Blockchain enabled Virtualized Cloud Security Solutions

Subjects: Computer Science, Cybernetics
Contributor: Mueen Uddin

Cloud computing is a well-known technology that provides flexible, efficient, and cost-effective IT solutions for multinationals to offer improved and enhanced quality of business services to end-users. The cloud computing paradigm is instigated from the grid and parallel computing models.

Keywords: blockchain ; cloud data centre ; cloud vulnerabilities

1. Introduction

In today's Digital World era, everything is available and accessible on the Internet through various technology-enabled solutions. Cloud computing is a data storage and access platform where client data is stored and accessed through digital devices and gadgets from any location using the Internet platform. It provides end-users with the facility to research out their data records, software and application tools, infrastructure platforms, and several additional cloud-enabled services and facilities effortlessly. The current revolution in information edge in big data and IoT engenders several security-related challenges that need to be solved and appropriately handled to help business enterprises grow and make better decisions for their business benefits. One of the critical questions is: how to store, access, and adequately manage these enormous quantities of data being generated through Information Communication Technology (ICT). Cloud computing provides the most flexible, reliable, and efficient ways to handle this vast data using cloud data centres called data farms or server farms. These facilities comprise millions of server machines arranged and placed in different infrastructures and models such as blade servers, racks, etc., to provide on-demand provisioning services and facilities to end-users and business firms [1]. The cloud computing platform is an innovative, extended, and improved computing facility compared to existing computing models such as grid and parallel computing, autonomic, and utility computing infrastructures based on a centralized client-server computing model being implemented and deployed in large tier level data centres [2]. It provides a ubiquitous service distribution model where different infrastructure facilities are provided to end-users in a wide range of personal file-sharing services to enterprise data warehouses [3].

It is essential to highlight that today's virtualized tier level cloud computing platforms require improved collaboration, responsiveness, promptness, and scalability features involving new technologies to enable better and dynamic on-demand service allocation and provisioning at the client level to support and enhance industrial throughputs, global competitive advantage using business analytical tools, etc. [4][5]. As cloud computing provides efficient, reliable, flexible, scalable, cost-effective, and agility-based solutions, its usage, adoption, and migration have tremendously enlarged and helped business enterprises earn better revenues every year [6]. This trend is helping CSPs, and their market share is increasing to more than 12% in software-based companies only, with increased revenue of almost $95 billion in the next five years of technology [7]. One of the significant advantages of cloud computing is its reliable and high-speed X as a Service (XaaS) facility, where different application and computing development processes and platforms are provided to clients on-demand, enabling them to save huge costs of installations and deployments as shown in **Figure 1** [8][9].

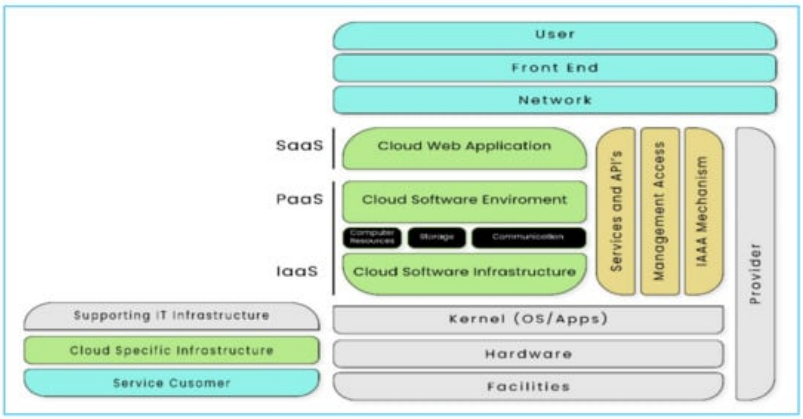

Figure 1. Cloud Reference Architecture.

In a virtualized cloud computing infrastructure facility, different types of services provided by CSPs include Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS) where cloud users can easily download and upload their required content from cloud storage and network systems, from anyplace and anywhere in the world using high-speed Internet [10][11]. The profligate rising of cloud computing adoption and migration is unavoidable. Most people are becoming more and more dependent on technology by storing their sensitive data and information on outsourced cloud platforms owned by CSPs. It is causing severe security risks and breaches, allowing attackers and cybercriminals to break into clients' data and services and cause substantial potential losses to cloud infrastructure platforms and systems [12]. Some of the major cloud security breaches include security at the physical level, virtual level, and, more importantly, web-based level in tier level virtualized cloud data centres [13][14]. Furthermore, there are security gaps between end-user and vendor assessments of cloud security, privacy, and transparency [15]. Similarly, the majority of enterprises with sensitive data, such as banks, financial institutions, insurance companies, etc., are also very reluctant to choose cloud computing services and platforms, as their primary concerns revolve around the integrity, privacy, secrecy, and confidentiality of their data being stored and accessed from the cloud platform [16].

The services provided by virtualized cloud infrastructure act as a black box to the end-user who has no idea or visibility about the location of actual storage and network mechanisms being used in the cloud data centre. In a multi-tenant environment, where a client has no idea about what is happening inside the cloud infrastructure, this engenders different vulnerabilities such as the CSP system administrator being able easily to change the operational functionality of different virtual machines (VMs) running in the facility as well as to modify the user authentication and authorization rules on behalf of CSPs, interrupting and changing user privacy and data integrity settings. Some of the existing virtualized cloud-enabled solutions such as VPNs, Firewalls, security policies, and procedures provide data and service security protocols and solutions such as differential-privacy mechanisms. However, lack of privacy and transparency controls on both the CSP side and client-side along with connectivity amongst the cloud vendors and their interactions can be easily abused by the attackers and assailants to unveil attacks, such as triggering linkages attacks against differential-privacy protection methods, and data mining-based linkage attacks as shown in **Figure 2** [17].

