IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FOG COMPUTING: An Extended Version of Cloud Computing

[1]Mr. T. Pandu Ranga, [2]Kotla Sachin

[1]Associate Professor, [2]Student [1]Data Science

[1]Geethanjali College of Engineering and Technology, Cheeryal Village, India

Abstract: Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications paradigms arise new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider, For securing user data from such attacks a new paradigm called fog computing can be used. Fog Computing is a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users. The motivation of Fog computing lies in a series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined network .This technique can monitor the user activity to identify the legitimacy and prevent from any unauthorized user access. Here we have discussed this paradigm for preventing misuse of user data and securing information.

Keywords **-Cloud Computing,Fog Computing,Data Security,Data Theft Attacks,Insider Attacks,Encryptions,Smart Grids,Vehicle Networks,Software Defined Network(SDN),Unauthorized Access,Data Leakage**

I. INTRODUCTION

In this era, Cloud computing is achieving popularity every day. The ease of use and storage which is provided to users for personal and business purposes is increasing its demand. Although, cloud computing provides an environment through which managing and accessing of data becomes easier but it have consequences such as data leakage, data theft, insider attacks etc. Very common risks now days are data theft attacks. The Twitter incident is one example of a data theft attack from the Cloud. Several Twitter corporate and personal documents were ex-filtrated to technological website Tech Crunch and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed. The attacker used a Twitter administrator's password to gain access to Twitter's corporate documents, hosted on Google's infrastructure as Google Docs. The damage was significant both for Twitter and for its customers. Van Dijk and Juels have shown that fully homomorphic encryption, often acclaimed as the solution to such threats, is not a sufficient data protection mechanism when used alone. To resolve these issues a mechanism which can detect such malicious activities is required. For this, Fog computing is paradigm which monitors the data and helps in detecting an unauthorized access.

Edge-based Data Processing:

- Fog computing moves computation, storage, and networking closer to the edge of the network, typically near the data source (e.g., IoT devices, sensors). By processing data locally, it minimizes the risk of data breaches that could occur if sensitive information is transferred to a centralized cloud.

Decentralized Architecture:

• Unlike centralized cloud computing, fog computing employs a distributed architecture where resources are spread across multiple devices and nodes at the edge. This reduces the single point of failure risks and ensures that data can be protected at various levels.

Latency Reduction:

• By keeping data processing closer to the end-user, fog computing reduces the latency associated with cloud computing. This is particularly important for real-time applications such as smart grids, autonomous vehicles, and smart cities where response times are critical.

Contextual Awareness and Local Decision Making:

• Fog computing systems are designed to make local decisions based on the context of the data and environment. This enables rapid detection of anomalies or suspicious activity (e.g., unauthorized access attempts) and can trigger immediate responses such as alerting administrators or blocking access, preventing data theft.

Security at the Edge:

• Security protocols such as encryption, access control, and intrusion detection can be implemented at the fog nodes, ensuring data protection as it travels across the network. Localized security measures reduce the chances of attacks compared to centralized cloud environments.

Scalable and Dynamic Security:

• Fog computing offers scalability, meaning that as the number of devices and users increases, additional fog nodes can be deployed to handle the growing security demands. Fog computing also supports dynamic security solutions where security measures can evolve based on real-time monitoring and threat intelligence.

Authentication and Identity Management:

• Fog computing enables better management of user identities and device authentication.With mechanisms such as multi-factor authentication (MFA) or token-based authentication, it ensures that only authorized users and devices can access sensitive data and services.

1. **User Authentication & Monitoring**

- Users log in to the cloud system.
- The system continuously monitors user behavior (e.g., login patterns, access frequency, location, and device).
- Any unusual activity triggers a security check.

2. **Behavior Analysis & Threat Detection**

- If a login or data request seems suspicious, the system analyzes the access pattern.
- The system compares the behavior with the user's historical behavior data.
- If behavior is normal → access is granted.
- If behavior is suspicious → a security mechanism is triggered.

