ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Handling Encryption and Data Loss prevention in the Cloud-Based Systems

Venkat Soma

New York Mets

ABSTRACT

The current study focused on assessing the handling encryption and data loss prevention in the cloud. Cloud-based systems also known as cloud computing, increase organisational efficiency for proper data management processes. Cloud-based data loss or leakage prevention (DLP) improve data visualisation; hence, the companies can understand the risks and issues through proper data management. This study highlighted the way handling encryption and data loss prevention in the cloud can be useful for the development of business processes and for managing all operations through proper data management. IoT-based and AI-based cloud computing assess root causes and provide a clear insight into business problems. Hence, they can improve their data loss risk management services and promote continuous improvement.

***Corresponding author**

Venkat Soma, New York Mets, USA.

Received: August 12, 2024; **Accepted:** August 19, 2024; **Published:** August 26, 2024

Keywords: Cloud-Based System, Handling Encryption, Data Loss Prevention, DLP, Cloud Computing, Risk Management, Information Management

Introduction

Cloud-based systems are crucial for the development of modern operations in each section of businesses. This is one of the advanced technologies that look into developing the delivery activities of any service or product, in that case, cloud computing assists in regular monitoring and observation of all operations in a company. "Cloud data loss prevention" (DLP) is an advanced solution for data management; it will be beneficial for efficient data management in a hybrid working culture. The cloud-based system is also known as cloud computing which makes an organisation or an entrepreneur more productive in their working sector. "Data classification", "pattern matching" and "machine learning" is used to accurate identification and safeguard to critical information. This system is supported by artificial intelligence (AI), which improves successful data security and management. The monitoring and observational operations are managed crucially based on the actions taken, the responsibility taken by different persons, the use of networks, and changes in the environment. It improves the traditional data loss prevention processes. Hence, the cloud system required proper design to gain proper insight from the monitoring and observational activities. For this reason, this research paper focuses on analysing the use of data loss prevention and handling encryption which can assist in the development of the business processes and operations through its cloud-based monitoring and observability.

Problem Statement

Cloud monitoring and cloud observability are systematic processes which investigate monitoring the reality and generated data. These increase observability in the organisational processes. Cloud data loss prevention (DLP) refers to a range of solutions that secure sensitive data stored in an organization's cloud storage against abuse or leakage. Traditional data loss prevention solutions are often implemented on-premises and focus on safeguarding an organization's endpoints and internal network architecture. This is also required for the development of reliability and optimal performance of the cloud resources. This tool increases the reliability and availability of specialised tools; their usage provides critical alerts and insights about the status and health of cloud computing. Cloud monitoring is also a crucial part of the security management of an organisation [1]. "Cloud DLP" is now part of "Sensitive Data Protection", a suite of services designed to assist companies in discovering, classifying, and safeguarding their most sensitive data. "Data discovery, inspection, de-identification, data risk analysis, and the DLP API" are all components of sensitive data protection approach [2].

Furthermore, when the concept of cloud observability comes, it investigates the capability to monitor and analyse the necessary logs which were generated by the internal system. Proper monitoring and analysis provide a company with adequate insight. Observability in a cloud system indicates a proper understanding of the service and system in the overall operation, which will have the capability to make queries and generate relevant and novel data. In this concern, cloud observability tracks the actions, and identifies the transit on any network. Moreover, it selects the information, which is necessary for risk management and design processes. These functions of monitoring observability allow an organisation to prepare a design process [3]. The cloud system improves communication technologies through advanced sensors and better signal processes. IoT devices and senses increase the industrial visibility of all information. Here, individual processes maintain high quality and standard of work. The IoT-based technology in the cloud system is associated with the detection of uncovering problems.

