

Review

# Next-Generation Blockchain-Enabled Virtualized Cloud Security Solutions: Review and Open Challenges

Mueen Uddin <sup>1,\*</sup>, Anjum Khalique <sup>2</sup>, Awais Khan Jumani <sup>3</sup>, Syed Sajid Ullah <sup>4</sup> and Saddam Hussain <sup>5</sup>

<sup>1</sup> Digital Science, Faculty of Science, Universiti Brunei Darussalam, Jln Tungku Link, Gadong BE1410, Negara Brunei Darussalam

<sup>2</sup> Department of Computer Science, SZABIST Hyderabad, Sindh 71000, Pakistan; khalique4u@gmail.com

<sup>3</sup> Department of Computer Science, Shah Abdul Latif University, Khairpur 66020, Sindh, Pakistan; awaisjumani@yahoo.com

<sup>4</sup> Department of Electrical and Computer Engineering, Villanova University, Villanova, PA 19085, USA; sullah1@villanova.edu

<sup>5</sup> Department of Information Technology, Hazara University Mansehra, Khyber Pakhtunkhwa 21120, Pakistan; saddamicup1993@gmail.com

\* Correspondence: mueenmalik9516@gmail.com

**Abstract:** 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. It uses virtualization, server consolidation, utility computing, and other computing technologies and models for providing better IT solutions for large-scale computational data centres. It encompasses different services for supporting data storage, networking, and computing for facilities and amenities for businesses and multinational corporations. The enormous elastic on-demand cloud provisioning resources and services and datasets are processed and stored in tier-level virtualized cloud data centres operated by third-party service providers called cloud owners. The primary issue with these cloud service providers is to provide and maintain data security, privacy, and confidentiality and service availability and data support for end-users. This paper reviews, highlights, and discusses some of the common cloud computing vulnerabilities primarily related to virtualization platforms and their implementations while outsourcing services and resources to different end-users and business enterprises. We then provided blockchain-enabled solutions for virtualized cloud platforms involving both the end-users and cloud service providers (CSP) to address and solve various security and privacy-related vulnerabilities. These solutions will help the data centre industry to improve its virtualized cloud services and resource provisioning facilities. Finally, we discussed different blockchain-related implementation challenges in cloud infrastructures.

**Keywords:** blockchain; cloud data centre; cloud vulnerabilities; virtualization vulnerabilities; virtual machines



check for updates

**Citation:** Uddin, M.; Khalique, A.; Jumani, A.K.; Ullah, S.S.; Hussain, S. Next-Generation Blockchain-Enabled Virtualized Cloud Security Solutions: Review and Open Challenges. *Electronics* **2021**, *10*, 2493. <https://doi.org/10.3390/electronics10202493>

Academic Editors: Bin Han, Simon Pietro Romano and Patrick Seeling

Received: 30 May 2021

Accepted: 1 July 2021

Published: 13 October 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 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].

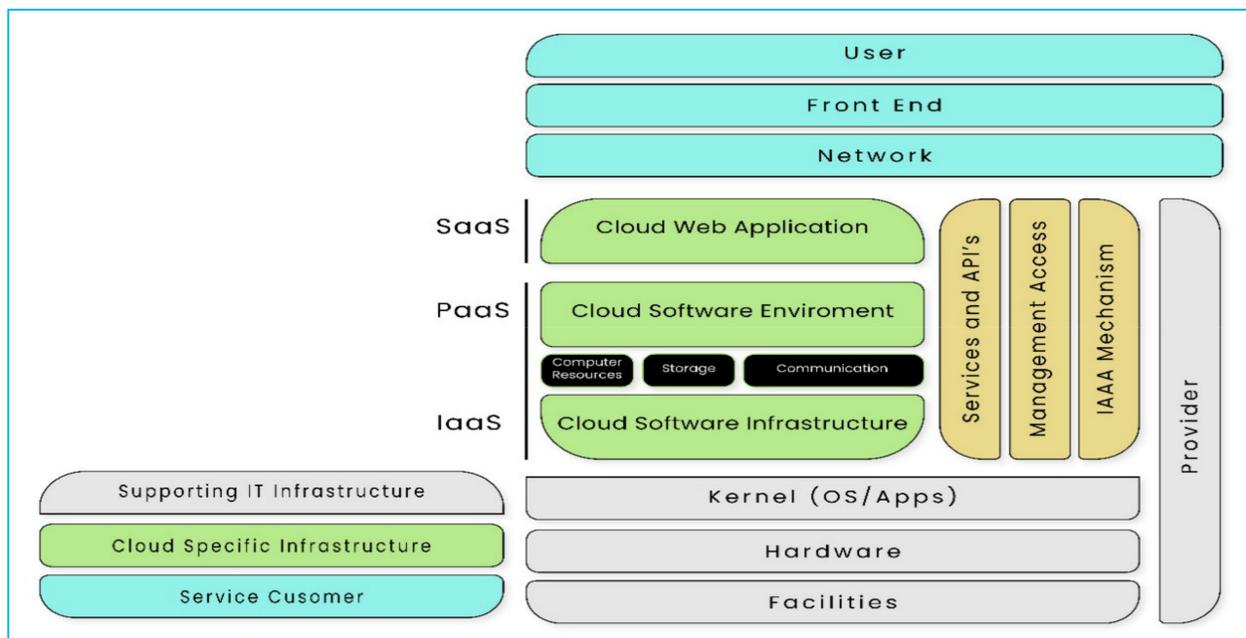


Figure 1. Cloud Reference Architecture.

