Virtualization, Data Storage and Management Challenges in Cloud Computing

by Rakeshpv

General metrics

34,316	5,028	449	20 min 6 sec	38 min 40 sec
characters	words	sentences	reading time	speaking time

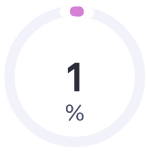
Score

This text scores better than 92% of all texts checked by Grammarly

Writing Issues

168	79	89
Issues left	Critical	Advanced

Plagiarism



5 sources

1% of your text matches 5 sources on the web or in archives of academic publications

Virtualization, Data Storage and Management Challenges in Cloud Computing

1st Rakesh Pv
2st Smith CD
3st Joshua Stalin S
PG Scholar , Department of Computer Science
Christ Deemed To Be University

***Abstract*—In cloud computing environments, virtualization has grown in popularity and appeal. A key technology in a cloud environment is virtualization. Due to several new security challenges, security concerns around virtualization technologies have become a significant worry for enterprises. The number of users is growing, and the volume of data they produce is growing exponentially due to the rapid growth of information technology, cloud computing, massive data, mobile connections, and other technologies. Multiple servers can be used with distributed storage technology to store data and distribute the storage load. Data blocking algorithm is being researched to speed up data backup reaction time and increase enormous data storage efficiency. The cloud service provider ensures the integrity, availability, privacy, and confidentiality of client data stored in the cloud. The data management research community and huge internet organizations have difficulty developing consistent, available, and scalable data management systems capable of supplying petabytes of data for millions of users. However, the desire to offer data management services in the cloud, the rise in cloud computing popularity, and the migration of numerous internet applications to the cloud have made it more difficult to design data management systems that offer consistency guarantees at a granularity greater than individual rows and keys. The primary difficulties and dangers associated with virtualization and data storage in cloud computing systems will be discussed in this presentation.**

I. Introduction

A. Virtualizarion in cloud

The development of a cloud computing environment relies heavily on virtualization technology. It enables multiple operating systems to co-exist on the same physical server as virtual machines (VMs), using the dynamic resource allocation on the same machine without interfering with one another. The use of several instances of the same application on a single or several cloud resources is made possible by virtualization technology [1]. Multiple users being able to run their applications simultaneously is scaleability that the virtualization layer naturally enables. The user can execute their programs on a single virtual machine without having access to the data of other users The rapid advancement of cloud computing has resulted in a several non-traditional security threats, and proposed a new and increased demand for information security. Virtualization has resurfaced as a means of improving system security and delivering on the value of cloud computing. It gives organizations and people an opportunity to utilize and improve the use of their hardware by increasing the number and types of tasks that a single machine can handle . Resource sharing and isolation are two significant advantages in a virtualization environment. One of the essential advantages of virtualization is the ability to allocate physical resources to VMs based on their needs. Virtual machines share access to central processing units, disc controllers, physical network cards, etc. Another advantage the virtual environment can provide is isolation; the VM isolates its data from other VMs. The failure of one VM has no bearing on the performance or execution of other VMs running on the same host. This study aims to identify and understand the main challenges and security issues of virtualization in cloud computing environments. Furthermore, it presents baseline recommendations for improving security and mitigating risks encountered virtualization to adopt secure cloud computing

B. Data Storage and Data Management

These cloud apps use large data centers and potent servers to host Web applications and services. The task of storing and processing large amounts of data in the cloud computing environment is inefficiently accomplished by conventional data storage technologies, including network storage, centralized storage, and distributed file systems. Cloud computing offers a wealth of advantages to its users, including free services, flexible resource usage, simple internet access, etc. By utilizing techniques like firewalls and virtualization, the Cloud Service Providers (CSPs) have pledged to guarantee the data security over stored data of cloud clients. CSPs have complete control over customer data, hardware, and cloud applications. As a result, the cloud needs safe storage and administration techniques to protect the data privacy and integrity of the data. These applications‘ erratic load characteristics, rising demand for data storage while ensuring 24/7 availability, and various degrees of consistency requirements provide new difficulties for cloud data management. These contemporary application requirements need solutions that offer scalable and reliable data management as a cloud service. Cloud computing technologies and products are being developed by Google, Amazon, IBM, Microsoft, Sun, and other IT juggernauts. Applications that have been expanded to be accessed through the Internet are also referred to as cloud computing.