IoT-based cloud computing is beneficial for data visualisation. Increased data visualisation can generate random data which can be connected to the web application framework. Data encryption is cloud algorithm process using big data analytics and IoT. "Hierarchical identity-based encryption" (HIBE) and "cipher-text policy attribute-based encryption" (CP-ABE) are two algorithms to prompt the use of data [4]. The study mentioned that visualisation and monitoring activities will be crucial for effectively keeping the software's behaviour [5]. The cloud-based system strengthens software performance by maintaining cost and quality. Regular monitoring and visualisation of information is crucial to consider these as one of the most efficient ways to continue the checking processes on the processes of software. Here, the cloud-based monitoring tool with regular data assists one in understanding the complexity and behaviour of the collected data. As a result, it eases in drawing conclusions and making necessary decisions at the end.

Data encryption uses supportive and distributed tracing techniques to trace, monitor, and control micro-service-based distribution applications of "International Data Corporation". It promotes distribution-based assessment and information management; hence, it can be controlled by cloud computing orchestration platforms. Cloud computing's control, flexibility, and convenience of use are coupled with several security risks. According to the International Data Corporation's assessment, security is regarded as the most significant of the nine identified difficulties of cloud computing. As a result, a highly secure system is required to protect an organisational entity, its resources, and assets [6]. There are various "open-source container orchestration platforms" such as Docker Compose and Kubernetes. Their monitoring aspects look into managing the deployment of distributed applications for the usage of resources based on the application components. Hence, these mechanisms do not support any sophisticated monitoring services. Again, the nature of distributed application, as well as metric observation can be related to the interactions among the components of the applications [7]. In addition, handling encryption and "data loss prevention" (DSP) require proper logging machines and distributed tracing machines so that third-party intrusions can be monitored and restricted. Hence, these issues need to be resolved for the betterment of the application and software services in an organisation.

Solution

The recent years experienced a huge integration of online operations to enhance the operational fields from traditional to digital. In that case, the companies felt an increasing need to secure the data, along with managing the digital operational fields. Operational security and technical complexities can be managed by implementing cloud computing processes. Data Loss/leaking Prevention (DLP) refers to the security procedures used by companies to prevent the leaking of personal and sensitive data (PII). ISACA® recommends data security methods to assure confidentiality, integrity, and availability. Metrics are chosen based on subject matter expertise, industry best practices, professional standards, frameworks, and legislation [8]. Hence, cloud security practices can be promoted through the development of risk mitigation processes through cloud security requirements. Risk controlling features, such as ISO 27002 is an international standard which promotes risk management approaches. These are useful for increasing good security controls in the IT sector [9]. The cloud ecosystem allows the local government and other stakeholders to collect information on the risks regarding contractual and legal requirements. As a cloud-based security system, an organisation can incorporate the safety parameters in its technological and business requirements through advanced Cloud DLP and data encryption.

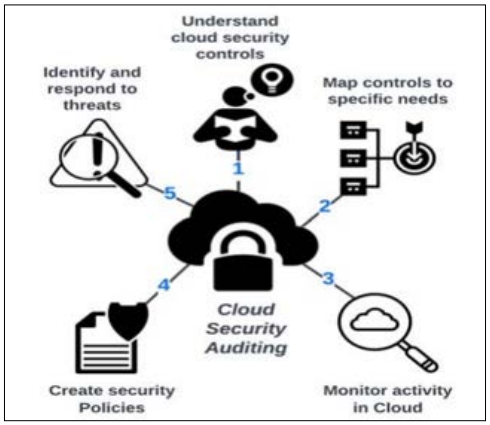

Figure 1: Auditing in Cloud Security Management Processes [10].