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 comput-

ing 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].

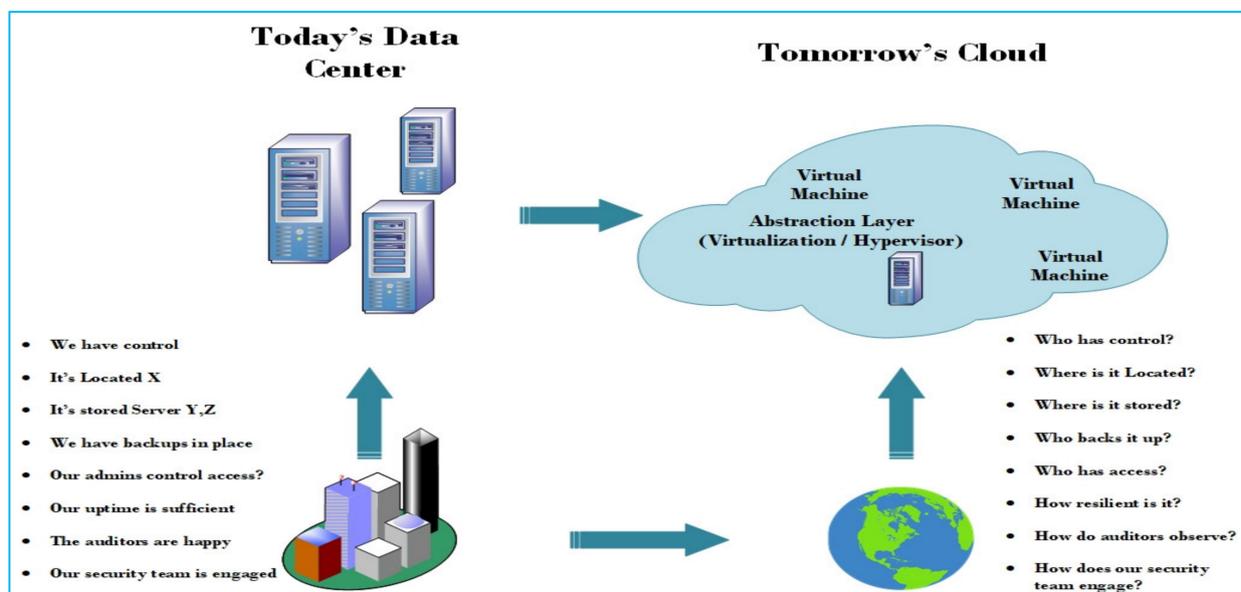


Figure 2. Cloud Computing Challenges.

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 vir-

tual 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]. This paper explores and evaluates various cloud security issues and threats happening at multiple cloud infrastructure levels, focusing on virtualization specific threats and vulnerabilities. It then provides Blockchain-enabled solutions for these problems highlighted to improve and enhance the services provided in virtualized cloud computing platforms.

## 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.

1. Multitenancy (more for CSP compared to Client)
2. Velocity of attack (more for CSP compared to Client)
3. Information assurance (Client)
4. 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 rogue 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].

Furthermore, Yang proposes a BCoT framework with a joint cloud computing collaboration environment where multiple clouds are interconnected securely through a P2P ledger network called IoT service based on a joint cloud blockchain: The case study of smart traveling [61]. Equations and mathematical expressions must be inserted into the main text. Two different types of styles can be used for equations and mathematical expressions. They are in-line style and display style.

#### 4. Blockchain as Technology Solution

A blockchain is an open, distributed, decentralized, shared, and immutable ledger technology that records the registry of assets and transactions between multiple parties across a peer-to-peer (P2P) network in an efficiently verifiable and permanent way. It comprises chained blocks of immutable data timestamped and validated by miners or participating stakeholders of the network replicated across multiple participants, each of whom collaborates in its maintenance. A blockchain platform is a (P2P) network environment where transaction records and parameters (value, state) are controlled through business logic using smart contracts. Blockchain uses Elliptic Curve Cryptography (ECC) and various hashing mechanisms such as SHA-256 to provide strong cryptographic proof for data authentication and the integrity system [62].

The block data contain a cryptographic list of all performed transactions and a hash to the ledger network's previously stored block. The new information recorded on the ledger is immutable and append-only. It helps create and provide a cross-border global distributed trust among various participating stakeholders to determine the information provenance, called the "System of Proof". It enables us to develop faster settlements, increased network capacity (scalability), enhanced transparency, enhanced integrity, and more secured transactions without the involvement of Trusted Third Parties (TTP) or centralized authorities and services that can be easily disrupted, compromised, or hacked. A blockchain network provides a shared and distributed ledger that is open to all stakeholders on the network. Each transaction is verified and validated by most consensus nodes actively participating in the P2P network before being appended to the ledger. Once these transactions are validated and verified by consensus algorithms, the block data become immutable [63]. Blockchains can be classified as:

- Public or Permissionless Blockchains: An open network system where the nodes and devices can freely access without permission. The ledger is shared and transparent for anyone to join in.
- Private or Permissioned Blockchains: A user or participating node has to be permitted by the blockchain network authority before he/she could get access to the network. It is restricted to a particular group of participants (better access control), making it more secure and transparent, increasing popularity.