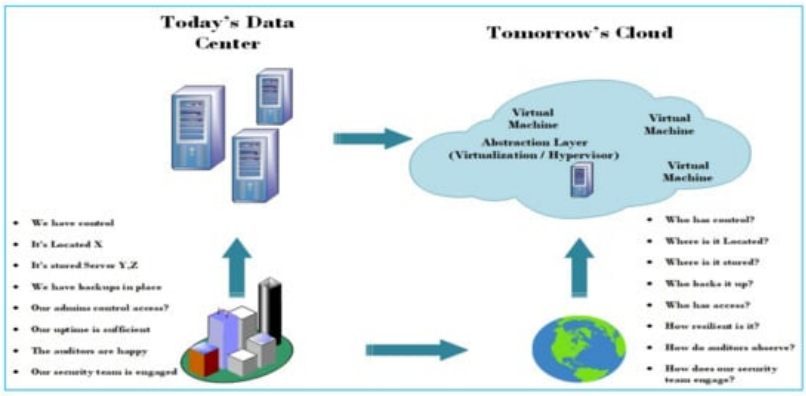

Figure 2. Cloud Computing Challenges.

Blockchain is one of the latest core technologies that has drawn attention as a next-generation promising solution for the problems mentioned above highlighted in cloud computing infrastructures in the recent information era. It helps to create a decentralized network of untrusted participants (peers) where a ledger of blocks of records is created. It enables us to establish an authentication system for peer nodes to share securely virtual cash, services, and encrypted transactions on

the network to develop a secure and trusted relationship among the participating peers [18]. Blockchain helps CSPs to handle (distribute, store, and record) cloud transactions and services effectively in a way that does not compromise end-users' Quality of Service (QoS), and acts as middleware technology to provide sensitive data protection, avoid delays in sensitive data, and avoid delays in searching and sorting vast chunks of data being stored and processed on the cloud platform using encrypted cryptographic methods [19].

Blockchain technology provides resilience in cloud infrastructure by creating a distributed ledger of processed and executed transactions on the cloud platform. It diminishes the problem of a single point of failure as provided by the cloud paradigm [20]. It also enhances transparency and scalability in the cloud network by improving the computation power through the number of distributed peers in the network without using a centralized computing model. The encrypted security model supported by blockchain also enhances the security and integrity of data being stored and processed on the cloud infrastructure through robust cryptographic hashing mechanisms such as SHA-256 or encryption using ECC or RSA to generate digital signatures for every transaction being processed or accessed on the network [21].

Furthermore, blockchain technology also helps cloud computing CSPs to offer the best approach for the application developers to create a virtual database of their services and transactions with one click, just as Pay-Per-User can be used to improve the autonomy of their cloud services further since these services will be carried out through a decentralized mechanism where functionalities are performed autonomously without the intervention of central authorities. This process enhances the trustworthiness amongst the participating clients as QoS information is persistent and cannot be modified [22].

2. Problem Background

Cloud computing technology has become another buzzword after the introduction of Web 2.0 to Web 5.0. It provides on-demand services such as storage, processing, infrastructure, etc., to business enterprises over the Internet. It supports another vision of IT whereby programming applications and computational resources are pooled and provisioned as organizations and end-users demand these services over virtualized ICT infrastructures accessible through the Internet [23]. The end-users do not need to have built-in computing and network infrastructure to use these services provided by a cloud computing platform. The collaboration and integration of cloud computing with industrial applications have currently brought many security issues and challenges for both the CSPs and the clients [24]. Cloud computing supports inclinations for customers (i.e., end-users and pro-communities), which can refit some part of their businesses to the cloud infrastructures, helping them in lessening the cost of ownership, working, and keeping up the enrolling establishment, as well as in growing flexibility and scalability by adopting to cloud platforms [25].

2.1. Cloud Data Centre Security Concerns and Threats

One of the critical challenges faced by today's clouds is their data level security, as the majority of the enterprise's sensitive and vital data needs proper security measures as hackers can steal the business data, such as daily sales, profit reports, financial reports, etc. [26]. These security issues pose substantial barriers to adopting cloud-enabled solutions in business enterprises, especially the cloud services provided by trusted and non-trusted third-party service providers [27]. Thus, cloud computing paradigm apprehensions with traditional data privacy, data integrity, accessibility, and privacy issues need to be sorted out and solved using the newest technologies and techniques [28]. So far, our work has focused on discussing various security threats in the cloud environment. However, while promising virtually unlimited storage and computing power, the cloud paradigm introduces latency to the equation, which might not be acceptable in specific scenarios.