These cloud apps use large data centers and potent servers to host Web applications and services. A cloud application is accessible to anyone with a reliable Internet connection and a primary browser. For instance, Google has made a point of pushing application engines built using the Google File System, MapReduce, BigTable, and other techniques that give customers ways to handle large amounts of data. The task of storing and processing large amounts of data in the cloud computing environment is inefficiently accomplished by conventional data storage technologies, including network storage, centralized storage, and distributed file systems. After the personal computer and the Internet, cloud computing—the foundation of the new generation of IT—will become the third focal point of the global information technology revolution

II. Cloud computing and cloud storage

Cloud computing infrastructures can help businesses better use the money they invest in IT gear and software. They achieve this by automating the management of the collection of systems as a single entity and dismantling the physical boundaries present in isolated systems. A system that is ultimately virtualized is the cloud, which is a logical progression for data centers that use technology for automated systems administration, task balancing, and virtualization. Through real-time workload balancing, a cloud architecture can be a more affordable method of providing information services, simplifying IT management, encouraging innovation, and improving responsiveness. Web 2.0 applications may be instantly launched and scaled up as much as needed, thanks to the Cloud. The platform supports conventional JavaTM and LAMP (Linux, Apache, MySQL, PHP) stack-based applications and cuttingedge designs like MapReduce and the Google File System, which enable rapid scaling of applications across thousands of servers.

A. Cloud storage definition and its architecture

A solution called cloud storage offers features ike data storage and corporate access. It assembles several storage devices using application software based on characteristics of cluster applications, grid techniques, distributed file systems, etc. Cloud storage can be considered a system for cloud computing with massive capacity storage in addition to just the storage in cloud computing. The storage layer, the fundamental management layer, the application interface layer, and the access layer comprise the bulk of the cloud storage system architecture

B. Distributed data storage technology

Cloud computing is a cutting-edge computing model that uses many servers and mainly consists of technologies for managing cloud computing platforms, programming models, virtualization, data management, data storage, etc. Data storage in cloud computing uses distributed storage technologies, and redundancy storage ensures data reliability [4]. Data storage across many independent storage devices using an extensible system architecture and various storage servers is the central concept of distributed storage systems. Utilizing location data saved on the server location, shared storage load not only increases system dependability, availability, and access effectiveness, but it is also simple to extend

C. The file system

The distributed file system creates a single, hierarchical multiple-file server on the network by combining the geographical locations of the files on several computers under a single namespace. Users and dispersed files on various servers share the same space in front of the network. Data management and access are easier for users. For instance, GFS, the Google File System, is a distributed file system that is expandable and designed for use by largescale, distributed programs that access massive volumes of data. GFS was designed with a different concept from the conventional file system. It is made for Google application features and large-scale data processing

D. P2P storage technology

Peer-to-peer technology (P2P), often referred to as peer-interconnected network technology, is a novel type of network technology that depends on network users' computer power and bandwidth rather than a small number of servers. Only equal peer nodes exist in a pure point-to-point network, which acts as both a client and a server for other nodes on the web. P2P networks can be used for various things, including file-sharing programs and real-time media businesses [5]. Mass data, super largescale user scale, high availability, and traditional data storage and administration are new features based on cloud computing that bring new issues. Traditional data management and storage are now up against fresh obstacles. The distributed storage system and the associated technologies are versatile and flexible enough to handle challenging data management and storage jobs. However, the 3 demands of the vast data scale and user scale remain unmet

III. Data deduplication Technology

The current study is focused on how to effectively store and manage the enormous amount of data generated by different businesses and individuals utilizing distributed data storage technology, which is a result of the rapid development of comprehensive data technology and mobile Internet. Data deduplication technology has recently been employed as a successful method for managing and storing large amounts of data. The main goal is to remove redundant data from the data collection by deleting duplicates and keeping only one of them.

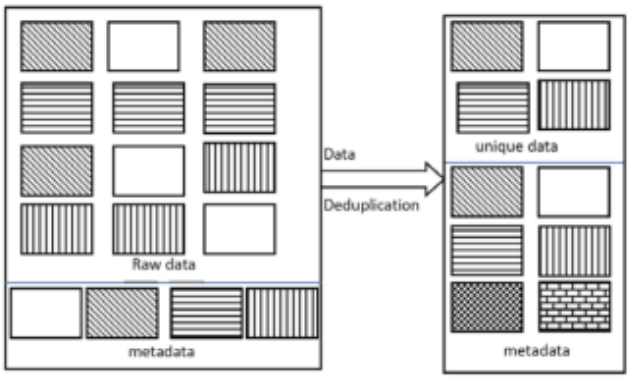


Figure 2. Data Deduplication

Massive data in a big data and cloud computing context highlights the issue of data storage. Using ”deduplication” technology can preserve backup data for extended periods, save more backup space, and lower the data center’s resource usage. The speed of data backup is unaffected by data deletion. How does the data deletion technique take file segmentation into account? What formula is used to determine the data block fingerprint? How should data blocks be retrieved? It is especially significant.

