Materials Today: Proceedings 62 (2022) 4828–4836

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Cloud security framework and key management services collectively for implementing DLP and IRM

Shahnawaz Ahmad [a,*], Shabana Mehfuz [a], Javed Beg [b]

[a] *Department of Electrical Engineering, Jamia Millia Islamia (A Central University), New Delhi-110025, India*
[b] *Oracle, Noida, Uttar Pradesh, India*

ARTICLE INFO

Article history:
Available online 30 March 2022

Keywords:
Data Loss Prevention
UNIX
MySQL Server
Data Loss Management

ABSTRACT

A free and open-source framework management solution can help organizations as well as end-users. An agentless, completely controlled, centrally administered, and freely distributed source, cloud-based data leak control includes enhanced data loss protection management for both corporations and end-users. An Open-Source Framework in the cloud zone was used to construct the data loss prevention tool. This framework can be released under an Open License or a Free License, making it freely usable by end-users throughout the world. You can run it on any of these platforms: Linux, Windows, or UNIX. It relies on open database connectivity and MSSQL credentials for its database connectivity, although MySQL Server is used for database connectivity. As many as hundreds of individual files or thousands of multiple files can be accessed simultaneously by the Open User Data Loss Management Console, which can identify the case-sensitive information among them.

1. Introduction

The unauthorized leaking of sensitive information from a corporate network or database [1] is a huge hazard to organizations. Confidential information might jeopardize a company's ability to compete. Even if no sensitive personal data is exposed, a firm's image can be negatively affected by data breaches, especially if customers perceive the organization to be dishonest. Insider threats are the most common cause of data leaks [2,3]. The use of Data Loss Prevention (DLP) solutions is a common defense strategy to reduce the risk of data breaches. Unauthorized disclosure or improper use of confidential data can be detected with DLP technologies [4]. To distinguish between approved and harmful transactions, DLP systems keep a model of either allowed (whitelisting) or malicious (blacklisting) behaviour. This model can be defined by an expert's knowledge or previous transactions.

Cloud computing adds an element of risk to the development of secure IT systems since vital functions are frequently outsourced to a third party. To demonstrate compliance and ensure data security, availability, and integrity are all hampered by outsourcing's "externalized" nature. Because of this, the control over data and operations passes from the client organization to their cloud suppliers. Patching and setting firewalls, for example, might be delegated to the cloud service provider rather than the end-user. Customers must build confidence with their service providers and understand the risks associated with how these providers implement, install, and maintain security on their behalf. When it comes to outsourcing, some companies choose to use private or hybrid models rather than public clouds. Many other areas of cloud computing must be re-examined in terms of risk and security. In the cloud, finding where data is stored might be tricky [5]. Layers of abstraction have obscured previously visible security mechanisms. Many security and compliance issues might arise as a result of this lack of visibility.

As a result, cloud security is vastly different from traditional IT security because of the huge sharing of infrastructure. But as IT infrastructures become more dynamic, there is greater potential for malicious activity and data compromise due to factors such as workload balancing and shifting service-level agreements. As a result of the increased automation required by infrastructure sharing, the danger of operator mistakes and oversight can be reduced, hence improving security. Cloud computing models, on the other hand, must still place a heavy emphasis on isolation, identity,

[*] Corresponding author.
E-mail address: shahnawaz98976@gmail.com (S. Ahmad).

https://doi.org/10.1016/j.matpr.2022.03.420
2214-7853/Copyright © 2022 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Conference on Innovative Technology for Sustainable Development.

and compliance because of the hazards inherent in a massively shared infrastructure [6].

1.1. Cloud data security issues

Data security is one of the most important cloud security concerns. The security of data at rest and the security of data in transit are two of the most important aspects of moving data to the cloud. Many distinct types of cloud data exist, including user identity, audit, runtime, and application data. Security needs to be provided depending on the type of data. For very sensitive data, such as a user database, security must be extremely high. If the data is merely a user's name and password, a privacy guarantee is all that is needed. The security implications for the user will differ depending on the value and type of data. A cloud system's data security architecture is depicted in Fig. 1. Authentication, Confidentiality, Integrity, Scalability of Keys, Access Control, Policy, and Compliance are some of the data security concerns associated with the cloud (CSA 2009).

Confidentiality is critical for Cloud data due to features such as multitenancy and remote storage as well as third-party cloud providers and huge data exchange. When it comes to ensuring the privacy and security of all of your data, encryption is vital. One of the most difficult aspects of encryption is distributing and maintaining the many sets of encryption and decryption keys. There must be no tampering with the data at rest or in transit to ensure that it is secure. There must be a way for cloud customers to verify the integrity of their data while it is in transit or at rest [7]. Because the data is stored in the cloud, it is more susceptible to alteration by other cloud users. An integrity method that allows for frequent integrity checks, third-party audits, and dynamic data is necessary.

1.2. Key management

The study of securely transmitting and receiving data via a public channel is known as cryptography. The algorithm and the key are the two essential components of cryptography. Encryption is done using an algorithm, which is a type of mathematical procedure used to encrypt data using a key as a parameter of the algorithm itself. Encryption and decryption are two of the algorithmic aspects of cryptography that deal with the conversion of plaintext to ciphertext. The development and distribution of a cryptographic key are fundamental to encryption, just as encryption is fundamental to computer security. While encryption methods are tough to crack, the cryptographic key is an obvious target for hackers. Encrypted files and sessions can be decrypted by anyone who has the cryptographic key [8]. As a result, the key (and its handling) must be as secure as feasible. For a system to be secure, both the development and distribution of strong keys must be done correctly. Key production, updating, distribution, and deletion are all part of key management, which is now a critical responsibility. An application that is designed to be used by multiple people uses group keys to share common data, while session keys are used to pass information back and forth. Key production, updating, distribution, and deletion are all handled by Group Key Management (GKM).

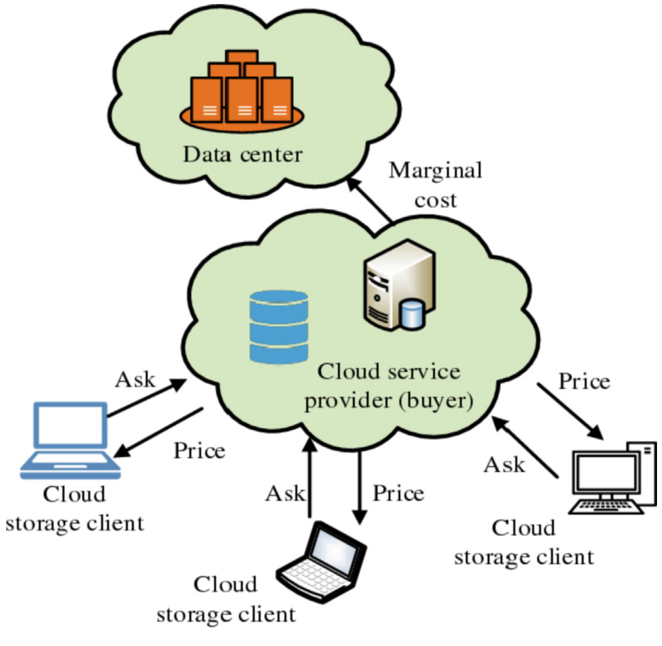


Fig. 1. The data security architecture of cloud.

