Avoid data tampering.
Software Decoys For Insider Threats	1.Software-based decoy system. 2 Code obfuscation technique	1. Avoid data theft 2. Avoid data tampering
Fog Computing : Mitigating Insider Data Theft Attacks In Cloud	1.SVM classifier-User behavior profiling. 2.Decoy technology.	1. Works well with even unstructured and semi-structured data like text, Images, and trees. 2. Avoid data theft 3. Avoid data tampering.
Detecting Traffic Snooping in Tor Using Decoys	1.Decoy traffic n Tor network	1. Prevent HTTP session hijacking attacks. 2. Avoid data theft and data tampering.
A Hybrid Protocol To Secure Cloud From Insider Threats	1.Selective encryption with data cleaning 2.Enhanced neural network based user profiling 3 Decoy technology	1. 1.Avoid data theft 2. Avoid data tampering. 3. Handle a large number of data sets.

4.CONCLUSION

Using decoy technology and user behavior profiling avoid data tampering and data theft attacks commonly take place in the cloud. Using this technology protect a large amount of data in the cloud. Decoy technology fakes malicious insider by providing bogus information. For implementing decoy technique many methods are used . With the help of fog provide a layer of security for user information stored in the cloud. During user behavior profiling if any unauthorized user activity is suspected and verified by security questions, return decoy information to the attacker.

REFERENCES

[1] Sethuraman Srinivas And Sripriya Menon, "Data-Driven Techniques For Neutralizing Authentication And Integrity Issues In Cloud", In ARPN Journal Of Engineering And Applied Sciences,2017, Vol.12, No.4, Pp.614-656

[2] Kellep A. Charles, "Decoy Systems: A New Player In Network Security And Computer Incident Response"International Journal Of Digital Evidence Winter 2004, Volume 2, Issue 3.

[3] Nilesh. V.Koli, "Secured Cloud Computing With Decoy Documents", International Journal Of Advances In Computer Science And Cloud Computing, Vol2, November 2014

[4] Ahmad Almogren, "A Security Model For Preserving The Privacy Of Medical Big Data In Health Care Cloud Using A Fog Computing Facility With Pairing-Based Cryptography", IEEE Access, November 2017.

[5] J.Yuil, "Honey Files: Deceptive Files For Intrusion Detection", IEEE SMC Information Assurance Workshop,2004

[6] Ms.B Ankayarakanni, "Alleviating Malicious Insider In Cloud Through Offensive Decoy Technology", International Journal On Information Science And Computer, Vol 8, July 2014.

[7] rohit ghodake, "data security system in the cloud by using fog computing and data mining", international journal of advanced research in computer science and software engineering volume 7, issue 3, March 2017

[8] Brain M Bowen, "Baiting Inside Attackers Using Decoy Documents", International Conference On Security And Privacy In Communication Systems,2009

[9] Yonghee Park, "Software Decoys For Insider Threats", ASIACSS, May 2012

[10] Malek Ben Salem, "Fog Computing: Mitigating Insider Data Theft Attacks In Cloud", In IEEE Symposium On Security And Privacy Workshops,2012, Pp.489-498

[11] Sambuddho Chakravarty, "Detecting Traffic Snooping In Tor Using Decoys", International Conference On Recent Advances In Intrusion Detection, Pp.222-241

[12] Sriram M And Krishna D, "A Hybrid Protocol To Secure Cloud From Insider Threats", In IEEE International Conference On Cloud Computing, 2015, Pp.489-499.