3. **Decoy Information & Fake Data Generation**

- If unauthorized access is detected, fake (decoy) data is generated instead of real data.
- The attacker receives decoy files that appear real but contain misleading or useless information.

4. **Identity Verification through Security Questions**

- The system prompts the user to answer a pre-set security question.
- If the answer is correct → real data is provided.
- If the answer is incorrect → only decoy data is shown.

5. **Incident Reporting & Response**

- If unauthorized access is detected, the system logs the activity.
- Alerts are sent to the user and cloud administrators.
- The attacker’s session is monitored or blocked based on severity.

II. FOG COMPUTING TASKS

1. Data Processing at the Edge:

- Processes data closer to the user, reducing latency and improving efficiency.

2. Real-time Analytics & Decision Making:

- Performs real-time data analysis to support time-sensitive applications like smart grids and autonomous vehicles.

3. Security & Access Control:

- Monitors and restricts unauthorized access.
- Implements authentication and encryption mechanisms.

4. Bandwidth Optimization:

- Reduces the load on cloud servers by handling computations locally.

5. Data Storage & Management:

- Provides temporary or permanent storage for processed data before sending it to the cloud.

III. TYPES OF DATA MINING SYSTEMS

- **Device-Level Fog Computing:**Runs on end devices such as IoT sensors, smartphones, or edge gateways.Used for local processing and decision-making.

- **Gateway-Level Fog Computing:**Uses network gateways and routers to process and filter data before sending it to the cloud. Common in smart homes and industrial automation.

- **Edge Server-Based Fog Computing:**Deploys dedicated edge servers near end-users for computing, storage, and security tasks.Used in smart cities, autonomous vehicles, and healthcare systems.

- **Cloudlet-Based Fog Computing:**Small-scale cloud data centers placed at the network edge.Provides low-latency services for mobile applications and augmented reality.

- **Micro Data Center (MDC) Fog Computing:**Compact data centers with computing and storage capabilities.Used in large- scale IoT deployments like smart grids and connected factories.

IV. DATA MINING LIFECYCLE

The lifecycle of fog computing consists of several stages that define how data and services are processed at the edge of the network. Below are the key stages:

Data Generation & Collection: Sensors, IoT devices, and user applications generate raw data.Data is collected through connected devices in real-time.
Preprocessing & Filtering: The fog nodes (gateways, routers, or edge servers) filter, preprocess, and clean the data.Reduces redundant or unnecessary data before transmission.
Local Processing & Analysis: Computing tasks are performed at the fog layer instead of the cloud to reduce latency.AI and machine learning algorithms can be applied for real-time decision-making.
Storage & Caching: Processed data is stored temporarily in local fog nodes or micro data centers. Frequently accessed data can be cached for faster access.

Security & Access Control: User authentication and encryption mechanisms protect the data. Anomaly detection systems monitor for unauthorized access or threats.

Communication with Cloud: Only relevant or high-priority data is sent to the cloud for long-term storage or further analysis. Reduces bandwidth usage and cloud dependency.

Action & Response: Based on the analysis, actions are taken automatically (e.g., traffic light changes in smart cities).Alerts or reports are sent to users or administrators if needed.

V. THE DATA MINING MODELS

Fog computing models define how computing, storage, and networking resources are utilized at the edge of the network. The **Device-to-Device (D2D) model** allows devices to communicate directly without cloud involvement, making it ideal for smart homes, IoT networks, and autonomous vehicle communications. In the **Device-to-Gateway model**, end devices such as IoT sensors and cameras send data to a gateway for local processing before forwarding relevant information to the cloud, commonly used in industrial automation and smart healthcare. The **Gateway-to-Cloud model** involves gateways and fog nodes acting as intermediaries between edge devices and the cloud, reducing cloud dependency and improving response times in applications like smart cities and real-time analytics. The **Peer-to-Peer (P2P) Fog model** enables multiple fog nodes to interact and distribute processing tasks, beneficial for large-scale IoT applications such as smart grids and disaster management. Finally, the **Hierarchical Fog Computing model** follows a multi-layered structure where computing tasks are divided across different levels, including edge devices, fog nodes, and the cloud, making it suitable for complex systems like autonomous vehicles and 5G networks. Each of these models plays a crucial role in optimizing computing performance and enhancing security in fog computing environments.