1.2.1. Group key management

Scalability, forward secrecy, backward secrecy, Key independence, Collusion resistance, Trust relationship, and Resilience are some of the security and performance criteria for efficient group key management in the cloud. When it comes to cloud data sharing, there is a lot of movement in the group dynamics. As the size of a group grows, the group key management system must be capable of handling this growth without sacrificing efficiency. The group key should be changed whenever a member enters or departs a group. The member who quits the group is denied access to the group's data, and the data cannot be decrypted once the individual leaves the group. Backward secrecy prohibits new members' access to the group's old data. It prevents new members from accessing data that was previously encrypted [9]. The complete keying material must be independent of each other for a GKM to preserve key independence. Because of this, the GKM must be strong enough not to allow expelled or expelled members to construct the key, thus guaranteeing the freedom of collaboration. Putting too much faith in a large number of communication entities is essential. Group key management should be deployed and evaluated using a threat model and security analysis. Every time a member enters or leaves the group, the distribution of group keys must be efficient. Key rekeying processes must be accelerated and improved in terms of speed and efficiency by reducing communication and computation costs, as well as key storage costs, as a result of the GKM operational requirements.

1.2.2. Key generation

By seeding the HSM or TTP with a cryptographically secure True Random Number Generator, a key management system can generate the necessary keys for both entities. The keys can also be produced using cryptographic procedures. The keys and their properties will subsequently be placed in the database of the key store. Name, activation date, size, and instance are only some of the attributes that can be assigned to an object. A key can be activated immediately, or it can be scheduled to be activated at a later date. An appropriate level of security for the data being secured and the ability to survive attacks throughout its useful life should be assigned to each key. This level of protection is often measured in bits. The algorithm will dictate the length of the key. Because of its high level of security, asymmetric cryptosystems implementing asymmetric algorithms are commonly employed for the distribution of session keys [10]. As a result of their small key lengths and ease of use, ECC is the most popular choice for encryption and decryption. Compared to RSA and Elgammal crypto schemes, the ECC algorithm is more appealing in the cloud because of its high-security level.

1.2.3. Key distribution

Data on the cloud is being shared by an ever-increasing number of people at the same time that they are leaving the group. When a user joins a group, the cloud provider or a trusted third party like a Security Manager distributes a group key and a private key to him (SM). Changing the group key when a user enters or leaves the group ensures forward and backward secrecy. All other users must be given the new group key. On the subject is how to distribute this Group key securely while safeguarding it from outsiders, how to handle frequent key changes, and how to overcome a break in the key-distribution strategy The cloud's group key management system relies heavily on the distribution of group keys. There are three main types of group key management schemes: central, decentralized and distributed.

In this paper section, 1 introduces key management techniques and cloud security issues and section two gives a brief discussion of the Data Loss Prevention system, and then section 3 gives the idea of Information Right management. Section4 explains the related work about this work and the proposed methodology explained in the 5th section. Finally, results are given in the 6th section and the work is concluded.

2. Data loss prevention / data leak prevention

Data loss prevention (DLP) solutions attempt to protect sensitive information in various ways. It is possible to locate or classify sensitive material while it is still in storage by scanning file servers and endpoints.

Even when sensitive information or documents are in transit, such as on a network or a removable storage device. It's also important to keep track of who has access to the data while it is being used [11]. Hackers typically use pre-established dictionaries to search for information on a person's financial status, intellectual property, and other valuable assets. Data Loss Prevention for all data types is indicated in Fig. 2.

To put it plainly, DLP is like a "policeman" stationed outside of the network's perimeter to keep an eye out for what is attempting to exit and who is doing it. For sensitive data that violates a business guideline, it also checks for it in network repositories.

This is a strong technology; however, securing sensitive information is a major challenge:.

- How does it know what's allowed to depart and what's not?
- Is it feasible to effectively "close" or control all of the available egress points of firm data?
- The cloud, mobile phones, and other devices used by the business: are these all within my control?
- Where does "the policeman" go if something breaks free from his grasp and leaves the network? Is there a way to limit who has access?

Conventional data loss prevention (DLP) systems are limited in what they can do. It is a one-to-one relationship. There is no "binary" in everyday life. Defining policies that clarify the requirements for data to properly leave the organisation without generating a high number of "false positives" might be difficult for an IT expert. It's tough to reply appropriately if the data or information isn't classified [12]. Classifying the data is often necessary before the DLP can begin scanning any repositories and determine what should be treated as confidential and what shouldn't.

As a result, the DLP configuration, classification, and policy management processes must be rigorously tested by the IT department to ensure the lowest possible number of false positives. Remember that an IT department may have a tough time determining what information is sensitive and what is not. This data belongs to the people who interact with it regularly, and they are the ones who can tell you what's important and what isn't.

Another issue is how the documents are used after they are distributed. There is nothing stopping receivers from forwarding or saving the data on USBs or other removable media once it has left the enterprise. This is true for mobile devices as well, where secu-

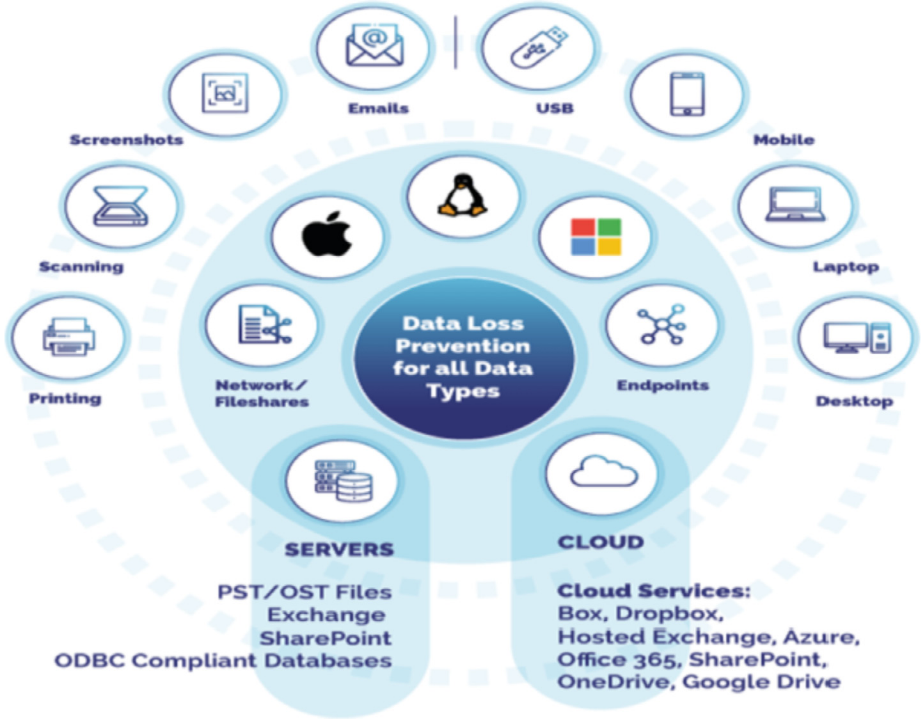


Fig. 2. DLP Program.

rity is often viewed as "all or nothing." Data on mobile devices is frequently delegated to MDM software by businesses to prevent unauthorized access or use.