Cloud systems can be used in a diverse range of activities in different management activities. Cloud computing is crucial in developing smart cities; smart communication, smart networks, and smart traffic control are promoted by the effective use of cloud-based systems in each system. In that case, controlling traffic between different cloud services ways can be conducted through ingress or egress traffic management services. This process can be beneficial for developing data protection protocols from data theft issues or unauthorised actions of data management. This is crucial to prevent data leakage in any multi-cloud providing services; hence, the multicult providing services need to encrypt both transcript and rest programmes [10]. Again, the cloud auditing system is another positive section which can increase security systems through eminent data protection activities. Cloud security auditing can understand the cloud security controls, and map the controls to special needs; it can monitor all the activities in the cloud system. Based on the identified issues, the cloud system allows an organisation to create further security policies. It can identify and respond to all the risks properly [mentioned in Figure 2]. The most important advantage of the cloud management system is data protection. To be more prompt, an individual or an organisation can secure necessary data from phishing and theft issues. In the current business processes and operational practices, online order and digital payment systems are quite common. Hence, both the sellers and buyers are required to input their personal information; now, the cloud "data loss prevention" needs to secure that information from third-party intrusion. Captcha breaking and Google hacking are some threats to data breaches in network traffic management and transport protocols. "Domain name server" (DNS) is also crucial for the development of business processes regarding significant network security [11]. "Internal protocol" (IP) addresses and "file allocation table" (FAT) are used to secure information from a malicious insider attack.

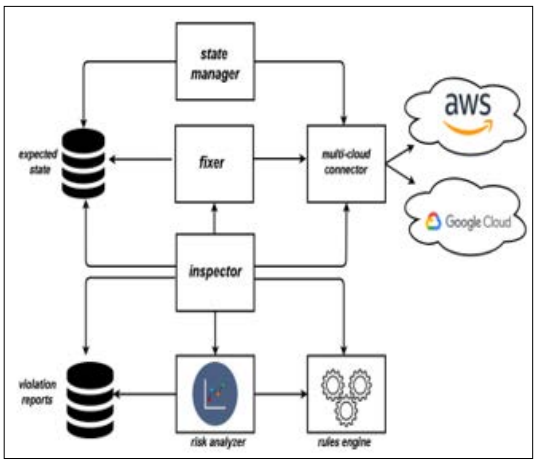

Figure 2: High-Level Architecture of CSB Auditor [12].

The study of [8] mentioned that CSB Auditor can be implemented to reduce the security threats from the private cloud computing protocols and increase service validity. In this concern, architectures and APIs of the cloud service providers (CSP) can enrich the monitoring and surveillance activities. Continuous auditing in the multi-cloud system can detect the issues in software and promote safety and security concerns in the additional activities. A CSB Auditor Dashboard can show the expected state, cloud state and summary of all alerts based on the information on security from CSP. The state manager's initiatives manage "Google Cloud Storage" (GCS) which provides security alerts for any violation. On the other hand, the "Rules Engine" specifies the audit check detail in two categories, such as "enterprise security rules" and "compliance rules". These look after the operation of all buckets of the cloud system; here, the storage auditor and iam auditor systems work as a part of the CSB Auditor [12]. It reads and writes permission to retrieve the cloud system activities and the respective cloud connector interface. Amazon's AWS and Google's Google Cloud also use multi-cloud connectors to conduct a high-level architecture of CSB Auditor; here, the use of inspector and fixer works for risk analysis and rule engine. The violation report works with the development of the business processes and the management of the internal data [mentioned in Figure 2]

Uses

The cloud system can be used for the development of business processes through transparency and clarity in the internal management approaches. An openable "black box" can be used for reflectional transparency management. Here, the panacea is used as a controlling platform; it increases data encryption handling which is required for the development of dealing with system-based problems. In addition, Cloud DLP allows for studying complex systems of a company, which assesses the development of the business processes through the principal concerns of analytical and normative scope. It increases the learning and knowledge generation among the users; in this concern, the data encryption system increases observability in the cloud computing structure. The "Black Box Society" increases "intelligibility" for transparency and provides remedies for unauthorised access. In all organisations, 'transparency practices do not simply make organizations observable, but actively change them' to generate visibility [13]. On the other hand, micro-service management approaches are crucial to maintaining micro-service tracing and analysis activities. A large microservice system requires proper analysis after tracing. To assess the operational efficiency, visualisation and statistical metrics can be developed through the information from regular and continuous surveillance. Cloud computing can be strengthened by its collaboration with machine learning, big data, and data mining aspects. Hence, the companies can use their existing as well as new issues to utilise the business opportunities [14]. It requires proper data analysis and improves industrial data visualisation. At first, the service is analysed by logging; the data collection process is done by monitoring and observational activities. After processing the data, core information is stored for further analysis and usage [Mentioned in Figure 3].