Furthermore, the cloud paradigm introduces several security vulnerabilities to the infrastructure. This paper revolves around IaaS security issues and challenges, where traditional virtualization functionalities are commonly used. A break in the virtualized infrastructure's security opens a direct gateway for attackers to ambush unswervingly on organizational layers, making such attacks more prevailing and perilous [29]. The majority of cloud users are uninformed about the risks of storing and communicating their private data and information in a shared virtualized cloud environment. Therefore, critical technological restraints such as transparency, multi-tenancy, velocity-of-attack, information assurance, data privacy and ownership, compliance, encryption, and integrity should be handled more prudently. It implies that the clients are entirely not secure and immune to the threats in their cloud infrastructures. It calls for an appropriate secure cloud mechanism to be developed and deployed to handle today's Internet technologies [30]. This paper also discourses various security issues at different levels in virtualized data centre infrastructures, threats, and specific solutions provided by blockchain technology. Some of the prevalent virtualized security issues are explained below.

- Multitenancy (more for CSP compared to Client)

- Velocity of attack (more for CSP compared to Client)
- Information assurance (Client)
- Data privacy and ownership (Client)

2.1.1. Multitenancy

Multitenancy has been recognized as one of the significant security issues in a virtualized cloud computing model. It is defined as a shared virtualized environment where computing resources are shared, i.e., separate virtual machines are operating and processing in the same physical server machine to achieve economic gain. It directly enables attackers with information leakage and increased attack surface that directly affects the integrity, confidentiality, privacy, and trust issues. It creates new targets for intrusions as both the attacker and the victim share the same physical server machine. The major problem in a multitenancy environment is “how to assure data isolation in a multi-tenant environment?”. It needs a vertical solution from the Software-as-a-Service (SaaS) down to Infrastructure-as-a-Service (IaaS). Regardless of the advantage of multitenancy (distributed processing groundwork) to a CSP, it is an enormous security stress for cloud clients [31].

2.1.2. The “Velocity-of-Attack”

The virtualized cloud computing infrastructure harnesses the power of thousands of computing nodes, combined with the homogeneity of the hosts’ operating system. It leads to a situation where any present security threat will spread and amplify more rapidly, called the “speed of ambush” factor, and has a more significant impact than a typical client-server network. It is essential to highlight that the hosts in a virtualized environment must understand their trust boundaries and responsibilities to secure the cloud environment set by CSPs before moving to the cloud [32][33].

2.1.3. Information Assurance

The issues of end-to-end security, privacy, and business integrity and continuity are of greater complexity in a cloud computing world than in a single data centre. Some critical issues of cloud security include trust, multitenancy, encryption, and compliance. Information assurance is collecting innumerable information practices that cloud computing service providers and vendors must follow and implement to certify the privacy, secrecy, confidentiality, integrity, accessibility, and availability of their customers’ information and data stored on cloud storage. It is one of the foremost security characteristics and apprehensions which makes sure that every client working on the cloud infrastructure is real and are appropriately authenticated and authorized with legitimate rights and extensions assigned to them by CSPs [34].

2.1.4. Data Privacy and Ownership

Information protection and ownership are key cloud security issues for clients. It guarantees that information stored in the cloud is “sheltered.” Data privacy and proprietorship explicitly identify the menaces of unapproved information exposure due to a lack of privacy policies in cloud infrastructure. Clients do not know if the third-party or cloud computing vendors have privacy policies similar to or better than their policies. Therefore, CSPs’ responsibility is to let a client create and assign an access control list outlining how, when, and by whom the data will be accessed. Moreover, clients also fear that their critical and confidential data are being viewed by cloud vendors and owners while stored and processed. They also want to see the access logs and audit trails of all cloud users and vendor employees. Furthermore, cloud CSPs and vendors might need provisions for external audits on their infrastructure and controls [35]. A CSP needs to guarantee that private and Personally Identifiable Information (PII) about its customers is lawfully shielded from unapproved exposure. Confidential information includes:

- Single user Identification on Cloud
- Clients’ details as per request
- Ownership of client data

2.2. Virtualization-Specific Vulnerabilities, Security Concerns, and Threats

In its technological uprising, virtualization technology enables us to implement cloud computing key attributes by creating a virtualized environment from abstract hardware resources (servers, storage, and other network equipment) by separating operational functionalities from the underlying hardware devices. It allows the creation, installation, configuration, effective allocation, and adjustment of multiple VMs on a different physical host machine (servers). The hypervisor, also called the Virtual Machine Monitor (VMM), one of the critical components of virtualization technology in

the cloud computing paradigm, offers significant benefits in terms of functional segregation, performance isolation, live-migration-enabled load balance, fault tolerance, portability of applications, and higher resource utilization [36]. However, the design, implementation, and deployment of virtualization technology also open up new threats and security vulnerabilities and is being targeted by attackers for malicious activities in the cloud infrastructures.

IaaS permits the clients to access different VMs and install their own operating systems as needed to perform their computational queries without installing appropriate security measures and solutions. Unfortunately, these types of settings in virtualized cloud infrastructures create significant vulnerabilities and limitations when we perform security-critical computations and store sensitive data. For example, there are no secure means currently available that guarantee the trustworthiness and fidelity of a Virtual Machine (VM) in terms of its origin and identity and the reliability of the data being uploaded, stored, and processed by server machines and storage devices [37]. Furthermore, other attack pathways, such as predefined and prebuilt VMs and other virtual equipment and appliances carrying malicious and malevolent codes, erroneously configured virtual firewalls, Intrusion Detection Systems (IDS) systems and networks, an inaccurately installed and configured hypervisor, and information leakage or VM escape through offline configurations. In reality, protecting a VM is more complicated and resource-consuming compared to physical machines [38]. Furthermore, multiple clients sharing the same virtualized environment can cause security vulnerabilities, as many components involved in the configuration process create complex management issues, leading to DDoS types of service attacks and losing clients' sensitive and critical data [39]. Another problem is the deficiency of trust among participating clients with their data privacy and data assurance requirements.