Companies usually start with a "monitoring" phase to determine what type of data leaves the network before moving on to a "blocking" phase, which necessitates stricter policy and categorization administration. As a result, blocked processes will not cause false positives if the policy is improved. Data that should be available or communicated may be blocked, resulting in substantial noise in the company [13].

While DLP solutions can identify, monitor, and limit sensitive data transmission on the network, they can't prevent it, the effort required to put them in place and keep them refined while avoiding false positives should not be underestimated. Last but not least, data can be transmitted anywhere while still being protected at the network's "perimeter.".

The DLP is used to prevent sensitive data from being lost, misused, or accessed by unauthorized individuals. When it comes to regulatory compliance like HIPAA, PCI-DSS, or GDPR, data loss prevention (DLP) software can identify and classify regulated, sensitive, and business-critical data. Alarms, encryption, and other safeguards are used in detection and response to prevent end-users from revealing sensitive information that could harm the company's reputation mistakenly or maliciously. Software and solutions that monitor and regulate endpoint behaviour, filter data streams on corporate networks, and monitor data in the cloud are all used to prevent data loss. Additionally, DLP can be utilized for forensics and incident response in addition to reporting for compliance and auditing.

2.1. Use cases for DLP

When it comes to protecting personal information and intellectual property, data loss prevention (DLP) is an essential tool for many enterprises.

2.1.1. Personal information protection / compliance

Some of the kinds of information that your organization collects and stores are PHI (Personal Identifiable Health Information), PCI (Payment Card Information), and others. This means that you may be subject to regulations like "HIPAA (for PHI)" and "GDPR (for EU residents' data)" requiring you to safeguard the private information of your clients. Using a DLP, you may find and classify sensitive information, and then keep track of the events and actions that are connected to it. Compliance audits are also possible with the reporting tools.

2.1.2. IP protection

Your company's finances and reputation as a trusted brand could be harmed if your intellectual property, trade secrets, or state secrets are stolen. Intellectual property can be classified in both organised and unstructured forms using DLP technologies like Digital Guardian. By creating regulations and controls, you can prevent this data from being leaked unintentionally [14].

2.1.3. Data visibility

Do you want to be able to track the flow of data in your business better? Endpoints, networks, and the cloud can all be part of a comprehensive enterprise DLP solution. You'll be able to see how employees in your company interact with data if you do this. These are only three of the many uses for data loss prevention (DLP), but they may also be used to address issues such as "insider threats", "Office 365 data security", "user/entity behaviour analysis", and more.

3. Information Rights management (IRM)

When it comes to Data-Centric Security, this technology allows for the application of protection to files that travels with the files. "Enterprise Digital Rights Management" or "EIP&C" is another name for it (Enterprise Information Protection & Control) [15]. This application allows you to keep track of who has access to your files when they're accessed, and whether or not anyone is trying to access them without your permission. Permissions can also be set for documents. If you don't want specific people to be able to access a file again, you can revoke access to it in real time.

In just three minutes, your paper may have been printed, forwarded to five other individuals, forwarded to another ten people, and altered by all of them. When we develop a document, we own it, but when we share it, we no longer own it and the recipient can do with it what they please. To ensure that the data is owned by the user, regardless of who has shared it with, this technique tries to address it. IRM process is explained pictorially in Fig. 3.

As a result, the IRM has established a policy to protect data even when it is no longer on the network, whether it is saved in the cloud, on a mobile device, or elsewhere. If someone has gained access to data that they shouldn't, it might be blocked. An expiration date can be added to documents. If we don't want a user who can only read to have the option of editing or printing a document, we can grant them real-time permissions (e.g., allow them to edit when they were previously only allowed to read). Convenience in implementation, however, allows you to begin utilizing this solution immediately and encrypt and manage the data that your organization handles internally or with third parties, which is a benefit.

Making this technology user-friendly so that users can manage protected data virtually as if it were unprotected data, is a huge challenge. These include apps like "Office", "Adobe", and AutoCAD"; "file servers"; "SharePoint"; "Office 365 Cloud applications"; "G-Suite"; and "Box" etc. ensuring that everything is compatible. In addition, IRM systems must deal with the issue of automatic defence [16]. However, regardless of the user's decision, the protection of information. In this case, folders on file servers or document management systems could be really useful.

4. Related work

The use of many new technologies has grown increasingly widespread as Internet technology has developed at such a rapid pace. Big data and cloud computing are advancing at a breakneck pace, and they are proving to be invaluable tools for streamlining data storage and management. However, in the large data cloud computing environment, the data system itself has some data security issues. Big data cloud computing environments need to be studied to increase people's information security during the data processing and integration process. Data and information security issues can only be addressed in this manner, and the reliability and security of data transmission can only be improved this way.

Insider risks for data theft are considered to be one of the most serious threats by many organizations. An insider can inadvertently unintentionally divulge important information (Social engineering has resulted as a result of this) Systems that monitor the content and environment in which sensitive information is exchanged, such as in a "file system", "an email server", "instant messaging", are known as data leakage prevention systems. M. Kiperberg et al. developed Efficient DLP-Visor, a context-sensitive DLP system (2021). They intercepted system calls in Windows operating systems with Kernel Patch Protection enabled using DLP-visor, a thin hypervisor. As long as DLP-Visor is running, no sensitive data will ever leave a preset set of directories, whether