A. Fixed-length block

The file is syncopated with the predetermined block size using the fixed-length block technique, and both the md5 weak and strong check values are run. The primary purpose of the invalid check value is to increase the effectiveness of differential coding; to do this, first calculate the soft check value and run a hash search, and only then should you compute the md5 substantial check value and run additional hash lookups. The computation of a weak check value is much smaller than that of an md5, which can significantly enhance coding performance. The fixed-length block technique has the advantages of simplicity and fast performance. Still, it is susceptible to data addition and deletion, making it inefficient and unable to be modified and optimized in response to content changes.

B. The CDC algorithm

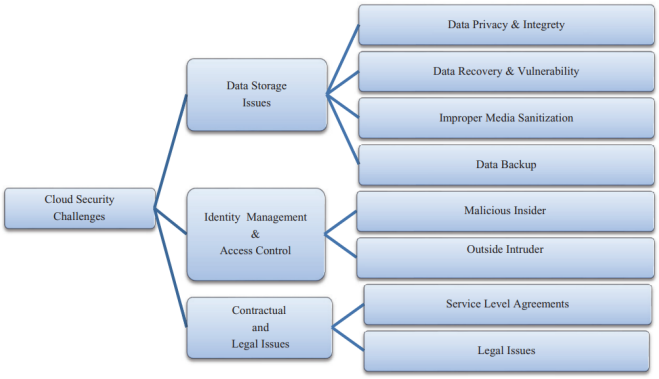
The network file system LBFS [6], based on the CDC variable length block algorithm, promotes repetitive data deletion based on various content block ideas. The CDC technique first divides the file into data blocks with different levels of growth using the Rabin fingerprint algorithm [6]. Second, each data block’s fingerprint is determined using a fixed4 size sliding window and the hash technique. The resulting data block fingerprint is then compared to the data block fingerprints already in the storage system. Such agility within a data center has been made possible by virtualization, a critical technology. Hardware virtualization enables a flexible mapping of virtual machines to servers in a data center by creating a logical separation between applications and the underlying physical server resources. Virtual machine platforms also support the ability to live-migrate virtual machines from one server to another without experiencing application downtimes. This allows VM containers to be resized to accommodate changing workloads. The same data blocks with the same fingerprint value are then erased, leaving the file system with just one data block. As a result, the amount of disc space the data takes up is effectively lowered, and the effectiveness with which the area is being used is increased. However, it is challenging to estimate the size of data blocks while the CDC algorithm is being run. The overhead is too high, and the granularity is too fine. Separating the data blocks may result in a significant number of substantial and small data blocks, and these two extreme examples are not currently a better option.

C. The core technology of Storage Technology

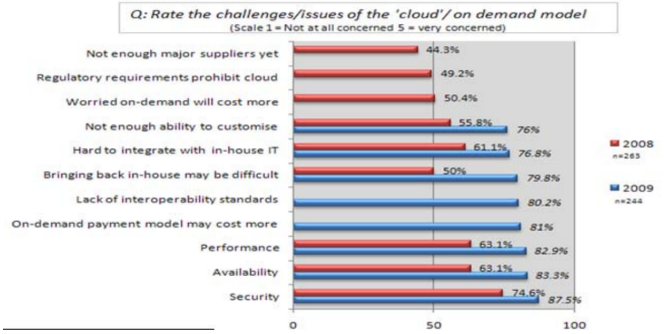
The demand for massive data storage from applications has grown in recent years, directly influencing the emergence and development of highperformance storage technology. As a result, technologies like the Google File System and Hadoop Distributed File System are now widely used in cloud computing. Cloud storage can offer a more dependable service because problems like equipment breakdowns, updates, and upgrades are fully considered. Instead of using storage devices directly, customers utilize the Data Access Service offered by the complete cloud storage system. Therefore, cloud storage is a service rather than storage in the traditional sense. With multiple service forms of network hard drive, online storage, online backup, and online archive storage service, cloud storage offer direct data storage services for end users and indirect data access in application systems, among other kinds of assistance. Operating systems, service protocols, user applications, and enormous volumes of data are all saved in storage systems. Cloud computing service providers must create a sizeable globalization and storage center to achieve ample data storage. As an illustration, Google‘s significant success in cloud computing is mainly attributable to its cutting-edge cloud storage infrastructure built on GFS.GFS is a distributed file system that can handle massive amounts of dispersed data. The maintenance of metadata, the namespace of the stored files and partnerships, the mapping of files to unions, and the location of each block copy‘s storage are all handled by the controller server. The file is divided into fixed-size blocks (64M) and stored in the chunk server.