One of the significant issues in the virtualized cloud data centre is protecting clients' sensitive data from leaking over the Internet from attackers and unwanted people [40]. On the other hand, the stored data in the storage devices are unencrypted and handled by a different type of cloud administrators hired by CSPs, causing trust and integrity issues [41]. These vulnerabilities and limitations require a macro-level solution for identified common cloud infrastructure level security threats and concerns to provide secure, efficient, and transparent services to cloud end-users. Cloud vendors and CSPs are putting substantial costs and exertions in securing their virtualized cloud infrastructures to achieve maximum compliance with the prevailing industry security services management standards, such as Amazon Cloud lately accomplished the Payment Card Industry Data Security Standard (PCIDSS) compliance certification and Microsoft Azure Cloud prerogatives compliance with ISO27001 security standards [42]. However, cloud-based applications and services' overall security still needs better implementation and configuration services and advanced security services with fine-grained access controls bonded between virtualized services such as IaaS, SaaS, and PaaS cloud virtualization platforms.

This section has identified and evaluated numerous virtualized cloud security issues and challenges revealed in recent years in diverse virtualization components, such as VMM, VMs, and guest operating systems, and disk storage images and devices [43]. Attackers use specific malicious and spiteful programs and tools in VMs to get illegal access permissions to record and log different screen updates and keystrokes across physical and virtual server machines (terminals) to gain sensitive and critical information required. Once a cloud network is compromised, it becomes relatively easy to duplicate and copy live VM images to create and configure new VM image files causing VM image sprawl. In this vulnerability, a colossal number of rogue VMs are created to generate DDoS and other types of network attacks. Similarly, attackers and intruders cause hypervisor-based attacks to exploit the vulnerabilities. The hypervisor controls multiple operating systems to operate concurrently on a single hardware platform, usually the physical server machine. A hacked and compromised hypervisor allows hackers to attack and control each VM installed and configured on a virtual host. Attackers use different APIs, software stacks, and coding bugs to control the degree of security assurance for the privacy and secrecy of cloud environments [44]. **Figure 3** highlights various attack types in different virtualized environments.

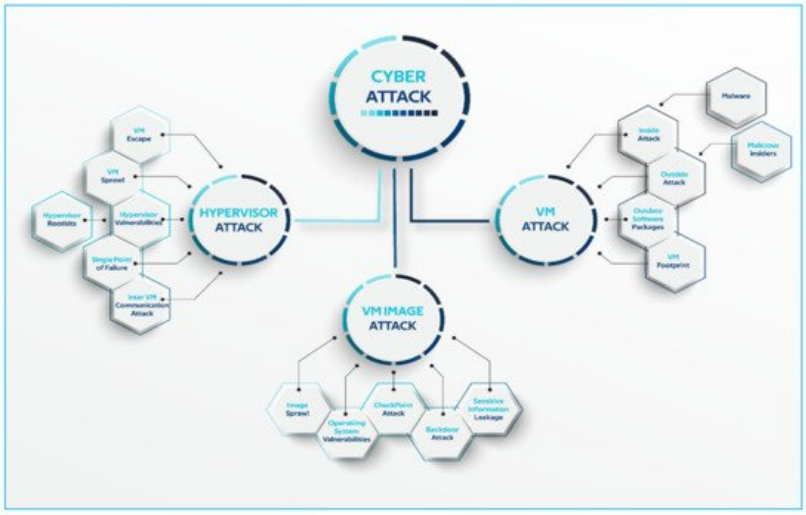

Figure 3. Virtualization Attack Types.

2.2.1. VM Theft or VM Stealing

Hypervisor vulnerabilities allow an attacker to use VMs for a longer duration of time. By changing/manipulating the set configurations, such as memory, CPU, and cache manipulations, an attacker is permitted to hijack the VM along with its resources. This type of attack is also called VM theft or VM stealing or theft-of-service attack, as VMs have insufficient security controls permitting their unapproved duplication of development [45]. In this attack, the cloud infrastructure is financially affected, along with no record or logs of the user's activities, leading to further risks related to the cloud paradigm. VM theft can be restricted by applying Duplicate and Move restrictions on VMs, which have more sensitive and critical data. This solution is considered an underlying security mechanism where VMs are limited/tied to function and operate in a fixed secure physical server machine to stop VM duplication. A VM with duplicate and move limitations cannot run on a hypervisor familiarized with other physical machines; hence, its movement and duplication can be prevented. Even though these limitations are fundamental to the protection of VMs against VM theft, it still has several disadvantages, such as limiting the VM's crosswise movement across multiple physical machines to share and execute different workloads based on applications being executed [46].

2.2.2. VM Escape

In a virtualized cloud infrastructure, VMs are designed and created to support secure isolation between the host physical machines and VMs. Virtual machine escape is a security vulnerability within a VM or the whole virtualized cloud infrastructure. An attacker exploits the operating system's exposures running inside a virtual machine and inserts malicious code. When a VM executes this malicious package code, it allows the attacker to access and control the virtual network's primary hypervisor. It further breaks up the isolated boundaries between several VMs, thus bypassing the hypervisor to interconnect with other VMs in the network directly and get control of the host. It creates privacy, integrity, and trust issues in the cloud infrastructure and opens up the doors for other attackers to access and control other host machines and launch further attacks. These attacks include VM creation, VM manipulation, VM deletion, resource quota amendment, and changes, etc., and the attacker can also play with access privileges allocated to explicit VMs [47].