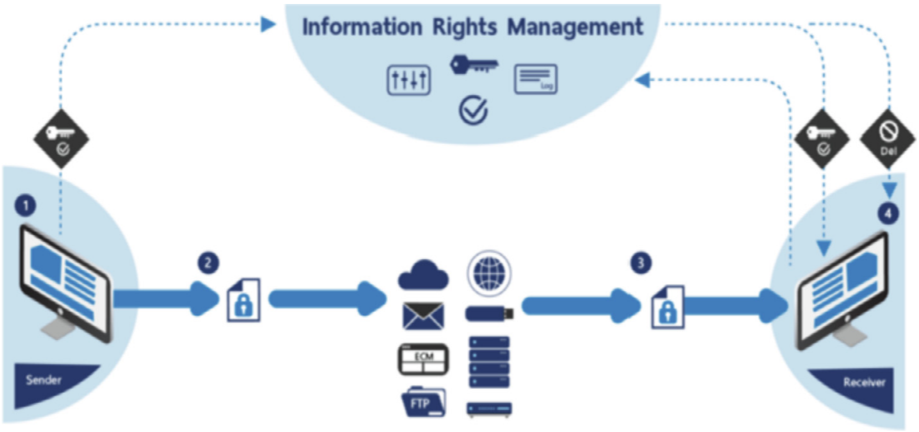


Fig. 3. Information Right Management.

they are on the file system, in inter-process interactions, in networking, in the system register, or the system clipboard. Efficient DLP-Visor can be used in real-world applications because of its 7.2 percent performance overhead. DLP-visor logs have been updated to make it easier to notice and log a DLP incident. During inactive periods, efficient DLP-visor deletes the majority of the log data while retaining the most critical information about leaks and attacks.

Because of cloud storage technologies, the globe has experienced a rapid shift from local storage devices to enormous virtual data centers. As a result, it has become one of the most widely utilized services on the cloud platform for transferring and sharing data between numerous individuals and companies. When a company grows, it can meet the demands of its customers at every turn. In this fast-evolving industry, however, security and privacy are at the top of the list of worries and needs. Some of the most serious problems for people's financial and information security stem from issues such as a lack of data visibility, unencrypted storage sinks, and data overflow. One of the main difficulties we have today is current data security and advisory methods for monitoring data sinks. We'll examine some of today's most up-to-date state-of-the-art security implementations in this study by A. Syed et al., (2020).

When it comes to production, Additive Manufacturing has seen significant advancement in recent years, allowing for the creation of a new market for customized items at cheap unit costs. In addition, everyone has the potential to be a designer. However, the necessary tools are only available to everyone. Connecting customers with manufacturers is the goal of Cloud Manufacturing. Consequently, this study by V. Haseltalab et al (2019) provides a realistic fabrication approach for 3D printers that can help cloud manufacturing. To demonstrate this integration, two different 3D printers were used. The advantages of this strategy, such as using a small memory size for running each printer and the ability to change the design while fabricating, are discussed in detail by constructing sample specimens.

Rapid prototyping technology (SERPT) is a key 3D printing technology that has grown significantly in recent years. In this study by K. Cui et al., the key faults in the process of Digital Light Processing 3D printing are outlined to optimize printing quality and enhance accuracy (2019). In addition, a closed-loop transfer function based on the DLP 3D printing technology is built to measure and analyze all current errors. It is then suggested that the printing defects can be corrected or compensated by using a closed-loop negative feedback mechanism is used to compare the size of the developed model to the size of the goal model. The new printing model size is fitted linearly, which lowers the DLP 3D printing mistake. Then a more precise 3D printing model might be created.

Most cloud infrastructure security breaches have been triggered by human mistakes and misconfigured resources in recent years. To solve these problems, new security models are required. These models must use proactive tactics and be continuous, customer-centric, and not centered on traditional security paradigms like intrusion detection. Torkura et al. (2019) propose a cloud security system based on Chaos Engineering principles. Fault Injection Testing is a technique used by Chaos Engineering to prevent non-security problems in cloud infrastructure. Using similar methods, CloudStrike aims to introduce flaws that could compromise a system's integrity, confidentiality, or availability. For the most part, CloudStrike makes use of the connection between resiliency and safety models. The outcomes of early studies are instructive and forward-looking.

5. Proposed architecture

Users can utilize the data leakage prevention software portal to handle your sophisticated leak management features. As opposed to the main point solution, which uses a cloud-based data leakage prevention technology with super-fast speed and full security

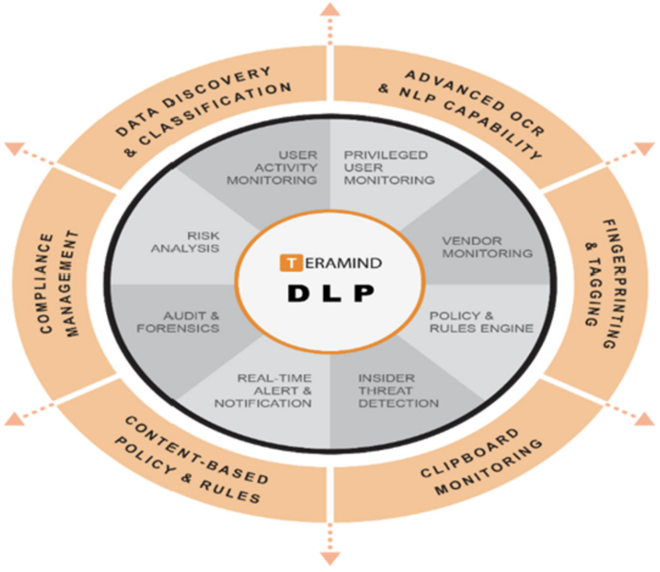


Fig. 4. Cloud-based DLP Open-source management framework.