IV. SECURITY CHALLENGES IN CLOUD COMPUTING

customers can access ondemand services via the internet thanks to the cloud computing architecture, which saves data and application software with little administration effort. However, customers don’t have reliable obligations or policies when using cloud management. Data storage security challenges, including privacy, confidentiality, integrity, and availability, will result from this. This paper concentrated on cloud computing data storage security challenges and presented cloud service models, deployment models, and a range of security issues in cloud environment data storage and described potential solutions for the data storage problems that ensure privacy and confidentiality in a cloud environment.



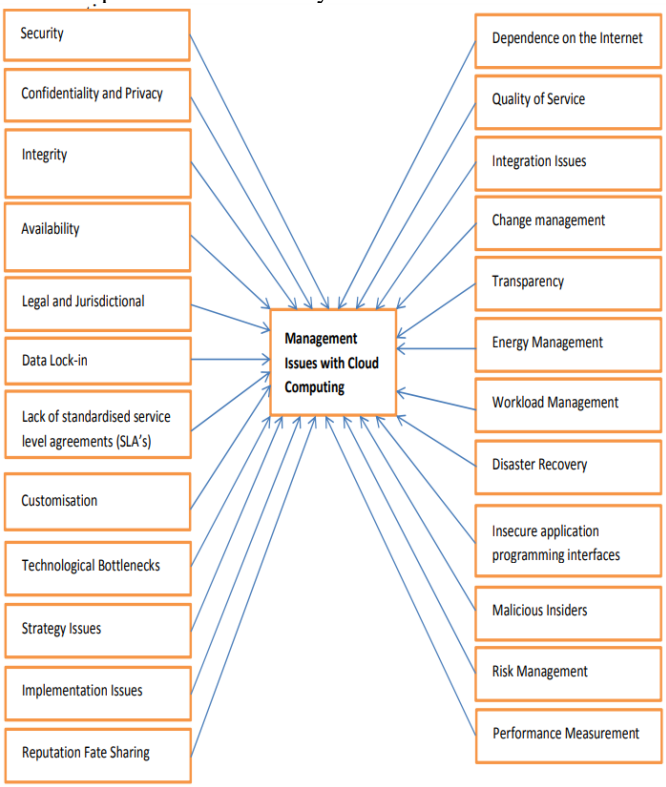
The above figure shows the challenges dealt in the paper [1]. In the paper they have also provided an identity management and access control solution i.e., Identity management systems for Cloud Environments with Simple Privacy-Preserving Identity Management (SPICE), i.e., in order to provide anonymous authentication, access control, accountability, unlikability, and user-centric authorization, the SPICE ensures group signature. The SPICE offers the above features with just one registration. After registering with a reputable third party, users receive unique credentials for all of the services provided by CSP. The user generates an authentication certificate by using the credentials. The user must generate their needed authentication certificate using the same credentials, while different CSPs expect different properties for authentication. They have also mentioned one more solution referring some papers in their article i.e., Role-based multi-tenancy access control (RB MTAC) has been suggested in which Role-based access control and identity management are combined in the RB MTAC [1]. the security issues that must be appropriately handled and managed in order for cloud computing to reach its full potential; the goal is to present an overall security viewpoint on the technology. The findings from the International Data Corporation corporate panel poll on cloud dangers and Gartner's list of cloud security issues. In this paper the author's also talks about the types of clouds, cloud computing delivery models, cloud computing concerns, information security requirements and also shows the cloud challenges survey.



The author present's his methods for managing and safeguarding confidential data, emphasizing strategies for securing data services. The author specifically designs information-sharing protocols for the responsibilities of secret (private) data communication which will be one of the alternatives mentioned. This protocol is provided in the form of algorithms to resolve the problems of safeguarding and securing data against the unlawful acquisition. This paper also specifies that data services are specific information that needs to be secured, and this data-securing duty will be carried out through data-sharing protocols. Here the data protection domain is divided into different levels, within which the tasks will carry out data management and protection. The authors' approach to data security, which involves using cryptographic threshold techniques to divide the secret among a specific group of secret trustees and enhancing them simultaneously by applying linguistic techniques to describe the shared secret, creates a new class of protocols known as intelligent linguistic threshold schemes.