2.2.3. VM Sprawl and VM Image Sprawl

Virtual machine sprawl or virtualization sprawl and VM image sprawl is a situation in a virtualized cloud infrastructure. Cloud vendors, CSPs, and cloud administrators have no effective control and management over the creation, deletion, and configuration of VMs and their image files during the live migration process. The sprawl also includes resources shared and provisioned to these VMs such as memory, cache, storage, network channels, CPU, etc. This scenario underutilizes these resources as they cannot be assigned to other VMs because of a lack of control and proper management of these cloud resources [40]. This situation usually occurs when multiple VMs are created and set up by different departments in the same enterprise without the knowledge, control, policies, and proper procedures followed by cloud administrators. It leads to the formation of bottlenecks on server machines, which further leads to crashed systems because of low resource availability in a cloud environment.

2.2.4. VM Inside and Outside Attacks

Virtual machines can be attacked and infected with malware and operating system rootkits. An attacker can have multiple perspectives. An inside attacker always wants to attack a cloud data centre's IT infrastructure for personal gains. Another

attacker can be a rouge CSP administrator or an inside employee who intends to exploit cloud vulnerabilities for getting access to sensitive and critical information. It can also be a cloud owner with malicious intent. In this attack, the attackers get complete control of the VMs in the facility and ultimately control the whole network to create illegitimate copies and backups of VMs, delete and modify several VMs service-level-agreements and can log in to a customer's VMs for administrative purposes [23].

In outside attacks, VMs are co-located and connected through virtual network connections, shared memory, and other shared resources. A malicious VM inside this network can determine where another VM's allocated memory lies. It allows this VM to read or write to that specific location and interfere with the other's operation [37].

2.2.5. VM Cross Side-Channel Attack

In virtualized cloud infrastructures, resource sharing techniques such as deduplication of data and co-location of computation (multiple VMs placed on the same physical server machines) are critical for enhancing the efficiencies of VMs. However, they also increase the security risks to OpenSSL AES implementations as they build a powerful cache-based attack on AES and recover the keys of an AES implementation in a targeted VM. Therefore, it is essential to highlight that long-term co-location of computation should not be allowed along with the deduplication of data being disabled. In these cross VM side-channel attacks, a malicious VM can quickly penetrate the isolation between several VMs and get access to shared hardware and software resources and cache locations to extract confidential information from the target VMs [34].

2.2.6. Outdated Software Packages in VMS

Obsolete software packages in virtualized cloud environments allow us to create and install new low-cost VMs for performing diverse tasks, extend and branch new VMs based on old ones, create image files of existing VMs, and even roll back machines to previous states [41]. These operations pose serious security threats, and implications such as a VM rollback may depict a software bug or vulnerability that has already been fixed.

2.2.7. Hyperjacking

A hypervisor or VMM is installed to execute several guest VMs and applications concurrently on a single host physical server machine and provide separation amongst the guest VMs in a cloud environment [33]. These hypervisors are vulnerable and prone to attacks from various hackers. Hyperjacking is an attack on the hypervisor. In this attack, hackers inject a rogue hypervisor or take malicious control over the installed hypervisor between the target system and the hardware to control the internal server resources within a virtualized cloud environment. The attacker tries to attack the target operating system below the VMs to execute its malicious code and applications on VM [48]. The most important thing about the hypervisor is that attackers can efficiently run unauthorized applications over the system without realizing any suspicious activity to the administrator. It is essential to highlight that regular security measures such as firewalls, IDS systems, and other antivirus tools are ineffective against these threats. The operating system, running above the rogue hypervisor, is unaware that the machine has been compromised.

2.2.8. Data Leakage

Confidential and sensitive data stored on third-party cloud storage platforms are potentially vulnerable to unauthorized access and manipulations. In cloud environments, when secure shell protocols are employed to encrypt and secure the stored data on virtual disks and communication between different VMs, hackers still apply different types of attacks such as side-channel attacks, which give hackers complete control of the CSPs' network. The hackers can efficiently extract useful and secret information such as a client's password lists and snatch personal and confidential data stored on cloud disks. Another vulnerability can be the hypervisor's compromise, which compromises the security of all VMs running on that hypervisor [49]. It is essential to highlight that all encrypted data will ultimately be stored in plain text in memory; otherwise, reading and writing become impossible using an editor.

Consequently, everything on the editor will be unsafe and insecure, causing the data to be naked and accessed by any unauthorized user in the cloud environment. Another possible vulnerability for data leakage happens during the live and offline VM migration process when VMs are transferred from source hosts to destination hosts while running. In this scenario, the current state of a running VM and other sensitive information stored in memory pages, etc. can be leaked while being transferred from source to destination. It can cause security vulnerability towards stored data integrity and confidentiality [50].