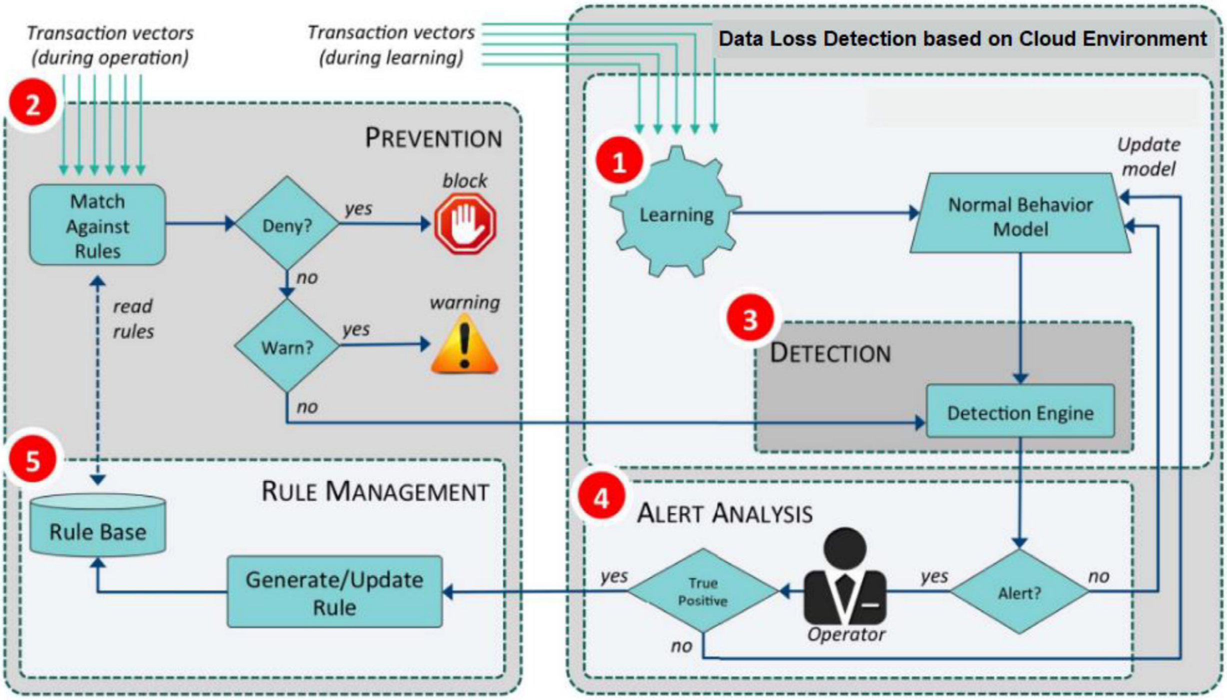


Fig. 5. Working diagram for the DLP framework based on Cloud Environment.

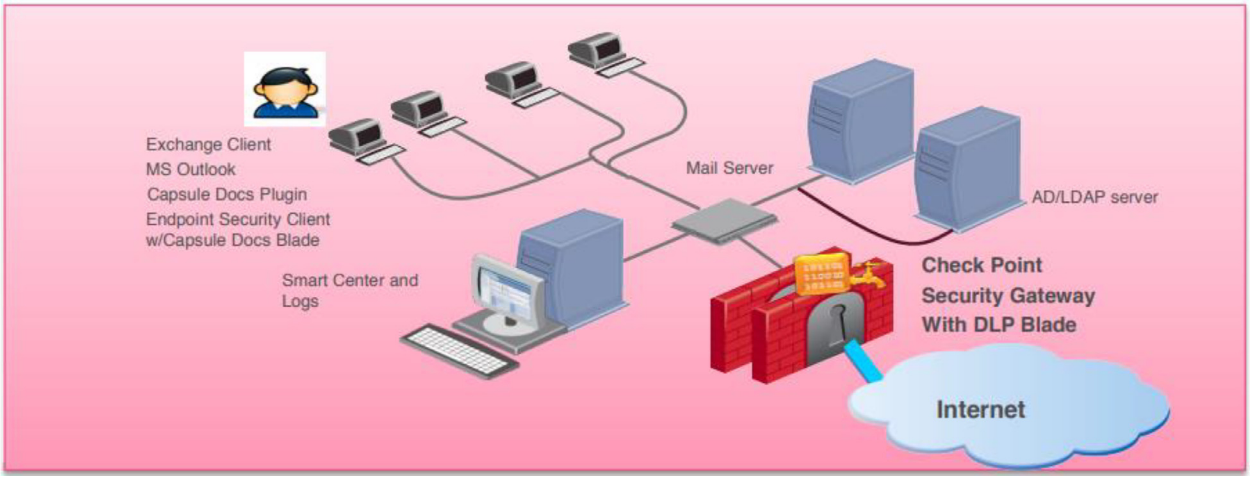


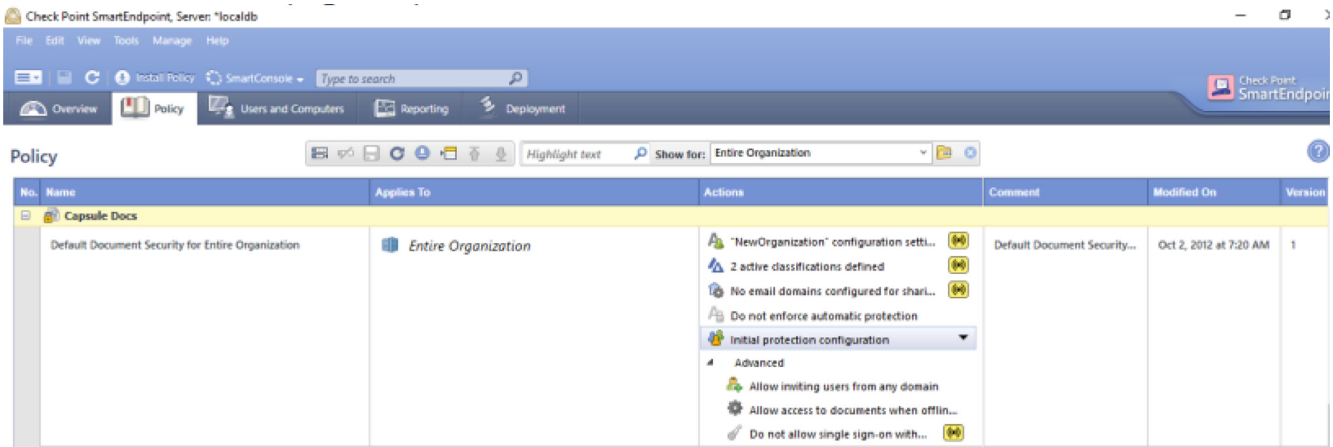
Fig. 6. Check Point Capsule Docs and DLP solution overview.

management, it is a highly scalable, adaptable, and cheaper open-source framework.

- An open-source application framework that works with a wide range of cloud-based web apps, as well as end-user accounts, is probably the most important and independent open-source application framework.
- There are no difficulties with performance or memory/data loss in a cloud environment with data leak management in place.
- It also protects end-users ’ personal information with comprehensive end-user and administrator policies on the web cloud, allowing the unified data leak control technology in place in the environment.
- This framework’s major purpose is to preserve cloud data users’ privacy and compliance with high-end security standards while allowing for improved flexibility and scalability for cloud data users.
- Additionally, through the application framework, it is possible to integrate complicated firewalls with network-based high-security equipment.

An open-source framework for advanced user data leakage management in cloud architecture is shown in Fig. 4 includes Web Cloud Integration, Data Leakage Prevention with multi-layer protection and varied security policies, and User/Admin Access to the Web Console - Data Prevention Suite. An advanced privacy system protects both corporate and individual customers’ personal information by offering Layer 6 data protection and identity-based policies for both users and administrators based on usernames or other user credentials.

- In addition, it is interoperable and meets the needs of other 3rd party security and data protection standards with a great deal of flexibility.


