ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 12; Issue 01; 2024; Page No. 22-24

Securing Cloud Infrastructure: Leveraging Fog Computing for Enhanced Protection

Sweety

Dept of computer science and Engineering, Vaish college of Engineering, MDU Rohtak

E-mail: sweetyahlawat6@gmail.com

Conflicts of interest: Nil

Corresponding author: Sweety

Abstract

In essence, a cloud is a collection of several dedicated servers connected by a network. A network-based environment called "cloud computing" is centered on resource or computation sharing. Customers just pay for the resources they use in the cloud; they are not required to pay for local resources like infrastructure or storage. Thus, this is the primary benefit of cloud computing and the primary cause for its increasing popularity in the modern world. Because it may lower processing costs while enhancing the flexibility and scalability of computer processes, cloud computing is also one of the most exciting technological advancements. However, security is the primary issue that arises with clouds. Furthermore, security and privacy are currently the two key issues that need to be taken into account. We are developing a new technology called fog computing to address the security issue. By offering security within the cloud environment, fog computing simply expands on cloud computing rather than replacing it. We can improve the cloud experience by separating user data that must reside on the edge with Fog services. Fog computing's primary goal is to put the data close to the consumer

1. Introduction

Cloud computing has emerged as a fundamental technology shaping the modern digital landscape, offering unparalleled scalability, flexibility, and accessibility for organizations across various industries. However, amidst its widespread adoption, security concerns loom large, threatening the integrity and confidentiality of sensitive data stored and processed within cloud environments. As cyber threats continue to evolve in sophistication and frequency, traditional security measures often fall short in providing adequate protection against emerging attack vectors. In response to these challenges, fog computing has emerged as a promising paradigm to augment the security posture of cloud computing environments. Fog computing extends the capabilities of traditional cloud architectures by decentralizing computing resources closer to the network edge, thereby reducing latency and improving overall performance. Importantly, fog computing introduces a distributed approach to data processing and storage, minimizing the attack surface and enhancing resilience against cyber threats.

In today's worlds both large and small enterprises in the modern world employ cloud computing technologies to safeguard their data and access cloud resources as needed. Cloud computing is a subscription service. Cloud computing refers to a shared resource pool. New data security concerns may come from the way we use computers and maintain our personal and business information. Unauthorized access to cloud data is not prevented by encryption methods. Traditional database systems, as is well known, are often installed in closed environments, with users able to access the system via a limited network or the internet. Due to

the rapid expansion of the World Wide Web, users can access almost any database to which they are authorized from any location in the world. By creating an account on the cloud, an organization can access its resources from cloud providers and retrieve its data whenever and wherever it's needed. However, this comfort comes with some risks, such as those related to privacy and security. Fog computing is a new technology we are using to solve this challenge. To fully enjoy the benefits of fog computing, a user must register with the fog. Fog computing offers increased security in cloud environments. The user will receive an email or message indicating that he is prepared to use fog computing services as soon as he fills out the sign-up form.

1.1Existing System - In the existing cloud computing paradigm, data processing and storage primarily occur in centralized data centers, often located at a considerable distance from end-users. While this centralized approach offers scalability and accessibility, it also introduces inherent security vulnerabilities. Traditional security measures, such as firewalls, encryption, and access controls, are typically implemented to safeguard data within these centralized environments. Current data security methods, like encryption, were unable to keep the data safe from hackers. Whether the user was authorized or not is not verified. Solutions for protecting data from unwanted access are not the main emphasis of cloud computing security. Our data is not particularly secure when it comes to encryption. 2009 Our own private documents are stored in the cloud. There is not much security on this file. Thus, the documents are accessed by the hacker. One instance of a cloud-based data theft assault is the Twitter incident. It was hard to locate the assailant. Cloud computing security was established against attackers in 2010 and 2011. Furthermore, it demonstrates that current study findings that could be helpful to safeguard data in the cloud.