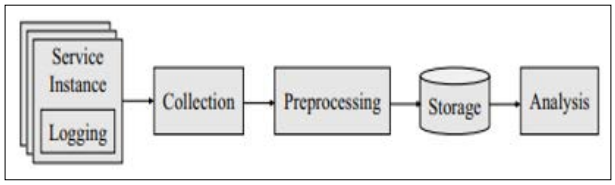

Figure 3: The use of Cloud Computing in Microservice Tracking and Analysis Pipeline [14].

The cloud-based system and internal improvement can be used in information management activities. In order to promote industrial monitoring activities, people will focus on the development of data management and internal controlling processes. Industrial decision-making processes are based on internal information on the investors, employees, customers, suppliers, and other stakeholders. Here, automation and responsive activities are conducted through crude technologies. Cutting-edge technology for industrial adoption is crucial for the development of internal cloud monitoring systems. The use of multiple tools and multi-level cloud monitoring systems improved the issues in data protection and future usage. S cloud computing facilitates cloud computing services, which promotes technological advancements. The high expertise uses the front-end and back-end measurement data; their use of monitoring tools allows them to implement custom solutions to each issue [15]. As a result, "problem detection and diagnosis" along with "measuring business value" is crucial for managing internal assessment.

Impact

DLP of the cloud-native application improves the internal organisational management processes. The handling encryption proceeds step-by-step; in the first step, it conducts a data analysis and visualisation. Data backends and data collectors control telemetry data through metrics, logs, and traces; these are the data that a cloud system uses. In the next step, the instrumentation occurs. Cloud-native applications and execution environments allow for micro-service programming analysis. In addition, the orchestration of system and container runtime is a crucial step. The last step analyses the commuting information, storage and the network system [16]. Hence, it can be mentioned that improvement in promoting cost efficiency, time management, compliance, safety and security management, and customer happiness, increases business values [15]. Analysing the root causes and discovering the unknowns assists an organisation in identifying threats. This step progresses to data encryption and management based on data algorithm is mentioned in Figure 4.

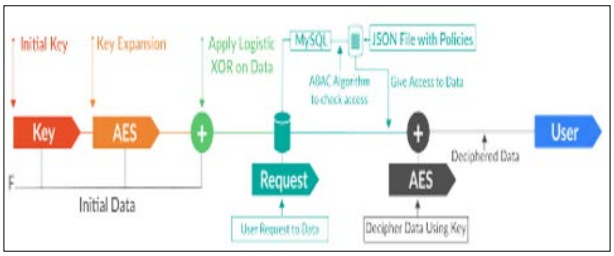

Figure 4: Algorithm for Data Access and Data Algorithm [4].

The attacker gains control of cloud providers through command-and-control before launching assaults. In this instance, 5000 assaults were created. The cloud computing server utilises an IDS algorithm to detect and block malicious activity and requests [4]. The study of categorises the cloud-based system performance of monitoring and observationally is crucial in two crucial parts; those are "open-source software", and "closed source software" [17]. The former is beneficial for open-source monitoring and observation. In the cutting-edge technology solution, Grafana and ELK Stack are important. These assessments in understanding the query, and visualisation of the present condition. As a result, this system can alert a company to risky situations. The latter actions also promote aid-based services after discovering the issues in the server.

Scope

Data loss prevention considers the combination of different types of signals, such as logs, metrics, and traces. These signals can be monitored and continued with the trade-off between the accessibility of rich information or data, and the complexity or performance aspects. The identification of the sets of information increases efficiency in data collection processes. It will increase the efficiency of the visualisation of data to improve a cloud-based information management system [18]. There are CPU usage, memory usage, in or out traffic, and served requests per second; these time-based data increase organisational efficiency [mentioned in Figure 5].