##### 4.1. Blockchain Key Characteristics

Blockchain is a revolutionary technology being implemented in almost all supply chain scenarios with several significant characteristics. These include immutability, transparency, decentralization, security, and privacy. All of these are extremely valuable and beneficial

for cloud security platforms and applications. This section will briefly describe these fundamental properties as follows:

#### 4.1.1. Immutability

It is one of the critical properties of blockchain where the stored and recorded transactions on the blockchain ledger cannot be undone; hence, they remain immutable and unchanged over a period of time. All the transactions executed on the blockchain network are by default timestamped and cryptographically hashed and linked to the previous block of data on the ledger. In this way, multiple data blocks are connected to build a chronological chain of blocks. The hashing process applied on every new block encompassing metadata of hash values of the previous block makes the blockchain ledger immutable, i.e., strongly unalterable. Thus, this property of blockchain makes it almost impossible to alter, amend, or even delete data from any block recorded on the ledger after being verified and validated by a majority of the participating peers on the blockchain network.

#### 4.1.2. Decentralization

This characteristic of blockchain makes it different from today's centralized networks where central systems or servers have complete control. There is no central authority or control mechanism in decentralized blockchains or third-party service providers to manage transaction processing. Instead, blockchain uses various consensus protocols to substantiate and corroborate transactions processed on the blockchain network in a more secure, transparent, reliable, and incorruptible manner. This incomparable property conveys promising benefits, such as eliminating the risk of single-point failure, saving operational and technical costs, and building trust among the participating stakeholders on the blockchain network.

#### 4.1.3. Transparency

The blockchain network's transparency feature ensures that all the transactions stored and recorded on the blockchain ledger are discernable and apparent to all the participating stakeholders on the blockchain network. It helps to achieve public integrity and verifiability of transactions performed on the P2P network by all the peers, reducing the risks of unauthorized data alternations.

#### 4.1.4. Security and Privacy

One of the most alluring facets of blockchain technology that makes it more useful and trustable is the notion of security and privacy on the ledger network. It uses Elliptic Curve Cryptography, distributed logs, and symmetric homomorphic mapping techniques where cryptographic hashing keys are randomly generated comprising alphanumeric codes, making it mathematically impossible to guess or decrypt. This property helps protect blockchain records against potential attacks, reduces data leakage apprehensions, and improves the blockchain network's overall security [64]. Furthermore, smart contracts and chain codes are created to provide privacy features to end-users by providing data provenance and trace and track facilities on the ledger network. Thus, blockchain guarantees data privacy and data ownership of individuals.

### 4.2. Blockchain Services

Blockchain-enabled solutions in cloud infrastructures provide transparent and secure cloud network management and services to end-users to help build a trust relationship to increase cloud services' usage in enterprises further. Along with other services, the blockchain network can also be deployed and hosted on an existing cloud platform to provide more secure and trustworthy services to cloud users and be called Blockchain-as-a-Service (BaaS). In particular, BaaS can offer several blockchain-enabled services to support cloud services and applications. Some of these services are described below:

#### 4.2.1. Distributed Shared Ledger

Blockchain technology is a shared distributed ledger open for all participating stakeholders on the network (i.e., cloud users, cloud nodes, and blockchain entities) to store and record their transactions such as information exchange or data sharing among cloud devices and cloud users securely and transparently after being verified by a majority of the participating peers using agreed consensus protocols. It enables industrial networks where cloud users can control and verify their transactions when communicating with the blockchain cloud.

#### 4.2.2. Consensus

The consensus mechanism aims to create an agreement within the blockchain network on different transactions performed on the ledger amongst the participating nodes. The consensus mechanism helps verify and substantiate the transactions being executed on the network by most peer nodes using some consensus algorithms to ensure that the network participant must follow the transaction rules. The primary objective of blockchain consensus mechanisms includes: facilitating a uniform agreement between nodes on the network, ensuring fairness and equity, incentivizing participant stakeholders to follow the rules making sure that the network remains fault-tolerant.

**Proof-of-Work (PoW):** The older and popular consensus algorithm among blockchain solutions involves a mining mechanism and combines the characteristics of P2P networks, Merkle chains, and cryptographic signatures.

**Proof-of-Stake (POS):** This solution was invented to overcome some of the discrepancies and inefficiencies of POW. It does not involve the mining process. Instead, participating users in the network are required to stake, i.e., lock up, some of their coins in a network wallet for a certain time to validate data blocks.

These algorithms help create steadiness and reliability in existing cloud systems, improving and ensuring better security for the existing cloud system. Interestingly, cloud users can use their virtual cloud machines to join the consensus process to receive rewards due to their efforts (i.e., cryptocurrency in Bitcoin).