Table 1: Existing survey for Fog computing & Cloud Computing

Fog Computing	**Authors**	**Publication**	**Summary**
1.	M. Hassan et al.	*IEEE Access*, 2019	Overview of fog computing concepts, architectures, and applications, highlighting benefits and challenges.
2.	S. Ruj et al.	*IEEE Access*, 2018	Discussion of security and privacy challenges in fog computing environments, with proposed solutions and future research directions.
3.	A. Mukherjee et al.	*IEEE Potentials*, 2019	Examination of fog computing's role in minimizing latency in IoT applications, focusing on performance and scalability improvements.
Cloud Computing	**Authors**	**Publication**	**Summary**
1.	T. Erl et al.	Pearson Education, 2013	Comprehensive overview of cloud computing concepts, technologies, and architectures, covering various deployment and service models.
2.	S. Subashini and V. Kavitha	Proceedings of ICACCI, 2011	Survey of security challenges in cloud computing environments, including data privacy, access control, and compliance issues, with proposed solutions.
3.	R. Garg et al.	*International Journal of Information Management*, 2013	Examination of cloud computing applications in the healthcare sector, discussing improvements in patient care, data management, and resource optimization.

1.2 Proposed System: We have introduced a novel method for enhancing data security in cloud environments, termed Fog Computing, which leverages user behavior and decoy information technology. This technique involves monitoring data access within the cloud and identifying abnormal access patterns. When unauthorized individuals attempt to access a user's data, the system generates decoy documents that are indistinguishable from real data. To verify the authenticity of the user, the system prompts them with a security question provided during the signup process. If the user fails to provide the correct answer, indicating potential unauthorized access, the system provides them with decoy documents. Conversely, if the user provides the correct answer, authentic data is provided to the user. This approach represents a departure from traditional cloud security methods and offers a proactive means of protecting user data against unauthorized access. [7]

2. SECURING CLOUDS USING FOG:

Securing cloud environments using fog computing offers a range of methods for storing files, documents, and media remotely, accessible to users via internet connections. The primary challenge in cloud security revolves around safeguarding user data to ensure only authenticated individuals can access it. This presents a fundamental security issue, as conventional methods often fail to provide the desired level of assurance. Despite relying on standard access control and encryption techniques, these approaches are prone to vulnerabilities due to implementation errors, insider threats, misconfigurations, and unforeseen sophisticated attacks.

Establishing a secure and reliable cloud computing environment is crucial, yet insufficient, as data breaches continue to occur, resulting in irreversible information loss. Addressing these challenges requires proactive measures to mitigate the impact of data theft. One approach involves diminishing the value of stolen data to potential attackers through preventive decoy tactics. By integrating additional security features, cloud services can be fortified against unauthorized access, enhancing overall data protection.

2.1 Decoy System: Decoy data, like counterfeit documents and other fabricated information, can be generated as needed to detect unauthorized attempts to access information and to disrupt the theft of the thief's obtained data. Providing false information can mislead an attacker into believing they have accessed valuable information, when they have not. This technology can be merged with user behavior profiling to enhance data security in cloud environments. Whenever unusual and unauthorized access to a cloud service is detected, the cloud can respond by delivering false information in a manner that appears genuine. The legitimate user, who owns the data, would recognize when false information is provided by the cloud and could prompt adjustments to the cloud's responses through various methods, such as challenge questions, to signal to the cloud security system that it has misidentified an unauthorized access attempt. In cases where unauthorized access is accurately identified, the cloud security system would inundate the attacker with substantial amounts of fabricated data, thus protecting the user's actual data. This can be accomplished by implementing two additional security features: (1) verifying the authorization of data access when abnormal data access is detected, and (2) confusing the attacker with counterfeit information provided as decoy documents.

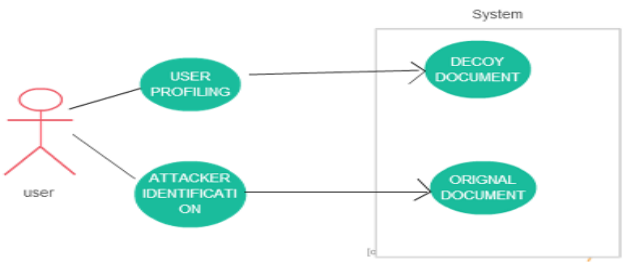

Fig 1: Decoy System

We've implemented the aforementioned strategies to identify illicit data access on a local file system by masqueraders, individuals who pose as legitimate users by acquiring their credentials. Our experiments conducted in a local file system environment indicate that integrating both methods can produce improved detection outcomes. These findings indicate the potential effectiveness of this approach in cloud environments, aiming to render cloud systems as user-transparent as local file systems. [8]

3.ARCHITECTURE OF FOG COMPUTING

Fog Computing system is trying to work against the attacker especially malicious insider. Here malicious insider means Insider attacks can be performed by malicious employees at the providers or users site. Malicious insider can access the confidential data of cloud users. A malicious insider can easily obtain passwords, cryptographic keys and files. The threat of malicious attacks has increased due to lack of transparency in cloud providers processes and procedures. It means that a provider may not know how employees are granted access and how this access is monitored or how reports as well as policy compliances are analyzed.