VI. THE KNOWLEDGE DISCOVERY PROCESS

1. User Authentication & Monitoring

- Users log in to the cloud system.
- The system continuously monitors user behavior (e.g., login patterns, access frequency, location, and device).
- Any unusual activity triggers a security check.

2. Behavior Analysis & Threat Detection

- If a login or data request seems suspicious, the system analyzes the access pattern.
- The system compares the behavior with the user's historical behavior data.
- If behavior is normal → access is granted.
- If behavior is suspicious → a security mechanism is triggered.

3. Decoy Information & Fake Data Generation

- If unauthorized access is detected, fake (decoy) data is generated instead of real data.
- The attacker receives decoy files that appear real but contain misleading or useless information.

4. Identity Verification through Security Questions

- The system prompts the user to answer a pre-set security question.
- If the answer is correct → real data is provided.
- If the answer is incorrect → only decoy data is shown.

5. Incident Reporting & Response

- If unauthorized access is detected, the system logs the activity.
- Alerts are sent to the user and cloud administrators.
- The attacker’s session is monitored or blocked based on severity.

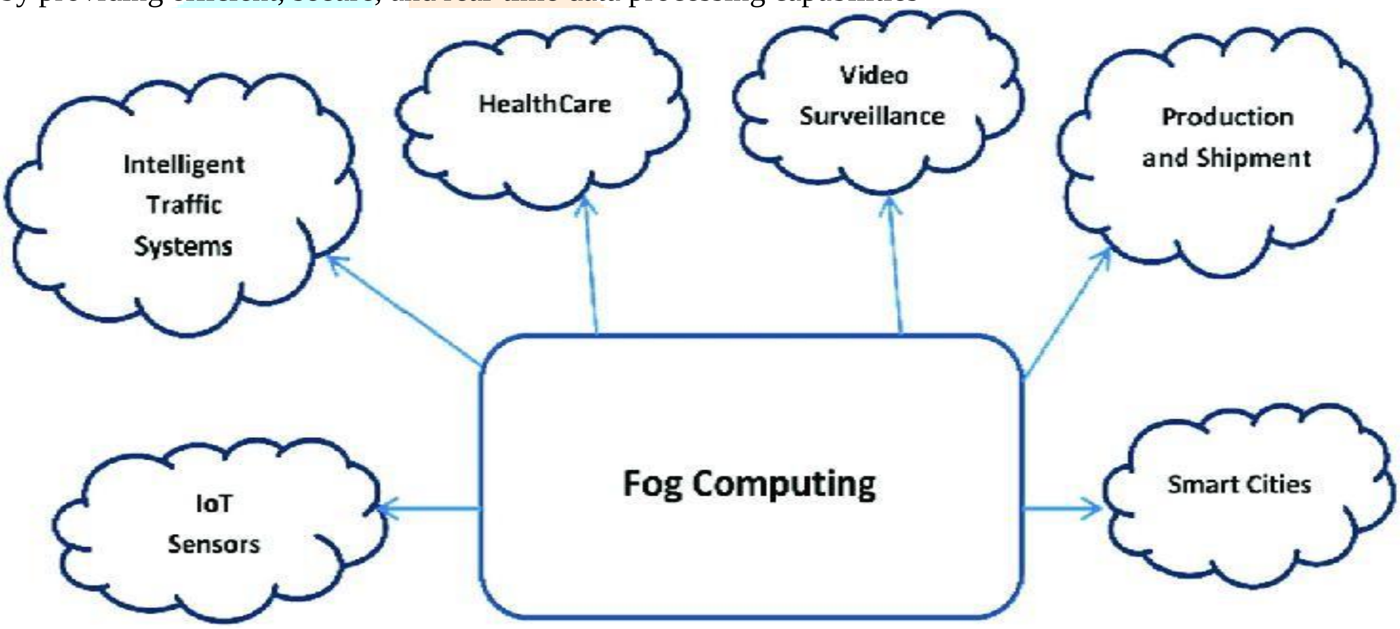
VII. DATA MINING METHODS

Fog computing employs various methods to enhance data processing, security, and efficiency at the network edge. Data Filtering and Preprocessing ensures that only relevant information is processed and transmitted, reducing unnecessary data load on the cloud. Real-time Data Analytics enables immediate decision-making, which is crucial in applications like smart cities, healthcare monitoring, and industrial automation. Edge Caching and Storage allow frequently accessed data to be stored locally, minimizing latency and improving performance. Security and Access Control Mechanisms help protect sensitive data by implementing encryption, authentication, and anomaly detection to prevent unauthorized access. Resource Allocation and Load Balancing optimize the distribution of computing tasks among fog nodes to ensure efficient performance and avoid network congestion. Device-to-Device (D2D) Communication facilitates direct interaction between IoT devices, reducing reliance on centralized cloud servers and enhancing response times. Machine Learning and AI Integration in fog computing helps detect patterns, predict failures, and automate processes in real-time. These methods collectively improve efficiency, security, and responsiveness, making fog computing an essential paradigm for modern distributed systems:

Security and Access Control Mechanisms help protect sensitive data by implementing encryption, authentication, and anomaly detection to prevent unauthorized access. Resource Allocation and Load Balancing optimize the distribution of computing tasks among fog nodes to ensure efficient performance and avoid network congestion. Device-to-Device (D2D) Communication facilitates direct interaction between IoT devices, reducing reliance on centralized cloud servers and enhancing response times. Machine Learning and AI Integration in fog computing helps detect patterns, predict failures, and automate processes in real- time. Fault Tolerance and Failure Recovery mechanisms ensure system reliability by quickly detecting and responding to hardware or network failures. Scalability and Adaptive Computing allow fog networks to dynamically adjust resources based on demand, ensuring efficient performance even in high-load situations. Quality of Service (QoS) Management ensures optimal network performance by prioritizing critical tasks and minimizing delays. Energy-efficient Computing techniques optimize power consumption by distributing workloads efficiently across fog nodes. These methods collectively improve efficiency, security, and responsiveness, making fog computing an essential paradigm for modern distributed systems.

VIII. DATA MINING APPLICATIONS

Fog computing has a wide range of applications across various industries due to its ability to process data closer to the source, reducing latency and improving efficiency.Fog computing is transforming industries by providing efficient, secure, and real-time data processing capabilities



FOG COMPUTING FRAMEWORK

A fog computing framework provides the structure and components necessary for efficient edge computing, enabling seamless interaction between IoT devices, fog nodes, and cloud infrastructure. At the edge device (IoT layer), sensors, smart devices, and actuators generate real-time data for local processing and transmission. The fog nodes (processing layer) act as intermediate computing devices such as gateways, routers, and edge servers, handling data filtering, preprocessing, and analytics closer to the source. The cloud infrastructure (core layer) serves as the backbone for large-scale storage and advanced computational tasks, including deep learning and long-term data management. To facilitate communication, various protocols like MQTT, CoAP.

X. CHALLENGES OF DATA MINING

Fog computing, while offering significant advantages in reducing latency and improving efficiency in data processing near the source, also presents several challenges. One of the primary concerns is security and privacy, as fog nodes operate in a distributed environment, making them susceptible to cyber threats such as data breaches, unauthorized access, and malicious attacks.

Ensuring end-to-end encryption, authentication, and secure data transmission becomes complex due to the heterogeneous nature of fog networks. Additionally, resource management poses a significant challenge, as fog nodes have limited computational power, storage, and energy compared to centralized cloud servers. Optimizing the allocation of tasks while maintaining performance and energy efficiency is a critical issue. Another challenge is network reliability and scalability since fog computing relies on a vast number of geographically dispersed nodes, which may experience connectivity issues, failures, or delays in communication.