#### 4.2.3. Smart Contract (Chain Codes)

Smart contracts and chain codes offer better services and applications to cloud users. Once we create and load smart contracts on the blockchain network, they execute independently with business logic built to perform the required tasks. It helps to create trust in existing cloud systems. Furthermore, smart contracts also provide security services, in particular, services related to user authentications and fined-grained access controls for data sharing and storage.

#### 4.2.4. Cryptography

Blockchain uses Elliptic Curve Cryptography (ECC) and various hashing algorithms such as SHA-256 to provide strong cryptographic proof for data authentication and integrity [65]. It ensures that blocks of data being stored and recorded on the ledger should remain integrated and untampered with. Hence, it improves the immutability and security of cloud user transactions.

#### 4.2.5. Blockchain Platform

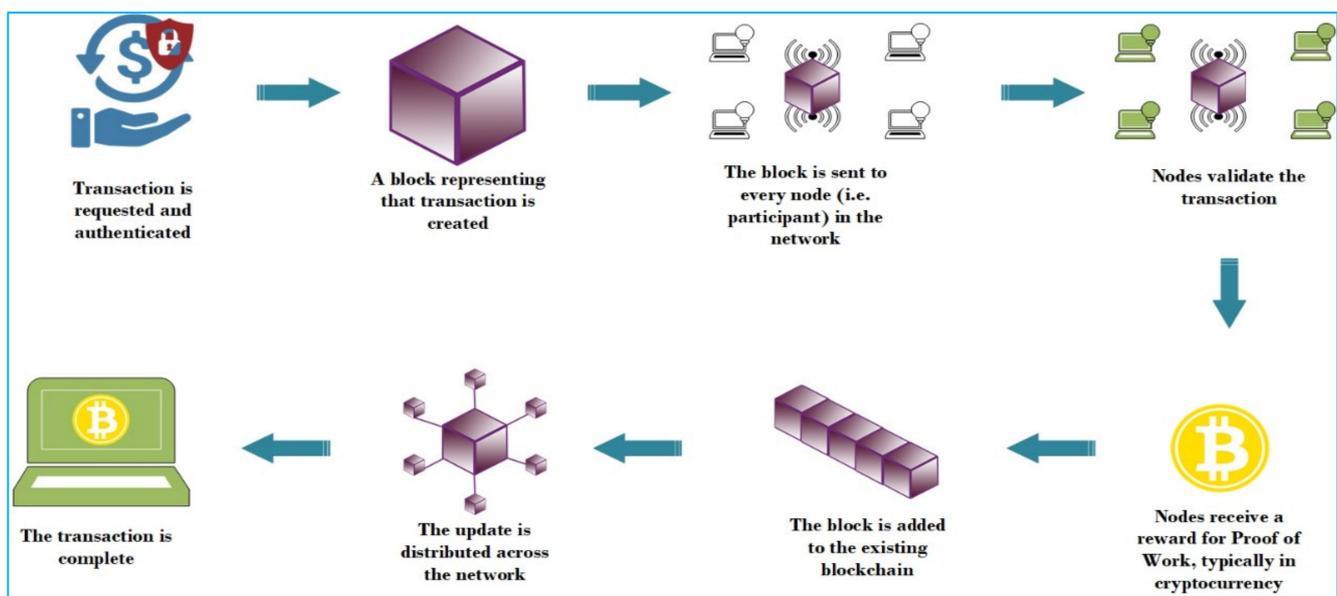
Blockchain is an immutable distributed decentralized ledger technology that enables sharing of data among the participating stakeholders in a peer-to-peer network. Blockchains are used and implemented in various technological scenarios based on their architectural characteristics and other parameters such as operation mode, consensus algorithms, programming languages support, smart contracts, transaction capacity, etc., as presented in Table 1 below.

**Table 1.** Blockchain Platforms.

Platform	Consensus Algorithms	Operation Mode	Programming Languages	Source
Bitcoin	PoW	Public	Ivy, RSK, BitML	[66]
Ethereum	PoW, PoS	Public and permissioned	Solidity, Flint, SCILLA	[67]
Hyperledger	PBFT	Permissioned	Go, Node.js, Java	[68]
Ripple	PoW	Permissioned	C++	[69]
R3 Corda	PoW, PoS	Permissioned	Kotlin, Java	[70]
Openchain	Partionned	Consensus	Java	[71]
BigChainDB	BFT	Public and permissioned	C++, Java	[72]
Chain core	Federated consensus	Permissioned	Java	[73]

### Bitcoin

It is one of the earliest and most popular digital currency-based blockchain platforms that runs on top of the blockchain infrastructure. It allows transactions between peers without a third-party, central authority, or server to issue and manage the currency transactions for many of today’s most popular cryptocurrencies. The bitcoin transaction information is always displayed on the ledger network so that all participating peers can validate and verify it to limit the currency issuance problem. The electronic currency supported by bitcoin is called a digital signature and is a chain of signatures in the blockchain network, as shown in Figure 4. When a peer performs a transaction in the network, the transaction owner’s coin is transferred to the next chain on the ledger with the hash value calculated from the previous transaction. The digital signature is transmitted to the public key of the next owner. The recipient peer of the signature can confirm and verify the ledger’s ownership to validate the blockchain network’s processed transaction [74]. In this way, all the participating peers on the network have the same blockchain and transaction records as stored by the peer nodes. Nevertheless, the invention of other blockchain platforms such as Ethereum and Hyperledger blockchains has wholly transformed this technology’s potential use in almost all industrial and technological domains. The potential use of space for blockchain has become interminable.