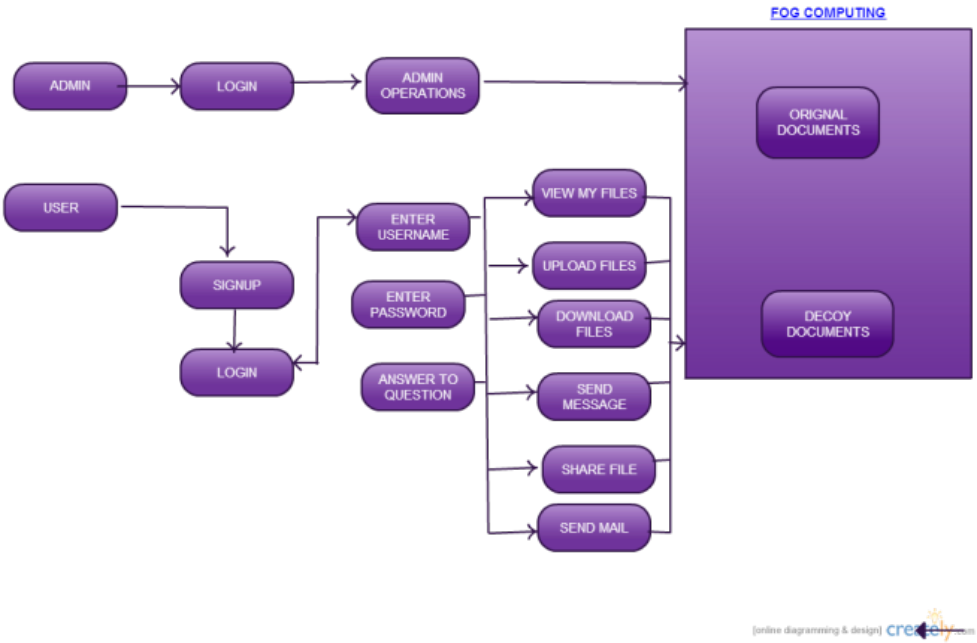

Fig -2: Architecture of Fog Computing

Above fig. states the actual working of the fog computing .In two ways login is done in system that are admin login and user login .When admin login to the system there are again two steps to follow:

step1: Enter username

step2: Enter the password.

After successful login of admin he can perform all admin related tasks, but while downloading any file from fog he have to answer the security Question if he answer it correctly then only original file can be download. In other case, when admin or user answer incorrectly to the security question then decoy document (fake document) is provided to the fake user. Decoy technology work in the given manner if you have any word ,suppose "MADAM" in the document then some alphabets are replaced as M->A then the given word become "AADAA" which have no meaning. In some Case ,if attacker getting to know that „M" is replaced by „A" in the given document and by applying reverse engineering he get result as "MMDMM".

When user login to the system he also have to follow the same procedure as admin. Operations like upload files/documents, download

files/documents, view alerts, send message, read message, broadcast any message all these can be perform by the user. ALERT this stream provide the detail knowledge of attack done on their personal file/document with details like date, time, no of times the attacker trying to hack that file/document. One of the key benefits of fog computing is that after every successful login, the user receives an SMS notification on their mobile device confirming the successful login. This feature serves as an alert mechanism for the user, notifying them when someone else attempts to access their personal fog account. Additionally, in the event that an attacker tries to download files or documents, the user also receives an SMS containing details such as the attacker's IP address, server name, date, and time on their mobile device. This provides the user with valuable information to identify and trace the attacker, enhancing security measures [9].