2.2.9. Denial of Service (DoS)

Denial of Service (DoS) attacks impend the cloud vendor's and CSPs' aptitude to respond to authentic clients' requests, which results in substantial economic losses. During DoS attacks, legitimate cloud users are prevented from accessing their data, resources, or services they want to use and access. During this attack, the hackers can create and install rouge and malicious VMs inside, which exhaust and block all the server resources and services from being provided to cloud users. These VMs can be used to initiate DoS and DDoS attacks against the hypervisor or any other VM that runs on the same hypervisor. These attacks can also be conducted against application software, such as operating systems and network components with servers or network routers, etc., to exploit weaknesses and vulnerabilities in communication protocols [51]. DoS attacks can also be applied against the hypervisor, where the attacker intends to utilize maximum resources and services memory, bandwidth, CPU cycles, etc. to degrade the cloud environment's performance by leveraging the hypervisor's design flaws and misconfigurations [47]. DoS attacks can also occur because of the weaknesses in various communication protocols such as TCP Sessions hijacking, IP Spoofing, and Corrupting DNS Server Cache.

3. Blockchain-Enabled Cloud Security Related Work

In the literature, research work on cloud security and blockchain is limited, with most work being engrossed in leveraging blockchain technology to benefit cloud computing security in general. The recent growing interest in integrating blockchain and cloud computing infrastructures has created many opportunities for researchers and cloud service providers to propose new innovative and commercial solutions involving next-generation blockchain-enabled cloud systems. Zhao propose a differentially private data sharing model in a cloud federation using blockchain technology. This model enables distributed resource provisions using a single cloud under the management of the blockchain network. Notably, the security is improved using blockchain-enabled smart contracts to allow distributed data control by cloud owners [52]. Sharma proposes a cryptocurrency-enabled blockchain solution for reducing cloud security risks [53].

Ali et al. [54]. propose a secure data provenance model in the cloud-centric Internet of things via blockchain smart contracts to achieve better cloud security and privacy. Waheed suggested a mobile intercloud system with blockchain to support complex cloud collaborative scenarios. Alcaraz, Cristina et al. discussed various security threats and their possible countermeasures for cloud-based IoT. The authors describe user identity and location privacy, cloud node compromising, layer removing or adding, and key management threats for clouds. The authors describe how blockchain-enabled platforms can facilitate and support the autonomous workflow and the sharing of services among cloud users and devices [55]. Nguyen introduces a mechanism for securely handling decentralized edge micro clouds' collaborative governance with blockchain-based distributed ledgers. This technique builds a joint cloud blockchain to secure decentralized collaborative governance services, i.e., storage, monitoring, and resource management for suitable performance on lightweight cloud computing nodes [56].

Tavana proposes a BCoT system for handling security-critical applications in cloud scenarios between cloud service providers, clients, and cloud devices. Their strategy was based on a forensic investigation framework using a decentralized blockchain platform [57]. Wang presents a blockchain-based data protection mechanism for cloud users to prevent inappropriate cloud data movement in cloud services and applications due to malicious tampering in Virtual Machine (VM) migration on cloud computing platforms [58]. Ruqia proposed Mchain: blockchain-based VM measurements secure storage approach in IaaS cloud with enhanced integrity and controllability in the same course. In this architecture, a two-layer blockchain network comprising a data validation layer and a PoW task layer is integrated with the IaaS cloud to enhance system integrity [59]. Zhang et al. propose blockchain-based public integrity verification for cloud storage against procrastinating auditors. This system's implementation demonstrates that blockchain technology has enormous potential to benefit cloud computing infrastructures to overcome controllability and performance problems in low system overhead and high data integrity [60].

References

1. Nzanywayingoma, F.; Yang, Y. Efficient resource management techniques in cloud computing environment: A review and discussion. Int. J. Comput. Appl. 2018, 41, 165–182.
2. Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. Integration of Cloud computing and Internet of Things: A survey. Future Gener. Comput. Syst. 2016, 56, 684–700.
3. Moura, J.; Hutchison, D. Review and analysis of networking challenges in cloud computing. J. Netw. Comput. Appl. 2016, 60, 113–129.