**Figure 4.** Bitcoin Blockchain.

### Ethereum Blockchain

The idea of Ethereum was first tossed and used publicly in July 2015 [75]. As opposed to the bitcoin blockchain, which is primarily used for digital currency transactions, Ethereum is developed to store transaction records using smart contracts. A smart contract is fundamentally a computerized transaction protocol (business logic) that executes the contract between the blockchain network's participating stakeholders to execute transactions. They are automated programs written in programming languages, such as Solidity, Java, etc., by the users to be executed on the blockchain network. An Ethereum blockchain network comprises EVMs (Ethereum Virtual Machines) similar to miner nodes in the bitcoin network. These EVMs are proficient in providing the cryptographically tamper-proof trustworthy execution and enforcement of smart contracts. The digital currency supported by Ethereum is called Ether. The smart contracts used in Ethereum have their accounts and addresses and are linked with their executable code and balance of Ether coins (gas). These smart contracts are executed on the EVM nodes. The storage space supported by EVMs is comparatively expensive; thus, for the execution and storage of large transactions, other remote decentralized data storage such as BitTorrent, IPFS, or Swarm can be used.

### Hyperledger Fabric Blockchain

It is a private, permissioned blockchain network that benefits from creating publicly accessible ledger data using open standards. Currently, hyperledger, which includes many versions such as Fabric, Besu, Indy, etc., is being used and implemented by various enterprises with production environments. It helps to create multiple private permissioned networks between different organizations or organizational units in the same organizations using channels. Access to these private blockchains is restricted to only selected stakeholders. The participating stakeholders' identities are already known and can perform their transactions securely and privately with better scalability, transparency, performance, and efficiency. These private blockchains focus on specific supply chain vulnerabilities and data to solve the privacy and confidentiality issues and challenges. These blockchain platforms bridge the gap between current systems and legacy systems and provide immutable, auditable, and traceable systems that complement the existing systems and processes.

To create a trusted environment between untrusted participants, the hyperledger fabric provisions an identity management service that manages user IDs and authenticates all network participants. It introduces a membership service that establishes rules and regulations by which different stakeholders are governed, authenticated, validated, and verified to be part of the blockchain network and allowed to access the ledger for ensuring secrecy, privacy, and confidentiality. The membership service is a new comprehensive novel design that revamps the whole process of nondeterminism, resource exhaustion, and performance attacks for the participating stakeholders [76]. Access control lists can be used to provide additional layers of permission. A specific user ID could be permitted to invoke a chain code application but blocked from deploying a chain code. ACLs are created and managed by network administrators in the hyperledger fabric, which can configure access to resources by associating those resources with existing policies. The ledger data can be stored in multiple formats, and consensus mechanisms can be switched in and out. The fabric provides secure and transparent Byzantine-Fault Tolerant (BFT) consensus algorithms for ensuring secure and reliable communication amongst the group of untrusted stakeholders [77].

## 5. Blockchain-Enabled Virtualized Cloud Security Solutions

Cloud computing amasses large networks of virtualized services hosted in large data centres referred to as data farms or server farms. These services are called Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The existing cloud infrastructures have reconciliation issues, particularly a Multi-Party environment where multiple users share the infrastructure. Some of the problems highlighted include expensive, vulnerable, and inefficient services and applications on cloud platforms.

Today's cloud users require that the transactions, services, and applications provided to them by cloud service providers should be transparent, efficient, secure, and authenticated, and have maximum granular access controls. All the transactions performed on the cloud network should be verified, corroborated, and endorsed by the trusted relevant parties. Business logic should be embedded within the database (Ledger) and executed to validate and store the transactions.

Blockchain technology has the potential and aptitude to resolve and unravel the majority of the problems and challenges being faced by today's virtualized cloud infrastructures. It provides secure, transparent, trustworthy, and efficient solutions for creating authorized identity management and registration systems for all cloud stakeholders. It also offers a reliable, dependable, distributed, and decentralized management and governance system for integrity, privacy, and efficient tracking and tracing service for all cloud-related transactions performed by cloud users. Blockchain also enables identities and services to be hidden entirely from end-users and can be managed and stored on the blockchain distributed ledger.

The use and implementation of blockchain technology in cloud infrastructures improve the cloud systems' overall security paradigm [78]. Some of the recent examples where blockchain-enabled cloud solutions are being implemented include the Oracle Blockchain Cloud Service project [79]. Furthermore, blockchain can also be beneficial in virtualized cloud environments. It provides the facility to register and give identity to all the connected cloud devices and services, with a set of attributes and complex relationships recorded on the blockchain ledger. This enables it to provide provenance at all levels in virtualized cloud supply chain networks. The cloud-enabled supply chain network can include multiple stakeholders such as cloud infrastructure facilities, vendors, suppliers, services, distributors, shippers, installers, owners, repairers, re-installers, etc. It also ensures anonymity in large-scale cloud environments. An electronic wallet is created and installed in cloud systems for anonymity to avoid access to private users' information to third-party service providers [80]. Blockchain-enabled smart contracts also play a significant role in managing, controlling, and most importantly securing cloud services and devices. In this section, we discourse and recapitulate some of the essential features of blockchain technology that can be enormously useful for cloud platforms, particularly in cloud security. Some of the blockchain-enabled cloud security solutions include:

#### *5.1. Blockchain-Enabled Virtualized Task Scheduling*

As virtualized cloud data centre operations and services are expanding, the need for a distributed, transparent, and integrated security solution is never more apparent than now. It entails dealing with complicated, critical, and long-term issues such as virtual machine task scheduling in a cluster of server machines. The blockchain-enabled distributed P2P virtualized cloud cluster solution provides better management of these tasks amongst the server machines distributed in a cloud infrastructure. The blockchain-enabled smart contract-based solution enables each node in the P2P blockchain network to correspond to a complex CSP. The blockchain system handles the optimal scheduling of virtualized tasks by generating optimum schedules for each connected virtual machine to engender a recommendation list of cloud services, storage servers, and cloud resource providers. The proposed solution is an attempt that determines cluster servers that guarantees minimum power penalty and also increases the overall resource utilization of a given server cluster. It further increases the decision logic to improve the efficiency and performance of virtualized server machines.

#### *5.2. Blockchain-Enabled Anonymity of Data Algorithms*

A virtualized cloud infrastructure comprises hardware and software components, devices, services, and applications. The implementation of blockchain can improve the security of these enabled algorithms to secure the whole system. One of the prominent features of virtualized cloud systems is the anonymity of users' information and services

data available on virtualized cloud environments. This feature is further inspired and improved by implementing blockchain-technology-enabled solutions [81] such as Electronic Wallets installed in large-scale clouds to store users' and services' data through blockchain platforms [82]. It is essential to highlight that these electronic wallets must be deleted appropriately to ensure user information security on the cloud once used. The recent example of such successful integration of the blockchain with cloud platforms is the Oracle Blockchain Cloud Service project [83].

Furthermore, cloud service records can be stored on a distributed ledger on the blockchain network where recorded data and services cannot be changed or added without the consensus of all peer nodes participating on the blockchain network. The identity of these cloud users and service providers can also be validated by applying consensus over the blockchain. Blockchain also provides better security and privacy solutions. It can effectively hide the physical location of data and use blockchain-enabled cryptographic algorithms to store the data on the blockchain ledger securely considering data sovereignty rules and guidelines in the permitted locations.

### *5.3. Blockchain-Enabled Data Integrity and Privacy*

The services and data processed and provisioned by CSPs connected through a blockchain network will always be cryptographically proofed and signed by the real sender that holds the unique public key and Global Unique Identifier (GUID). It ensures the authentication and integrity of the transmitted data or the on-demand provisioned service. Besides, these transactions will be recorded and stored on the blockchain-distributed ledger. These transactions can easily be traced and tracked by any of the participating cloud users or CSPs, which provides provenance to all cloud system stakeholders, thus creating trust and worthiness. Blockchain-enabled smart contracts help ensure user and service privacy using custom-defined access rules, conditions, and time to allow specific individuals or groups of users or machines to own, control, and have access to data at rest or in transit in a cloud infrastructure. These smart contracts have the control and authority to manage who has the right to update, upgrade, patch the data and services (software or hardware), provide new keypairs, initiate a service or repair request, change ownership, and initiate the provision or re-provision of a service.

### *5.4. Blockchain-Enabled Authentication and Authorization*

Blockchain smart contracts are created and executed by peer nodes (peers) to facilitate and enforce decentralized authentication and authorization rules and logic for providing single- and multi-party authentication to all cloud devices and users on the cloud computing platform. These smart contracts also provide improved authorization access rules for cloud users while accessing cloud services and data using Access Control Lists (ACLs). While in traditional clouds, authorization and authentication are done using Role-Based Access Management (RBAC), O-Auth 2.0, OpenID, OMA-DM, and LWM2M protocols. A smart contract's business logic has many programming functions, predefined rules, and conditions (contractual terms) defined by mutual agreement between the participating peers to read, execute, and update the ledger's current state, and are initiated through a transaction proposal [84].

### *5.5. Blockchain-Enabled System Resilience and Fault Tolerance*

One of the key characteristics of a blockchain network is its fault tolerance and resilience capacity as it provides provenance and tracks and a trace facility for all types of data and services being provisioned to cloud users at any location by CSPs. It implies that any single node in the blockchain network's failure will not affect the whole virtualized cloud infrastructure's functionality and continuity. It can be implemented by using blockchain as a sub-system in a cloud infrastructure solution. This blockchain-adopted sub-system works as a back-end solution (back-end-service) to record and store cloud data and services in a temper-resistant way using some blockchain algorithm. The overall system is called

Blockchain-as-a-Service (BaaS). In this solution, the connectivity between the virtualized cloud and back-end blockchain is implemented using smart contracts. In this complex infrastructure, cloud computing plays offloading when a complex computation workload is required and can be processed using these smart contracts.