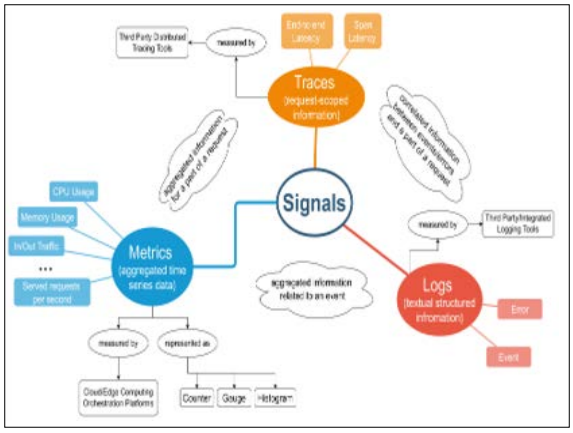

Figure 5: Different Signals into Logs, Metrics, and Traces [18].

The use of IoT-based infrastructure and its improvement can be conducted based on comprehensive monitoring coverage, real-time data processing, advanced data visualisation techniques, flexibility and scalability, and improving security and privacy management.

Table 1: Scope of Improving Security in Data Management Processes for Monitoring and Observability; Based on [19-21].

Comprehensive Monitoring Coverage	Future cloud-to-thing (C2T) applications necessitate data encryption systems that provide comprehensive coverage across diverse layers of the computing stack. This includes assessing cloud infrastructures, edge devices, and the communication networks connecting them [19].
Real-time Data Processing	The dynamic nature of C2T environments demands real-time data processing capabilities. Cloud DLP systems must be able to collect, process, and analyse data streams in real time to detect anomalies, predict potential issues, and trigger automated responses
Advanced-Data Visualization Techniques	Effective visualization techniques are required to present this data in an intuitive and actionable manner. The use of dashboards, heat maps, and trend analysis tools helps stakeholders quickly identify patterns, correlations, and outliers, facilitating faster decision-making and problem resolution [20].
Flexibility and scalability	Cloud DLP systems must be scalable to handle the growing volume of data generated by an increasing number of connected devices and applications. They should also be flexible enough to adapt to different use cases and requirements, supporting a variety of data sources, protocols, and analytics frameworks and managing time efficiency [20].
Security and privacy management	This includes ensuring secure data transmission, storage, and access controls, as well as compliance with relevant regulations and standards [21].

Such improvement increases opportunities in internal security management in all industries. The study of mentioned that monitoring and observability in cloud-based systems can improve hospital services in managing the records of patients and their histories [22]. These are also crucial for securing health insurance information and services. As a result, the companies can implement robust risk management plans that can improve healthcare services. This is the same for all organisations from all industries.

Conclusion

This study highlighted the way cloud computing can be used by its monitoring and observability. It will be beneficial for the development of organisational activities; now, the era of digitalisation increases the risks of data theft and third-party intrusion. Use of data encryption and Cloud DLP can promote cost and time efficiency in organisational tasks. Furthermore, proper identification of the risks and risky situations allows the companies to take necessary measures and robust risk assessment strategies to cope with those situations. This also allows organisations to utilise the market opportunities of increasing reliance and loyalty of all customers. All these are possible through efficient data management processes cloud-based systems.