Check Point SmartEndpoint, Server: *localdb
File Edit View Tools Manage Help
Install Policy
SmartConsole
Type to search
Check Point SmartEndpoint
Overview
Policy
Users and Computers
Reporting
Deployment
Policy
Highlight text
Show for: Entire Organization

No.	Name	Applies To	Actions	Comment	Modified On	Version
	Capsule Docs					
	Default Document Security for Entire Organization	Entire Organization	"NewOrganization" configuration setti... 2 active classifications defined No email domains configured for shari... Do not enforce automatic protection Initial protection configuration Advanced Allow inviting users from any domain Allow access to documents when offlin... Do not allow single sign-on with...	Default Document Security...	Oct 2, 2012 at 7:20 AM	1

Fig. 7. Check Point Smart Endpoint Console Policy Configuration.

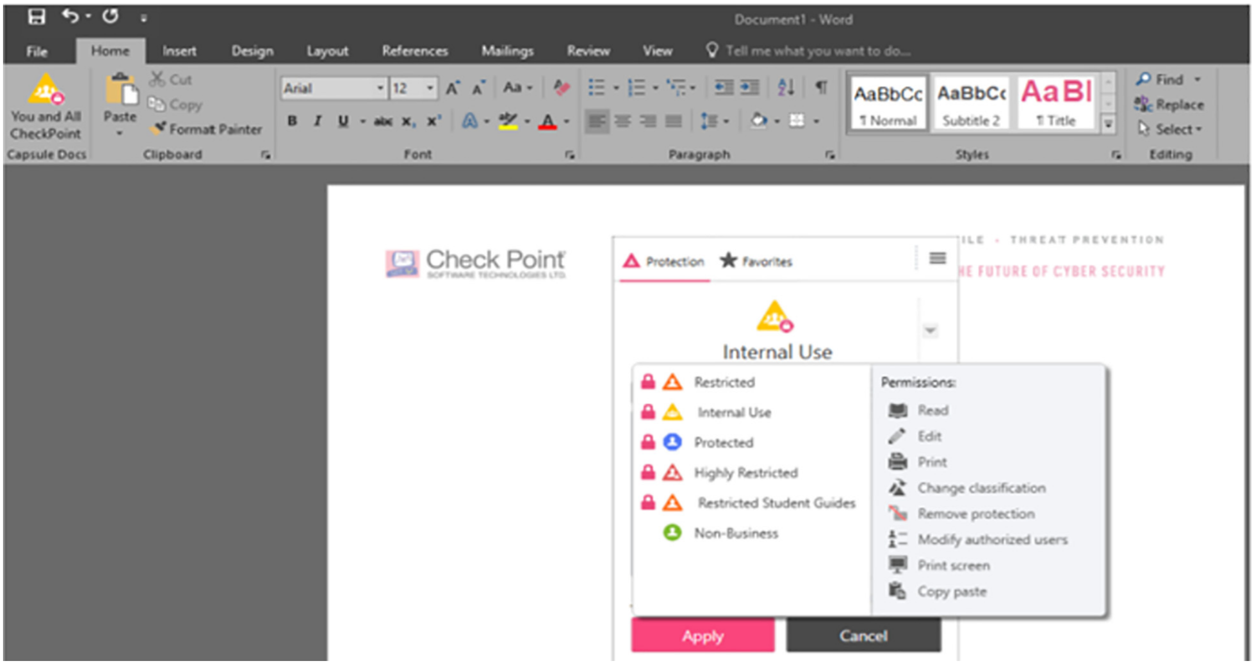


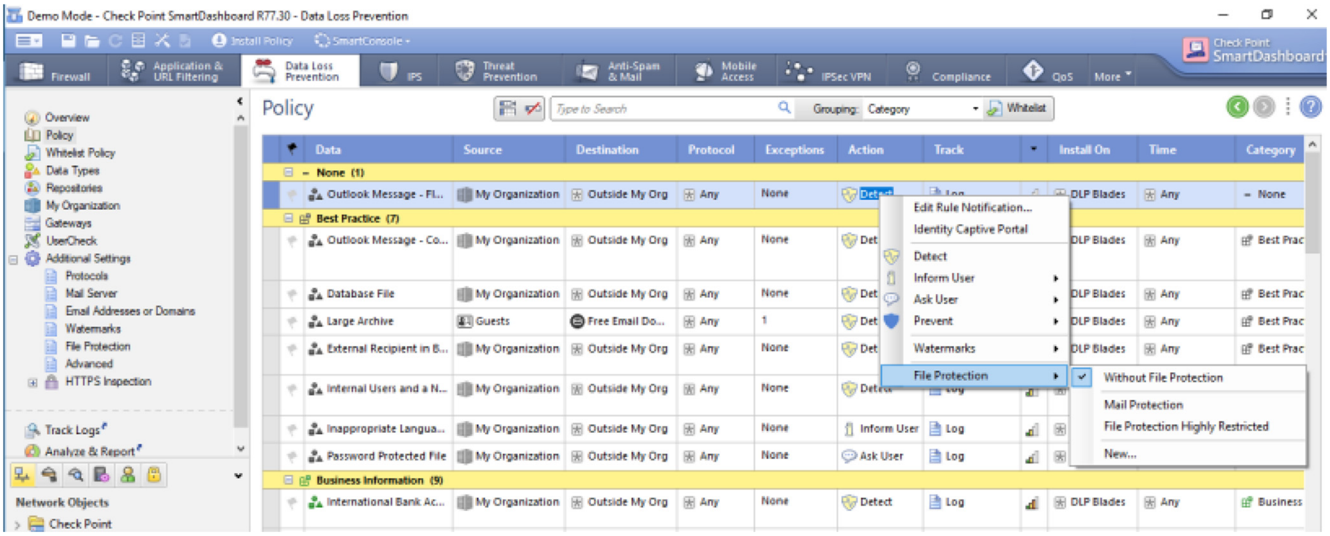
Fig. 8. Microsoft Word document with the Capsule Docs plugin installed.

- Data leak detection is included in the data prevention monitoring equipment, as well.
- For the data leak management online console to work, it comes pre-licensed under the terms of an open-source license.
- Advanced risk management tools can also be used to assess it.
- The standalone web cloud also offers User Data Loss Management for data leakage endpoints.
- Even if the user data leak management panel is running in an offline or online mode, it must be linked to the cloud webserver to function properly.
- With server storage data servers, administrators may also secure users' personal information from being leaked out.
- Your data can be protected from leakage when you store it in the cloud by employing a User Data Leak Management System.
- The working diagram for the DLP framework based on the cloud environment is shown in Fig. 5.