## 6. Discussion and Open Challenges

This section briefly outlines and explains notable open challenges in adopting blockchain technology for handling virtualized security threats and concerns. To ensure the better exploitation and implementation of blockchain technology, it necessitates a good understanding of the technology and what it entails to achieve the desired objectives.

### 6.1. Cloud Stakeholder Agreement

A blockchain network is a distributed P2P ledger network where all cloud stakeholders, including clients, cloud vendors, cloud owners (service providers), etc., store their core business data and information. Every stakeholder has access to this sensitive private data on the blockchain platform. Security, transparency, and assurance are considered significant issues and challenges to establish client trust in Cloud Service Providers (CSPs). As the number of clients increases and various cloud-enabled services are provided by cloud owners, new architectural, storage, and access issues are leveraged, causing trust deficiency and secrecy issues. Incentives and motivations are of an utmost necessity for blockchain-enabled systems to succeed and execute transactions on the blockchain-enabled cloud network. Potential stakeholders might be reluctant to participate in such networks since they could lose their competitive advantage, primarily when multiple business competitors exist in the same supply chain [85].

### 6.2. Attacks and Vulnerabilities

One of the most significant advantages and selling points of blockchain technology in cloud architectures is its resilience against various attacks, including physical attacks and cyberattacks. A recent cybersecurity report highlights several security risks, such as bad actors and man-in-the-middle attacks, being involved in the blockchain network, and exposing the network's vulnerabilities [86]. The current blockchain implementations are leaving inherent vulnerabilities and bugs due to immature processes and systems. Phishing scams, technology vulnerabilities, implementation exploits, and malware, due to lack of standards and procedures, present serious challenges to be addressed in moving forward.

### 6.3. Lack of Data Standardization and Scope

It is significant for enterprises to cater to what type of data will be stored on the cloud platform using blockchain ledger technology, i.e., on-chain or off-chain storage. It is pertinent to highlight that most of the client's data and other organizational information are private data and must be stored and verified against on-chain hash evidence. One of the significant aspects of data standardization is the size of the data stored on the ledger. Storing unimportant data on the blockchain ledger creates additional large transaction sizes that will affect the blockchain's efficiency and performance. To standardize the cloud data stored on the blockchain ledger to achieve better efficiency and performance, enterprises need to align and adequately define the size, type, and format of the data stored at the blockchain ledger. Furthermore, restricting access to the blockchain network also helps standardize the data stored and exchanged on the network.

### 6.4. Interoperability Challenge

Interoperability is defined as the mass adoption of cloud-enabled business software and platforms across multiple enterprises to integrate strategies efficiently. It serves as a means for users of different platforms and software to interact and conduct meaningful businesses seamlessly. The existing cloud platform architectures and solutions lack full interoperability as there are no standardized solutions to make integration, adaptability,

and implementation easier [87]. Furthermore, different blockchain platforms are coping with interoperability issues, ensuring maximum scalability and adaptability for enabling internal and external communication between various business enterprises.

#### *6.5. Regulatory Consideration and Compliance*

Cloud service provider (CSP) owners and policymakers need to consider and develop different cloud-related policies, configurations, regulations, and guidelines regarding the implementation of blockchain technology at various levels in virtualized cloud environments. The policies, procedures, and regulations should consider the implications and insinuations such as the distributed storage, ownership of blocks, and records in the ledger, and when this ownership changes, along with different access permissions and rights on the blockchain network. The cloud computing paradigm needs to collaborate and facilitate existing security and regulatory frameworks such as NIST for privacy and interoperability to develop and evolve new cloud-enabled services and platforms to formulate new administration policy objectives.

#### *6.6. Costs of Operating Blockchain Technology*

Blockchain technology enables us to provide secure, efficient, and regimented systems for performing real-time transactions. Finding and selecting the best-suited blockchain platform is not an easy task as most blockchain platforms are not fully developed, and hence are not stable to be implemented in diverse cloud platforms. Implementation, energy, and operating costs are among the most significant challenges faced by enterprises as the costs of running and implementing private permissioned blockchain systems are yet to be known to enable the secure and efficient management of various cloud services and platforms. The existing cloud platforms and legacy software systems are inefficient and centralized while executing the transactions, causing massive implementation and maintenance costs. Blockchain's open-source technology, properties, and distributed nature can help reduce the operating and management cost. Blockchain is an immutable and transparent technology; the storage, backups, and recovery become obsolete and gratuitous, along with abolishing data exchange integration points and time-consuming reporting activities.

### **7. Conclusions**

The new revolution begins in the IT Industry using cloud models; after the revolution, many companies can quickly get more benefits than in previous work. As well as many small and large organizations, even countries can achieve benefits from cloud storage. Even though cloud storage has many benefits, it still has a vulnerability and many other security issues. Whenever it concerns adopting cloud storage, the first barrier is seen as a security issue for online shopping or selling anything, so customers and vendors have security threats. This research highlights the various security challenges, vulnerabilities, attacks, and threats for adopting the cloud computing facility. In this paper, many of the security issues and challenges are discussed and many of the unique characterizations from cloud computing. Resource sharing, virtualization resources, and the public nature of the cloud are discussed. In this manner, this paper explores the various cloud computing services and provides well-organized security concern services. After the success of cloud computing, the government also adopted the services into their department to enhance performance, quality, innovation, and security. So, every citizen can quickly get their desired data. Afterward, the existing system and encountered security issues and cost issues were examined. So, on behalf of security issues, the 3-Tier system architecture can enhance service quality and improve cloud security. Moreover, the suggested model has three cloud service levels and focuses on the crucial aspect of the cloud security level. Many of the open issues and future work are discussed in the paper.