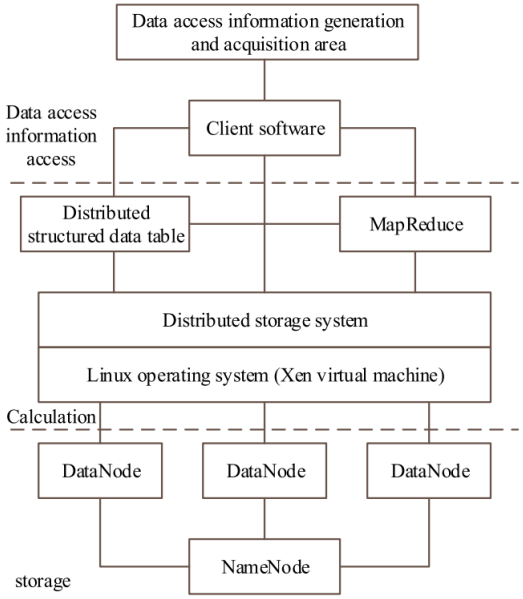
V. Data Management in Cloud Computing

This paper states that, Convenient and ondemand network access to a shared pool ofr econfigurable computing resources is made possible by the promising computing concept known as cloud computing. Data owners allow cloud service providers to hold their data on cloud servers, and data consumers can access the data from the cloud servers. This is the first cloud service that has been made available. The problem statement also specified, because data owners and servers have separate identities and business interests, this new paradigm of data storage service also presents new security issues. A third-party auditing service is necessary to ensure that the data is correctly hosted on the Cloud. This article provides a thorough solution analysis of storage auditing techniques used in the literature. First, it offers a list of specifications for the auditing protocol for cloud computing data storage. Then, it introduces a few current auditing plans and evaluates their performance and security. Some of the data storage auditing models specified here are system model and threat model



Future cloud computing experiences for businesses are promised by cloud computing. As long as academics and

companies keep working to find answers, the drawbacks of cloud computing, such as security concerns, confidentiality, and privacy concerns, strategic concerns, availability issues, data lock-in, etc., won't be a significant management problem in the future. Control mechanisms should be used to reduce security threats in order to make cloud computing more secure and cost-effective. This document also presents an overview of IS management concerns with cloud computing to aid management in cloud computing implementations. In order to guarantee integrity, privacy, and the availability of data and applications in the cloud, risks should be carefully examined.



The current Internet of Things (IoT) uses cloud computing data access storage techniques; the hash algorithm, however, has weaknesses in terms of inefficient data processing and limited fault tolerance. In order to improve the storage and data access methods for cloud computing, HDFS is introduced. Hash values are then used to optimize the configuration of data access information storage locations, allowing the data access storage distribution strategy to be optimized. HDFS is first used to optimize the data access storage architecture in accordance with problems of data access storage architecture in the Internet of Things. The IoT topology is then improved, and the size of data blocks is optimized using an effective method. The file storage design is optimized in the end. The enhanced cloud storage solution has been demonstrated through simulation testing to have clear performance gains regarding file read and write speed and memory utilization. The proposed optimization algorithm in the paper significantly increases file upload and download efficiency, data processing efficiency, and fault tolerance rate compared to the conventional hash algorithm. This fully demonstrates how superior is the proposed cloud computing data access storage optimization algorithm

VI. SECURITY CHALLENGES AND RISKS IN VIRTUALIZATION

A. User awareness

Because cloud service providers do not monitor their customers' surroundings, cloud service users are the weakest link in any information security system. Suspicious user accounts can enable attackers to conduct malicious activities undetected. Additionally, an attacker could use attack vectors for various social engineering techniques to visit malicious websites and gain access to the user's computer. It can then observe user actions, see the same data as the user, and steal user credentials to authenticate the cloud service. A frequently overlooked security concern is security awareness.