4. Alves, M.P.; Delicato, F.C.; Santos, I.L.; Pires, P.F. LW-CoEdge: A lightweight virtualization model and collaboration process for edge computing. World Wide Web 2020, 23, 1127–1175.
5. Suleiman, H.; Basir, O. Service Level Driven Job Scheduling in Multi-Tier Cloud Computing: A Biologically Inspired Approach. Comput. Sci. 2019, 9, 99–118.
6. Al-Mashhadi, S.; Anbar, M.; Jalal, R.A.; Al-Ani, A. Design of Cloud Computing Load Balance System Based on SDN Technology. Lect. Notes Electr. Eng. 2020, 603, 123–133.
7. Raju, C.J.; Babu, M.R.; Narayanamoorthy, M. Cost Effective Model for Using Different Cloud Services. In Emerging Research in Data Engineering Systems and Computer Communications; Springer: Singapore, 2020; pp. 313–319.
8. Loubière, P.; Tomassetti, L. Towards Cloud Computing. In TORUS 1—Toward an Open Resource Using Services: Cloud Computing for Environmental Data; John Wiley & Sons: Hoboken, NJ, USA, 2020; pp. 179–189.
9. Tripathi, A.K.; Agrawal, S.; Gupta, R.D. Cloud enabled SDI architecture: A review. Earth Sci. Inform. 2020, 13, 211–231.
10. Ehwerhemuepha, L.; Gasperino, G.; Bischoff, N.; Taraman, S.; Chang, A.; Feaster, W. HealtheDataLab—A cloud computing solution for data science and advanced analytics in healthcare with application to predicting multi-centre pediatric readmissions. BMC Med. Inform. Decis. Mak. 2020, 20, 115.
11. Wagh, N.; Pawar, V.; Kharat, K. Educational Cloud Framework—A Literature Review on Finding Better Private Cloud Framework for Educational Hub. In Microservices in Big Data Analytics; Springer: Singapore, 2020; pp. 13–27.
12. Vähäkainu, P.; Lehto, M.; Kariluoto, A.; Ojalainen, A. Artificial Intelligence in Protecting Smart Building's Cloud Service Infrastructure from Cyberattacks. In Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity; Springer: Cham, Switzerland, 2020; pp. 289–315.
13. Chitturi, A.K.; Swarnalatha, P. Exploration of Various Cloud Security Challenges and Threats. In Soft Computing for Problem Solving; Springer: Singapore, 2020; pp. 891–899.
14. Mthunzi, S.N.; Benkhelifaa, E.; Bosakowskia, T.; Guegan, C.G.; Barhamgic, M. Cloud computing security taxonomy: From an atomistic to a holistic view. Future Gener. Comput. Syst. 2020, 107, 620–644.
15. Chadwick, D.W.; Fan, W.; Costantino, G.; De Lemos, R.; Di Cerbo, F.; Herwono, I.; Manea, M.; Mori, P.; Sajjad, A.; Wang, X.-S. A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Gener. Comput. Syst. 2020, 102, 710–722.
16. Uddin, M.; Memon, M.S.; Memon, I.; Ali, I.; Memon, J.; Abdelhaq, M.; Alsaqour, R. Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. CMC Comput. Mater. Continua. 2021, 68, 2377–2397.
17. Juma, M.; Monem, A.A.; Shaalan, K. Hybrid End-to-End VPN Security Approach for Smart IoT Objects. J. Netw. Comput. Appl. 2020, 158, 102598.
18. Varga, P.; Peto, J.; Franko, A.; Balla, D.; Haja, D.; Janky, F.; Soos, G.; Ficzere, D.; Maliosz, M.; Toka, L. 5G Support for Industrial Iot Applications—Challenges, Solutions, and Research Gaps. Sensors 2020, 20, 828.
19. Zahmatkesh, H.; Al-Turjman, F. Fog computing for sustainable smart cities in the IoT era: Caching techniques and enabling technologies—An overview. Sustain. Cities Soc. 2020, 59, 102139.
20. Shahid, F.; Khan, A.; Jeon, G. Post-quantum distributed ledger for internet of things. Comput. Electr. Eng. 2020, 83, 106581.
21. Hassan, H.E.-R.; Tahoun, M.; ElTaweel, G. A robust computational DRM framework for protecting multimedia contents using AES and ECC. Alex. Eng. J. 2020, 59, 1275–1286.
22. Chen, N.; Li, F.; White, G.; Clarke, S.; Yang, Y. A Decentralized Adaptation System for QoS Optimization. Fog Fogonomics 2020, 213–247.
23. Baker, T.; Asim, M.; MacDermott, Á.; Iqbal, F.; Kamoun, F.; Shah, B.; Alfandi, O.; Hammoudeh, M. A secure fog-based platform for SCADA-based IoT critical infrastructure. Softw. Pract. Exp. 2020, 50, 503–518.
24. Ahmed, M.; Jaidka, S.; Sarkar, N.I. Security in decentralised computing, IoT and industrial IoT. In Industrial IoT; Springer: Cham, Switzerland, 2020; pp. 191–211.
25. Firouzi, F.; Farahani, B. Architecting IoT Cloud. In Intelligent Internet of Things; Springer: Cham, Switzerland, 2020; pp. 173–241.
26. Chandel, S.; Ni, T.-Y.; Yang, G. Enterprise cloud: Its growth & security challenges in China. In Proceedings of the 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Shanghai, China, 22–24 June 2018; pp. 144–152.
27. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. Int. J. Crit. Infrastruct. Prot. 2019, 25, 36–49.