4. FOG COMPUTING VS CLOUD COMPUTING:

There differences are as follows: [10]

Table 1

Requirements	Cloud Computing	Fog Computing
Latency	High	Low
Delay Jitter	High	Very low
Location of Service	Within the Internet	At the edge of the local network
Distance between client and server	Multiple hops	One hope
Security	Undefined	Can be defined
Attack on data enroute	High probability	Very low probability
Location awareness	No	Yes
Geo-distribution	Centralized	Distributed
No. of server nodes	Few	Very large
Support for Mobility	Limited	Supported
Real time interactions	Supported	Supported
Type of last mile connectivity	Leased Line	Wireless

Table 2

Cloud Computing	Fog Computing
Data and applications are processed in a cloud, which is time consuming task for large data.	Rather than presenting and working from a centralized cloud, fog operates on network edge. So it consumes less time.
Problem of bandwidth, as a result of sending every bit of data over cloud channels.	Less demand for bandwidth, as every bit of data's were aggregated at certain access points instead of sending over cloud channels.
Slow response time and scalability problems as a result of depending servers that are located at remote places.	By setting small servers called edge servers in visibility of users, it is possible for a fog computing platform to avoid response time and scalability issues.

This table summarizes the key differences between fog computing and cloud computing across various aspects, highlighting their respective strengths and weaknesses in different use cases.

5. APPLICATIONS:

Applications of Fog Computing are as follows: [11,12]

Table 3

1. Connected Vehicles (CV)	The Connected Vehicle distribution displays a rich setup of connectivity and interactions: cars to cars, cars to access points (Wi-Fi, 3G, smart traffic lights), and access points to access points.
2. Wireless Sensor and Actuator Networks (WSAN)	The real Wireless Sensor Nodes (WSNs), were designed to operate at particularly low power in order to extend battery life or even to make energy reaping achievable. Most of these WSNs involve a large number of less bandwidth, less energy, very low processing power, trivial memory motes, operating as sources of a sink (collector), in a unidirectional fashion.
3. IoT and Cyber-Physical Systems (CPSs)	Fogging based systems are becoming a significant class of IoT and CPSs. IoT is a network that can interrelate ordinary physical objects with identified addresses. CPSs article a constricted combination of the systems computational and physical elements. CPSs also organize the incorporation of computer and data centric physical and engineered systems.
4. Software Defined Networks(SDN)	SDN concept along with Fogging will determine the main problems in vehicular networks, irregular connectivity, collisions and high packet loss, by supplementing vehicle-to-vehicle with vehicle-to-infrastructure communications and unified control.
5. Decentralized Smart Building Control	The applications of this development are enabled by wireless sensors positioned to measure temperature, humidity, or various levels of gases in the building atmosphere. In this case, information can be exchanged among all sensors in a floor, and their analyses can be combined to form unfailing measurements.

6. CONCLUSIONS: The system initially featured only email functionality, but we have now integrated SMS capabilities. In the realm of Fog Computing, we introduce a fresh method to address insider data theft threats within cloud environments. This approach involves the dynamic creation of decoy files to deter attacks, while also reducing the storage overhead typically associated with maintaining decoy files in the cloud. By employing decoy techniques within Fog Computing, we aim to mitigate the risk of insider attacks in cloud systems [13].

References

1. M. Hassan et al., "Fog Computing: A Review on Concepts, Architectures, and Applications," IEEE Access, vol. 7, pp. 99682-99703, 2019.
2. S. Ruj et al., "Security and Privacy Issues in Fog Computing: A Comprehensive Review," IEEE Access, vol. 6, pp. 75976-76003, 2018.
3. A. Mukherjee et al., "Fog Computing: Towards Minimizing Latency in the Internet of Things," IEEE Potentials, vol. 38, no. 1, pp. 16-20, Jan.-Feb. 2019.
4. T. Erl et al., "Cloud Computing: Concepts, Technology & Architecture," Pearson Education, 2013.
5. S. Subashini and V. Kavitha, "Security Challenges in Cloud Computing: A Comprehensive Survey," Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 800-805, 2011.
6. R. Garg et al., "Cloud Computing: A Review of Applications in Healthcare," International Journal of Information Management, vol. 33, no. 5, pp. 875-881, Oct. 2013.
7. Cloud Computing for Dummies"
8. S. Muqtyar Ahmed, P. Namratha, and C. Nagesh, "Prevention Of Malicious Insider In The Cloud Using Decoy Documents."
9. Gehana Booth, Andrew Soknacki, and Anil Somayaji, "Cloud Security: Attacks and Current Defenses."
10. Ajey Singh and Dr. Maneesh Shrivastava, "Overview of Attacks on Cloud Computing."
11. Pew Research Center, "Social Isolation and New Technology," [Online]. Available: http://www.pewinternet.org/Reports/2009/18–Social-Isolation-and-New-Technology.aspx.
12. [Online]. Available: http://www.informaworld.com/smpp/content~db=all~content=a929065326.
13. Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.