B. Insecure APIs

A cloud computing provider provides users with infrastructure, software, and platform services, which they can access via interfaces. They created their interfaces using publicly available application programming interfaces. APIs pose several security issues, including improper authorizations, weak credentials, and clear-text transmission, which can impact the availability and security of cloud services

C. Inadequate security policies

The organization defines security policies to determine how to protect its assets from potential threats and deal with such situations when they arise. The cloud service provider's security policies may be insufficient or incompatible with an organization's security requirements. Inadequate security policies may expose some vulnerabilities, creating an insecure VM environment.On another side, VMs can be moved between physical environments as required. When a VM is migrated or moved from the source host to another, the destination host might not have enough security to protect the VM. Mobile VMs need baseline histories and security policies to move with them.

D. .Inadequate authentication and session management

Authentication techniques protect the system from bad actors who pose as legitimate users, developers, or operators to read, delete, or modify data. A virtual environment's authentication mechanism applies to end users and system components. Improperly designed or implemented authentication and session management application functions may impact access and control policy [6]. Furthermore, it allows attackers to compromise keys, session tokens, or passwords and exploit

E. Incorrect VM isolation

The hypervisor ensures VM isolation. The isolation between VMs prevents one VM from accessing another VM's virtual discs, applications, or memory on the same host. Furthermore, VM isolation limits the attack's scope. It complicates access to resources and sensitive data on the physical machine. An isolation violation occurs when an attacker communicates with other VMs on the same host using a compromised VM. As a result, a shared environment necessitates precise configuration to maintain strong isolation.

F. Insecure VM migration/mobility

The benefit of virtualization is the ability to transfer applications transparently from one host machine to another without stopping the VM. After migration, the application continues to run without interruption. The user is unaware that his VM has been migrated. The VM is migrated by copying the VM's application and the entire system state, including memory, CPU state, and sometimes disc, to the destination host. During migration, however, the attacker may steal and snoop or actively modify confidential information. As a result, the transmission channel must be protected and secured from various passive and active attacks.

VII. PROBLEM DEFINITION

One of the most severe threats to virtualization and cloud computing is malicious software that allows computer viruses or other malware that have infiltrated one computer's system to spread to the underlying hypervisor and, eventually, to the design of another customer. In a nutshell, one cloud computing customer could download a virus, such as one that steals user data, and then spread that virus to all other customers' systems.

A. Solution of the above problem

To prevent this, Hyper safe employs two components. The hyper-safe program uses a technique known as non-passable memory lockdown, which explicitly and reliably prevents anyone other than the hypervisor administrator from introducing new code. This also prevents external users from modifying existing hypervisor code. The technique used by Hyper-safe is known as restricted pointer indexing. This technique is known for first characterizing a hypervisor's normal behavior and then preventing any deviation from that profile. Only the hypervisor administrator can modify the male hypervisor code.

VIII. VIRTUALIZATION THREATS AND ATTACKS

A. Cross-VM Attack:

When a malicious virtual machine bypasses hypervisor-level isolation to attack co-located VMs, this is referred to as a cross-VM attack. Cross-VM attacks range from controlling other VMs by exploiting guest or hypervisor vulnerabilities to gaining personal data via side-channel attacks. Several VMs are co-residents on a single server to maximize resource usage; this co-resident placement may result in a cross-VM side-channel attack. A cross-VM side-channel episode begins with a co-location attack and poor isolation method implementation; a malicious VM conducts side-channel raids. As a result, sensitive information can be extracted to continue the attack using a different method to gain control of the entire system.

B. VM Rollback

Without VM awareness, the hypervisor can pause a running VM, capture a snapshot of the current disc, memory, and CPU states, and resume the image in the future. This feature is used for VM maintenance and fault tolerance, but it also allows the attacker to launch a VM rollback attack. The attacker can use old VM snapshots to run them without the user's knowledge, then delete the history of the VM execution and execute a different or identical shot again. Because the VM execution history is lost, the attacker can avoid or undo updates to some security mechanisms.

C. VM Sprawl

It occurs when the number of VMs on the same host continues to grow without control, and some are idle. Because VMs retain system resources such as network channels and memory, these system resources are effectively missing and cannot be allocated to other VMs. VM sprawl is a problem for cloud providers because many VMs necessitate a large amount of memory

D. VM Escape

A VM avoids a threat designed to exploit a hypervisor. It is a situation in which a malicious VM or user escapes the hypervisor's control. Malware software running in a VM can bypass the isolation between the VMs and the host in VM escape. As a result, the attacker gains access to the hypervisor, causing the entire system to fail. When the attack is successful, the attacker gains access to the storage hardware, computing power, shared resources, and other virtual machines.