References

1. Ogiela L, Ogiela MR, Ko H (2020) Intelligent data management and security in cloud computing". Sensors 20: 3458.
2. Google Cloud (2024) Cloud Data Loss Prevention (now part of Sensitive Data Protection) Google Cloud. https://cloud.google.com/security/products/dlp.
3. Ahmed T, Qureshi HA, Kaleem M, Nazir S (2021) Event monitoring and observability for industrial systems on azure cloud. In 6th International Electrical Engineering Conference. The Institution of Engineers Pakistan, April 2021. Available at: https://researchonline.gcu.ac.uk/ws/portalfiles/portal/43907404/Ahmed_T._et_al_2021_Event_monitoring_and_observability_for_industrial_systems_on_Azure_cloud.pdf.
4. Razaque A, Shaldanbayeva N, Alotaibi B, Alotaibi M, Murat A, et al. (2022) Big data handling approach for unauthorized cloud computing access. Electronics 11: 137.
5. Abbasi MB (2021) Observability of Industrial Data using an Analytics and Monitoring Platform. Available at: https://trepo.tuni.fi/bitstream/handle/10024/136292/AbbasiMuhammadBilal.pdf?sequence=2,
6. Seth B, Dalal S, Jaglan V, Le DN, Mohan S, et al. (2022) Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies 33: e4108.
7. Tzanettis I, Androna CM, Zafeiropoulos A, Fotopoulou E, Papavassiliou S (2022) Data fusion of observability signals for assisting orchestration of distributed applications. Sensors 22: 2061.
8. Omodara H (2022) Cloud security: A survey of Information Communication Technology (ICT) and cybersecurity professionals' perception on Data Loss Prevention (DLP) measures for Software-as-a-Service (SaaS) application-related data breaches and leakage. https://www.academia.edu/download/92532251/Cloud_Security_A_survey_of_ICT_and_Cybersecurity_professionals_perception_on_DLP_measures_for_SaaS_breaches.pdf.
9. Ali O, Shrestha A, Chatfield A, Murray P (2020) Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly 37: 101419.
10. Achar S (2022) Cloud computing security for multi-cloud service providers: Controls and techniques in our modern threat landscape. International Journal of Computer and Systems Engineering 16: 379-384.
11. Aljumah A, Ahanger TA (2020) Cyber security threats, challenges and defence mechanisms in cloud computing. IET communications 14: 1185-1191, 2020.
12. Torkura KA, Sukmana MI, Cheng F, Meinel C (2021) Continuous auditing and threat detection in multi-cloud infrastructure. Computers & Security 102: 102124.
13. Rieder B, Hofmann J (2020) Towards platform observability. Internet policy review 9: 1-28, 2020.
14. Li B, Peng X, Xiang Q, Wang H, Xie T, et al. (2022) Enjoy your observability: an industrial survey of microservice tracing and analysis. Empirical Software Engineering 27: 1-28.
15. Tamburri DA, Miglierina M, Di Nitto E (2020) Cloud applications monitoring: An industrial study. Information and Software Technology 127: 106376.
16. Kosińska J, Baliś B, Konieczny M, Malawski M, Zieliński S (2023) Toward the observability of cloud-native applications: The overview of the state-of-the-art. IEEE Access 11: 73036-73052.
17. Usman M, Ferlin S, Brunstrom A, Taheri J (2022) A survey on observability of distributed edge & container-based microservices. IEEE Access 10: 86904-86919.
18. Tzanettis I, Androna CM, Zafeiropoulos A, Fotopoulou E, Papavassiliou S (2022) Data fusion of observability signals for assisting orchestration of distributed applications. Sensors 22: 2061.
19. Volpert S, Eichhammer P, Held F, Huffert T, Reiser HP, Domaschka J (2023) The view on systems monitoring and its requirements from future Cloud-to-Thing applications and infrastructures. Future Generation Computer Systems 141: 243-257.
20. Kobi J (2024) Developing Dashboard Analytics and Visualization Tools for Effective Performance Management and Continuous Process Improvement. 9: 1697-1709.
21. Patwary AAN, Fu A, Naha RK, Battula SK, Garg S, et al. (2003) Authentication, access control, privacy, threats and trust management towards securing fog computing environments: A review. arXiv preprint arXiv:2003.00395. Available at: https://arxiv.org/pdf/2003.00395.
22. Shah V, Konda SR (2022) Cloud Computing in Healthcare: Opportunities, Risks, and Compliance. Revista Espanola de Documentacion Cientifica 16: 50-71.