Interoperability between different devices, vendors, and protocols is also a concern, as the lack of standardization can hinder seamless integration and operation. Furthermore, the cost of deploying and maintaining a fog computing infrastructure can be high, particularly for organizations that need to invest in new hardware, software, and skilled personnel to manage these distributed systems. Lastly, latency-sensitive applications, such as those in healthcare or autonomous systems, require real-time processing with minimal delay, making it essential to balance computing load dynamically across fog nodes, which is a challenging task.

Addressing these challenges requires continuous advancements in security frameworks, resource optimization techniques, standardized protocols, and robust network management solutions to ensure the efficiency and reliability of fog computing systems.

XI. CONCLUSION

In conclusion, leveraging user behavior profiling to detect malicious insider threats in cloud environments presents a proactive approach to cybersecurity. By monitoring data access patterns and deploying decoy documents as sensors, organizations can significantly enhance their ability to identify unauthorized access attempts in real time. The integration of challenge questions adds an additional layer of verification, ensuring that only legitimate users can interact with sensitive data. Furthermore, the strategic use of disinformation technology to mislead attackers not only protects valuable information but also serves as a deterrent against future attacks. This innovative method enhances cloud security by making unauthorized data extraction efforts futile, ultimately reinforcing trust in cloud-based services and social networks. As cyber threats continue to evolve, such adaptive security mechanisms will be crucial in safeguarding digital assets and maintaining data integrity.

XII. ACKNOWLEDGMENT

I am deeply grateful to Mr. T. Pandu Ranga for his invaluable guidance, constant support, and encouragement throughout the completion of this research paper titled "FOG COMPUTING: An Extended Version of Cloud Computing." His insightful feedback and expertise have greatly enhanced the quality of this work.

I would also like to express my sincere thanks to Mr. S. Tirupati Rao, Coordinator at Geethanjali College of Engineering and Technology, for his continuous support and coordination, which made this research endeavor possible.

I extend my heartfelt gratitude to Geethanjali College of Engineering and Technology for providing an excellent learning environment and the necessary resources to accomplish this research.

Finally, I am thankful to the International Journal of Research in Computer Technology (IJRCT) for giving me the opportunity to publish my work and contribute to the field of database security.

REFERENCES

[1] Madsen, Henrik, et al."Reliability in the utility computing era: Towards reliable Fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. TEEE, 2013.

[2] Zhu, Jiang. *Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture*, Service Oriented System Engineering (SOSE), IEEE: 2013.

(3) Sabahi, F. "Cloud computing security threats and responses", In Communication Software and Networks (ICCSN), 2011 IBBE 3rd International Conference on 2011,pp. 245-249.

[4] Stolfo, Salvatore J., Malck Ben Salem, and Angelos D. Kcromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." Security and Privacy Workshops (SPW). 2012 IBEE Symposium on. IBEE, 2012

[5] Madsen, Henrik, et al. "Reliability in the utility computing era: Towards reliable Fog computing." Systems,
Signals and Image Processing (TWSSIP), 2013 20th International Conference on. IBEE, 2013

[6] C. Wei, Z. Fadlullah, N. Kato, and I. Stojmenovic. *On optimally reducing power loss in micro-grids with power storage devices." IBEE Joumal of Selected Areas in Communications, 2014 to appear.

[7] Bonomi, Flavio, et al. "Fog computing and its role in the internet of things." Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM. 2012, pp. 13-16.

[8] Claycomb. W. R., & Nicoll, A. "Insider Threats to Cloud Computing: Directions for New Research Challenges", In Computer Software and Applications Conference (COMPSAC), IEBE 36th Annual, July, pp. 387-
394. 2012
395.
(9] Park, Y., & Stolfo, S. J. "Software decoys for insider threat". In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, May, pp. 93-94, 2013.

[10] Ivan Stojmenovic & Sheng Wen ." The Fog Computing Paradigm: Scenarios and Security Issues" In Proceedings of the 2014 Federated Conference on Computer Science and Information Systems pp. 1- 8.