E. VM Hopping

The process of jumping from one VM to another by exploiting vulnerabilities in the hypervisor or virtual infrastructure is known as VM hopping. Because the hypervisor has high privileges, using it would have serious consequences. When attackers gain malicious access to other users' VMs, they can monitor the target VM's resources, changing its configurations, removing stored data, and affecting the VM's integrity, availability, and confidentiality.

F. Hyperjacking

The hyperjacking attack inserts VM-based rootkits into the virtualized environment to control the entire virtualized environment. It injects and modifies a fake hypervisor beneath the original one. A VM-based rootkit established a covert channel to the hypervisor for malicious injection code, hiding it from the security mechanism. Because the hypervisor operates at a system's highest level of privilege, it would be challenging, if not impossible, for any operating system (OS) running on the hypervisor to detect it.

IX. RECOMMENDATION

A. User Awareness

To counter any attempt to tamper with the system, user awareness is essential to any plan. All parties involved, including service providers and organizations, must focus on staff education and training and use assurance processes to evaluate human resources. Small and medium-sized businesses, corporations, and government agencies can help raise user awareness by encouraging their professional staff to attend skill-building training courses at relevant institutes. End users should be aware of their rights and the threats to their privacy in virtual environments by participating in relevant courses and instructional activities.

B. Secure Host OS

Because the virtualization layer exists above the operating system (OS), protecting the OS on the host machine is critical. A compromised operating system provides an ideal environment for attacking the virtualization layer. Service providers must update the operating system version, remove or disable unnecessary software and services, and install a host intrusion detection system and anti-virus.

C. Secure the Hypervisor

The hypervisor is an additional software layer that sits between virtual machines and the underlying hardware, with or without a host operating system. Some hypervisors check for and install updates automatically. Updates can be administered using centralized patch management solutions. Disconnecting unused devices from the host can aid in hypervisor security. It is preferable to harden the hypervisor configuration to reduce areas of vulnerability.

D. Protect the VM

A virtual firewall is required to prevent VM-to-VM attacks, and a robust authentication mechanism is needed to avoid unauthorized access to VM. If a virtual machine is compromised, we must assume that all VMs on the same server is compromised. In this case, restore each guest OS to a previous good image or snapshot before the compromise. As a result, making a backup of the virtual drive used by the guest OS is a good idea. We must isolate and protect the memory of guest VMs from other VMs sharing the same physical system and from an untrustworthy hypervisor.

X. CONCLUSION

Virtualization is a widely used technique for extending the capabilities of physical computers by dividing resources among operating systems. Virtualization enablesmany instances of the same application on one or more cloud resources. In this study, we investigated the common challenges and risks of virtualization technology, as well as the main threats and attacks that may compromise virtualized systems in cloud computing environments.. Cloud service suppliers must communicate with their consumers about the amount of security they offer using their cloud. In this study, we initially covered several cloud computing models, security concerns, and research issues with cloud computing. Data security is a serious concern for Utilizing the cloud. There are numerous more security difficulties. Includes network and virtualization security facets. This The paper has emphasized each of these cloud computing problems. We believe that given how intricate clouds are, they will Obtaining end-to-end security is challenging. Updated security outdated security methods need to be updated and modernized needed to be drastically changed to be compatible with the architecture of clouds.A crucial research challenge is how to maximize the performance of the distributed storage system and guarantee its high reliability. in large-scale, vast data, virtualization, and high-scalability cloud computing environments. The slider algorithm is used in this paper to optimize storage space utilization, reduce data backup time, and enhance distributed data storage performance based on the cloud computing environment. The slider algorithm is based on data deduplication technology. This paper studies data partitioning technology.

REFERENCES

[1] . Geelan (2008),“Twenty one experts define cloud computing,”Virtualization, Electronic Mag., article available at http://virtualization.sys-con.com/node/612375.

[2] B. Loganayagi and S. Sujatha, “Creating virtual platform for cloud computing,” in Proc. 2010 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2010, pp. 1

[3] L. Garber, “The Challenges of Securing the Virtualized Environment,” Computer, vol. 45, no. 1, pp. 17-20, 2012

[4] Cloud Security Alliance,“The Notorious Nine. Cloud Computing Top Threats in 2013,” CSA, 2013. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats.cloudsecurityalliance.org. [Accessed: Oct.-2017].

[5] Cloud Security Alliance,“The Notorious Nine. Cloud Computing Top Threats in 2013,” CSA, 2013. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats.cloudsecurityalliance.org. [Accessed: Oct.-2017].