6. Results and discussion

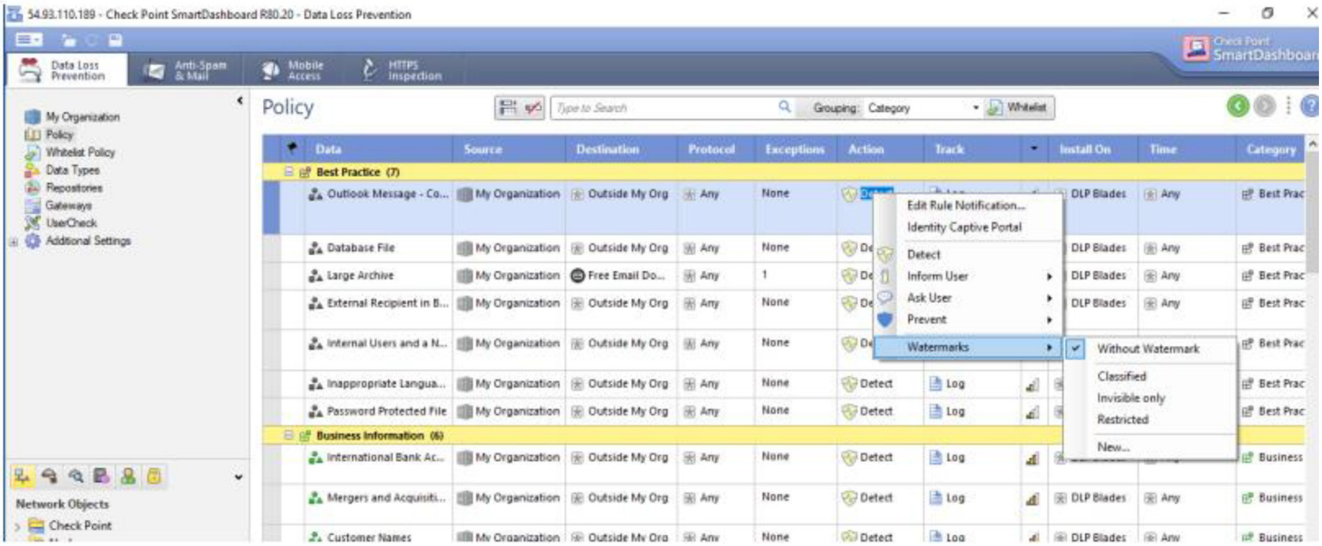
The dashboard of the DLP software is shown below. DLP data can be seen in real-time on the dashboard's graphical user interface. Network, Endpoint, and Data Centre incidents are grouped into three categories. There is also a breakdown of the number of occurrences or events that have occurred and their status. The number of incidents generated can be displayed in the dashboard according to the type of policy and content blade. With a mouse click, you can access a wealth of information. Some checkpoints are indicated in Figs. 6, 7, 8, 9, and 10.

Whenever a large enough number of events occur, DLP creates incidents that a security officer can review and manually rectify the security issues they represent. DLP Dedicated processes are in place to identify the fundamental cause of the problem and then implement the corrective measures necessary to fix it. Workflow is



	Data	Source	Destination	Protocol	Exceptions	Action	Track		Install On	Time	Category
	– None (1)										
	Outlook Message - Fl...	My Organization	Outside My Org	Any	None	Detect	Log		DLP Blades	Any	– None
	Best Practice (7)										
	Outlook Message - Co...	My Organization	Outside My Org	Any	None	Det			DLP Blades	Any	Best Prac
	Database File	My Organization	Outside My Org	Any	None	Det			DLP Blades	Any	Best Prac
	Large Archive	Guests	Free Email Do...	Any	1	Det			DLP Blades	Any	Best Prac
	External Recipient in B...	My Organization	Outside My Org	Any	None	Det			DLP Blades	Any	Best Prac
	Internal Users and a N...	My Organization	Outside My Org	Any	None	Detect	Log				
	Inappropriate Langua...	My Organization	Outside My Org	Any	None	Inform User	Log				
	Password Protected File	My Organization	Outside My Org	Any	None	Ask User	Log				
	Business Information (9)										
	International Bank Ac...	My Organization	Outside My Org	Any	None	Detect	Log		DLP Blades	Any	Business

Fig. 9. Smart Console DLP Policy. Configuring File Protection.



	Data	Source	Destination	Protocol	Exceptions	Action	Track		Install On	Time	Category
	Best Practice (7)										
	Outlook Message - Co...	My Organization	Outside My Org	Any	None	Detect	Log		DLP Blades	Any	Best Prac
	Database File	My Organization	Outside My Org	Any	None	De			DLP Blades	Any	Best Prac
	Large Archive	My Organization	Free Email Do...	Any	1	De			DLP Blades	Any	Best Prac
	External Recipient in B...	My Organization	Outside My Org	Any	None	De			DLP Blades	Any	Best Prac
	Internal Users and a N...	My Organization	Outside My Org	Any	None	De					Best Prac
	Inappropriate Langua...	My Organization	Outside My Org	Any	None	Detect	Log				Best Prac
	Password Protected File	My Organization	Outside My Org	Any	None	Detect	Log				Best Prac
	Business Information (6)										
	International Bank Ac...	My Organization	Outside My Org	Any	None	Detect	Log				Business
	Mergers and Acquisiti...	My Organization	Outside My Org	Any	None	Detect	Log		DLP Blades	Any	Business
	Customer Names	My Organization	Outside My Org	Any	None	Detect	Log		DLP Blades	Any	Business

Fig. 10. Smart Console DLP Policy. Adding the Watermark action to a DLP rule.

managed by a team of security professionals. In the event of recurring security incidents, additional departments such as legal, compliance, and so on are contacted to determine the proper course of action.

Enterprise Manager offers a reporting facility that security officers and executives can utilize to identify areas of risk, risk trends, and levels of regulatory compliance to better understand and remediate security issues. Reports can be generated based on the user's specifications.

Automatic and manual reporting options are available in DLP. if the report is configured to auto-send, then it will be sent at the chosen date, time, and location. Additionally, DLP provides the ability to produce custom reports for various business processes, kinds of violations, severity level, trending, and other variables. DLP reports are shown in Fig. 11.

7. Conclusion

Using the Data Leak Protection Control Console (DLPMC), the cloud-based data leak management system is re-defined in the cloud. Additionally, the data user can add extra keywords to combine both of the established user data types in the cloud for advanced data protection purposes. All of the components are easy to set up, including the framework, the user data loss management web console, and the cloud server. Following a successful setup of the data leak protection web console using private files, the trained user data can be partially detected using the online interface. Additionally, the Data Leak Management Web Console application is capable of self-teaching via the usage of user data files and directories, SQL databases, and ODBC databases. Companies, universities, and even individuals use an open-source framework that