28. Singh, N.; Singh, A.K. Data privacy protection mechanisms in cloud. Data Sci. Eng. 2018, 3, 24–39.
29. Bartolini, C.; Santos, C.; Ullrich, C. Property and the cloud. Comput. Law Secur. Rev. 2018, 34, 358–390.
30. Baumann, A.; Peinado, M.; Hunt, G.C. Shielding applications from an untrusted cloud with Haven. In Proceedings of the 11th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2014, Broomfield, CO, USA, 6–8 October 2014; pp. 267–283.
31. Aljahdali, H.; Albatli, A.; Garraghan, P.; Townend, P.; Lau, L.; Xu, J. Multi-tenancy in cloud computing. In Proceedings of the 2014 IEEE 8th International Symposium on Service Oriented System Engineering, Oxford, UK, 7–11 April 2014; pp. 344–351.
32. Jayanetti, A.; Buyya, R. J-OPT: A Joint Host and Network Optimization Algorithm for Energy-Efficient Workflow Scheduling in Cloud Data Centres. In Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing, Auckland, New Zealand, 2–5 December 2019; pp. 199–208.
33. Morabito, R.; Petrolo, R.; Loscrì, V.; Mitton, N. Reprint of: LEGIoT: A Lightweight Edge Gateway for the Internet of Things. Future Gener. Comput. Syst. 2019, 92, 1157–1171.
34. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Comput. Sci. Rev. 2019, 33, 1–48.
35. Kadam, S.; Motwani, D. Blockchain based E-healthcare record system. In International Conference on Image Processing and Capsule Networks; Springer: Cham, Switzerland, 2020; pp. 366–380.
36. Tank, D.; Aggarwal, A.; Chaubey, N. Virtualization vulnerabilities, security issues, and solutions: A critical study and comparison. Int. J. Inf. Technol. 2019, 1–16.
37. Pandi, G.S.; Shah, S.; Wandra, K. Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation. Procedia Comput. Sci. 2020, 167, 163–173.
38. Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion detection systems in the Internet of things: A comprehensive investigation. Comput. Netw. 2019, 160, 165–191.
39. Srinivasan, K.; Mubarakali, A.; Alqahtani, A.S.; Kumar, A.D. A survey on the impact of DDoS attacks in cloud computing: Prevention, detection and mitigation techniques. In Intelligent Communication Technologies and Virtual Mobile Networks; Springer: Cham, Switzerland, 2019; pp. 252–270.
40. Monge, M.A.S.; González, A.H.; Fernández, B.L.; Vidal, D.M.; García, G.R.; Vidal, J.M. Traffic-flow analysis for source-side DDoS recognition on 5G environments. J. Netw. Comput. Appl. 2019, 136, 114–131.
41. Van Der Werff, L.; Fox, G.; Masevic, I.; Emeakaroha, V.C.; Morrison, J.P.; Lynn, T. Building consumer trust in the cloud: An experimental analysis of the cloud trust label approach. J. Cloud Comput. 2019, 8, 6.
42. Castro, P.; Ishakian, V.; Muthusamy, V.; Slominski, A. The rise of serverless computing. Commun. ACM 2019, 62, 44–54.
43. Sierra-Arriaga, F.; Branco, R.; Lee, B. Security Issues and Challenges for Virtualization Technologies. ACM Comput. Surv. 2020, 53, 1–37.
44. Mavridis, I.; Karatza, H. Combining containers and virtual machines to enhance isolation and extend functionality on cloud computing. Future Gener. Comput. Syst. 2019, 94, 674–696.
45. Alwakeel, A.M.; Alnaim, A.K.; Fernandez, E.B. A survey of network function virtualization security. In Proceedings of the in SoutheastCon 2018, St. Petersburg, FL, USA, 19–22 April 2018; pp. 1–8.
46. Tiburski, R.T.; Moratelli, C.R.; Johann, S.F.; Neves, M.V.; De Matos, E.; Amaral, L.A.; Hessel, F. Lightweight security architecture based on embedded virtualization and trust mechanisms for IoT edge devices. IEEE Commun. Mag. 2019, 57, 67–73.
47. Zhang, X.; Zheng, X.; Wang, Z.; Li, Q.; Fu, J.; Zhang, Y.; Shen, Y. Fast and Scalable VMM Live Upgrade in Large Cloud Infrastructure. In Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems, Providence, RI, USA, 13–17 April 2019; pp. 93–105.
48. Alhenaki, L.; Alwatban, A.; Alamri, B.; Alarifi, N. A Survey on the Security of Cloud Computing. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 19–21 March 2019; pp. 1–7.
49. Win, S.S.; Thwin, M.M.S. Handling the Hypervisor Hijacking Attacks on Virtual Cloud Environment. In Advances in Biometrics; Springer: Cham, Switzerland, 2019; pp. 25–50.
50. Singh, S.; Sharma, P.K.; Moon, S.Y.; Moon, D.; Park, J.H. A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions. J. Supercomput. 2019, 75, 4543–4574.

51. Abbasi, H.; Ezzati-Jivan, N.; Bellaiche, M.; Talhi, C.; Dagenais, M.R. Machine Learning-Based EDoS Attack Detection Technique Using Execution Trace Analysis. J. Hardw. Syst. Secur. 2019, 3, 164–176.
52. Singh, S.; Sanwar Hosen, A.S.M.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access 2021, 9, 13938–13959.
53. Sharma, P.; Jindal, R.; Borah, M.D. Blockchain Technology for Cloud Storage: A Systematic Literature Review. ACM Comput. Surv. 2020, 53, 1–32.
54. Waheed, N.; He, X.; Ikram, M.; Usman, M.; Hashmi, S.S. Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM Computing Surveys (CSUR) 2020, 53, 1–37.
55. Alcaraz, C.; Rubio, J.E.; Lopez, J. Blockchain-assisted access for federated Smart Grid domains: Coupling and features. J. Parallel Distrib. Comput. 2020, 144, 124–135.
56. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. J. Netw. Comput. Appl. 2020, 166, 102693.
57. Tavana, M.; Hajipour, V.; Oveisi, S. IoT-based enterprise resource planning: Challenges, open issues, applications, architecture, and future research directions. Internet Things 2020, 11, 100262.
58. Wang, H.; Ma, S.; Dai, H.-N.; Imran, M.; Wang, T. Blockchain-based data privacy management with Nudge theory in open banking. Future Gener. Comput. Syst. 2020, 110, 812–823.
59. Ruqia, B.; Javaid, N.; Husain, A.; Hassan, N.M.; Hassan, H.G.; Memon, Y. Influential reasonable robust virtual machine placement for efficient utilization and saving energy. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing; Springer: Cham, Switzerland, 2019; pp. 549–561.
60. Zhang, Y.; Xu, C.; Lin, X.; Shen, X.S. Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors. IEEE Trans. Cloud Comput. 2019, 1.