[6]] A. Parashar and A. Borde, “Cloud Computing: Security Issues and its Detection Methods,” Int. J. of Engg. Sci. Mgmt., vol. 5, no. 2, 2015, pp. 136–140

[7] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning,“Managing security of virtual machine images in a cloud environment,” in Proc. ACM workshop on Cloud computing security - CCSW ’09, 2009, p. 91.

[8] B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[9] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, “On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[10] Aman Bakshi, Yogesh B. Dujodwala, “Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine,” ICCSN ’10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[11] B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC’2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[12] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran “Research Issues in Cloud Computing “ Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.

[13] R. Gellman, “Privacy in the clouds: Risks to privacy and confidentiality from cloud computing,” The World Privacy Forum,2009

[14] NareshvurukondaB, ThirumalaRao “A Study on Data Storage Security Issues in Cloud Computing” 2nd International Conference on Intelligent Computing, Communication Convergence, ICCC 2016, 24-25 January 2016, Bhubaneswar, Odisha, India

[15] Lidia Ogiela, Marek R. Ogiela, Hoon Ko ”Intelligent Data Management and Security in Cloud Computing” Selected Papers from the 11-th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2019) and the 22nd International Conference on Network-Based Information Systems (NBiS-2019)

[16] Ramgovind S, Eloff MM, Smith E “The Management of Security in Cloud Computing” 2010 Information Security for South Africa IEEE publication

[17] Mingzhe Wang, Qiuliang Zhang “Optimized data storage algorithm of IoT based on cloud computing in distributed system” Computer Communications Volume 157, 1 May 2020, Pages 124-131

[18]] Akinlolu Olumide Akande, Nozuko Aurelia April, Jean-Paul Van Belle “Management Issues with Cloud Computing” ICCC ’13: Proceedings of the Second International Conference on Innovative Computing and Cloud ComputingDecember 2013 Pages 119–124

[19] Kan Yang, Xiaohua Jia “Data storage auditing service in cloud computing: challenges, methods and opportunities” World Wide Web (2012) 15:409–428

[20] A Venkatesh, Marrynal S Eastaff "A Study of Data Storage Security Issues in Cloud Computing" International Journal of Scientific Research in Computer Science, Engineering and Information Technology 2018 IJS
[21] LiYibin, KekeGai, LongfeiQiu, MeikangQiu, ZhaoHuid "Intelligent cryptography approach for secure distributed big data storage in cloud computing" Information Sciences Volume 387, May 2017, Pages 103-115
[22] Kan Yang, Xiaohua Jia "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing" 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)
[23] Divyakant Agrawal, Amr El Abbadi, Shyam Antony, and Sudipto Das "Data Management Challenges in Cloud Computing Infrastructures" DNIS 2010: Databases in Networked Information Systems pp 1–10
[24] Research on Data Storage Technology in Cloud Computing Environment To cite this article: Caiyun Xu 2018 IOP Conf. Ser.: Mater. Sci. Eng. 394 032074
[25] J. Abawajy, M. Deris. Data replication approach with data consistency guarantee for data grids [J].IEEE Transactions on Computers, 2014, 63 (12): 2975–2987
[26] B. Liskov, J. Cowling. Viewstamped replication revisited [R]. Cambridge: DSpace@MIT, July 23, 2012
[27] H. Howard, D. Malkhi, A. Spiegelman. Flexible Paxos: quorum intersection revisited[J]. Distributed, Parallel, and Cluster Computing, 2016: 1–20
[28] Wood T, Ramakrishnan K K, Shenoy P, et al. CloudNet: dynamic pooling of cloud resources by live WAN migration of virtual machines [J]. IEEE/ACM Transactions on Networking, 2011, 46(7): 121-132.
[29] B. Liskov, J. Cowling. Viewstamped replication revisited [R]. Cambridge: DSpace@MIT, July 23, 2012
[30] P. Li, D. B. Gao, M. Reiter. Replica placement for availability in the worst case [C]. 2015 IEEE 35th International Conference on Distributed Computing Systems (ICDCS), Columbus, 2015, 599–608
[31] C. Clark, K. Fraser, S. Hand, J. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield. Live migration of virtual machines. In Proceedings of NSDI, May 2005.
[32] B. Cully, G. Lefebvre, D. Meyer, M. Feeley, N. Hutchinson, and A. Warfield. Remus: High availability via asynchronous virtual ma- chine replication. In NSDI, 2008.