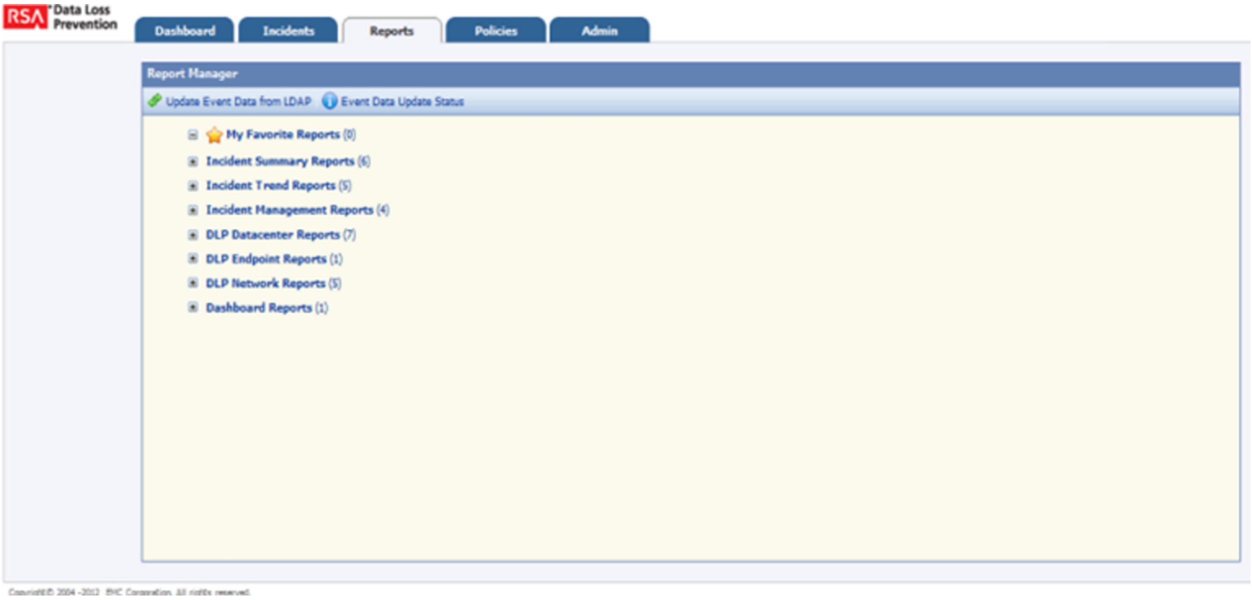

RSA Data Loss Prevention
Dashboard
Incidents
Reports
Policies
Admin
Report Manager
Update Event Data from LDAP
Event Data Update Status
⊟ My Favorite Reports (0)
⊞ Incident Summary Reports (6)
⊞ Incident Trend Reports (5)
⊞ Incident Management Reports (4)
⊞ DLP Datacenter Reports (7)
⊞ DLP Endpoint Reports (1)
⊞ DLP Network Reports (5)
⊞ Dashboard Reports (1)
Copyright© 2004 -2012 EMC Corporation. All rights reserved.

Fig. 11. Generated DLP Report.

can be put on any cloud server for enhanced data leak management with a high-sensitive monitoring tool in their data centers.

CRediT authorship contribution statement

Shahnawaz Ahmad: Data curation, Formal analysis, Conceptualization, Writing – review & editing, Investigation, Methodology. **Shabana Mehfuz:** Data curation, Investigation, Methodology, Validation, Software, Writing – review & editing, Software. **Javed Beg:** Data curation, Visualization, Investigation, Validation, Software, Software.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors acknowledge the financial support received own, for their support and encouragement in carrying out his college work. The authors also would like to acknowledge the administration of Jamia Millia Islamia, which the authors represent.

References

[1] M. Kiperberg, G. Amit, A. Yeshooroon and N. J. Zaidenberg, "Efficient DLP-visor: An efficient hypervisor-based DLP," 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid), 2021, pp. 344-355, DOI: 10.1109/CCGrid51090.2021.00044.

[2] O. Mejri, D. Yang, I. Doh, Cloud Security Issues and Log-based Proactive Strategy, in: 2021 23rd International Conference on Advanced Communication Technology (ICACT), 2021, pp. 392–397, https://doi.org/10.23919/ICACT51234.2021.9370392.

[3] A. Syed, K. Purushotham, G. Shidaganti, Cloud Storage Security Risks, Practices, and Measures: a Review, IEEE International Conference for Innovation in Technology (INOCON) 2020 (2020) 1–4, https://doi.org/10.1109/INOCON50539.2020.9298281.

[4] Z. Tang, A Preliminary Study on Data Security Technology in Big Data Cloud Computing Environment, International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE) 2020 (2020) 27–30, https://doi.org/10.1109/ICBASE51474.2020.00013.

[5] V. Haseltalab, U. Yaman, A Cloud Manufacturing Application for Additive Manufacturing Methods, IEEE International Conference on Mechatronics (ICM) 2019 (2019) 287–292, https://doi.org/10.1109/ICMECH.2019.8722949.

[6] Yuan Huihua, "Research on Data Security in Big Data Cloud Computing Environment[J]", *Information Technology and Informatization*, 2019.

[7] M. Kang, H. Kwon, A Study on the Needs for Enhancement of Personal Information Protection in Cloud Computing Security Certification System, International Conference on Platform Technology and Service (PlatCon) 2019 (2019) 1–5, https://doi.org/10.1109/PlatCon.2019.8669413.

[8] T. Halabi, M. Bellaiche, Towards security-based formation of cloud federations: a game theoretical approach, IEEE transactions on cloud computing 8 (3) (2018) 928–942.

[9] K. Cui, X. Shang, C. Luo, Z. Shen, H. Gao, G. Xiong, A Kind of Accuracy Improving Method Based on Error Analysis and Feedback for DLP 3D Printing, in: 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), 2019, pp. 5–9, https://doi.org/10.1109/SOLI48380.2019.8955020.

[10] K.A. Torkura, M.I.H. Sukmana, F. Cheng, C. Meinel, Security Chaos Engineering for Cloud Services: Work In Progress, in: 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), 2019, pp. 1–3, https://doi.org/10.1109/NCA.2019.8935046.

[11] W.u. Weiqiang, Comprehensive and multi-angle information security technology research and practice under cloud computing and big data environment[J], Communication World 000 (014) (2017) 45–46.

[12] K. Lingtao, Z. Hui, Data security analysis under the big data cloud computing environment[J], Network Security Technology and Application 000 (009) (2017) 82.

[13] Z. Qian, Y. Huibi, Exploration of big data security and privacy protection under cloud computing[J], Science Popular (Science Education) 000 (010) (2017) 192.

[14] A. Alshammari, S. Alhaidari, A. Alharbi, M. Zohdy, "Security Threats and Challenges in Cloud Computing", *Magnetism, vol,* III IEEE 4th International Conference on Cyber Security and Cloud Computing, 2017.

[15] A. Balobaid, W. Alawad and H. Aljasim, "A Study on the Impacts of DoS and DDoS Attacks on Cloud and Mitigation Techniques International Conference on Computing", *Analytics and Security Trends*, 2016.

[16] R. Boutaba, L.u. Cheng, Q.i. Zhang, On Cloud computational models and the heterogeneity challenge, J Internet Serv Appl 3 (1) (2012) 77–86.