**Author Contributions:** All authors contributed equally to this work and were involved at every stage in its development. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## 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. [[CrossRef](#)]
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. [[CrossRef](#)]
3. Moura, J.; Hutchison, D. Review and analysis of networking challenges in cloud computing. *J. Netw. Comput. Appl.* **2016**, *60*, 113–129. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
9. Tripathi, A.K.; Agrawal, S.; Gupta, R.D. Cloud enabled SDI architecture: A review. *Earth Sci. Inform.* **2020**, *13*, 211–231. [[CrossRef](#)]
10. Ehwerhemuepha, L.; Gasperino, G.; Bischoff, N.; Taraman, S.; Chang, A.; Feaster, W. HealthDataLab—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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
18. Varga, P.; Peto, J.; Franko, A.; Balla, D.; Haja, D.; Janky, F.; Soos, G.; Ficzer, D.; Maliosz, M.; Toka, L. 5G Support for Industrial IoT Applications—Challenges, Solutions, and Research Gaps. *Sensors* **2020**, *20*, 828. [[CrossRef](#)] [[PubMed](#)]
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. [[CrossRef](#)]
20. Shahid, F.; Khan, A.; Jeon, G. Post-quantum distributed ledger for internet of things. *Comput. Electr. Eng.* **2020**, *83*, 106581. [[CrossRef](#)]
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. [[CrossRef](#)]
22. Chen, N.; Li, F.; White, G.; Clarke, S.; Yang, Y. A Decentralized Adaptation System for QoS Optimization. *Fog Fogonomics* **2020**, 213–247. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]

25. Firouzi, F.; Farahani, B. Architecting IoT Cloud. In *Intelligent Internet of Things*; Springer: Cham, Switzerland, 2020; pp. 173–241. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
28. Singh, N.; Singh, A.K. Data privacy protection mechanisms in cloud. *Data Sci. Eng.* **2018**, *3*, 24–39. [[CrossRef](#)]
29. Bartolini, C.; Santos, C.; Ullrich, C. Property and the cloud. *Comput. Law Secur. Rev.* **2018**, *34*, 358–390. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
33. Morabito, R.; Petrolo, R.; Loscri, V.; Mitton, N. Reprint of: LEGIoT: A Lightweight Edge Gateway for the Internet of Things. *Future Gener. Comput. Syst.* **2019**, *92*, 1157–1171. [[CrossRef](#)]
34. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Comput. Sci. Rev.* **2019**, *33*, 1–48. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
42. Castro, P.; Ishakian, V.; Muthusamy, V.; Slominski, A. The rise of serverless computing. *Commun. ACM* **2019**, *62*, 44–54. [[CrossRef](#)]
43. Sierra-Arriaga, F.; Branco, R.; Lee, B. Security Issues and Challenges for Virtualization Technologies. *ACM Comput. Surv.* **2020**, *53*, 1–37. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]

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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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. [[CrossRef](#)]
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*. [[CrossRef](#)]
61. Yang, H.; Yuan, J.; Yao, H.; Yao, Q.; Yu, A.; Zhang, J. Blockchain-Based Hierarchical Trust Networking for JointCloud. *IEEE Internet Things J.* **2019**, *7*, 1667–1677. [[CrossRef](#)]
62. Dasgupta, D.; Shrein, J.M.; Gupta, K.D. A survey of blockchain from security perspective. *J. Bank. Financ. Technol.* **2019**, *3*, 1–17. [[CrossRef](#)]
63. Aileni, R.M.; Suci, G. IoMT: A blockchain perspective. In *Decentralised Internet of Things*; Springer: Cham, Switzerland, 2020; pp. 199–215.
64. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *J. Parallel Distrib. Comput.* **2020**, *143*, 148–166. [[CrossRef](#)]
65. Hu, J.-W.; Yeh, L.-Y.; Liao, S.-W.; Yang, C.-S. Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for Internet of Things devices. *Comput. Secur.* **2019**, *86*, 238–252. [[CrossRef](#)]
66. Delgado-Mohatar, O.; Felis-Rota, M.; Fernández-Herraiz, C. The Bitcoin mining breakdown: Is mining still profitable? *Econ. Lett.* **2019**, *184*, 108492. [[CrossRef](#)]
67. Cao, B.; Zhang, Z.; Feng, D.; Zhang, S.; Zhang, L.; Peng, M.; Li, Y. Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digit. Commun. Netw.* **2020**, *6*, 480–485. [[CrossRef](#)]
68. Wang, S. Performance Evaluation of Hyperledger Fabric with Malicious Behavior. In *International Conference on Blockchain*; Springer: Cham, Switzerland, 2019; pp. 211–219. [[CrossRef](#)]
69. Bekhouche, L.; Saou, R.; Guerroudj, C.; Kouzou, A.; Zaim, M.E.-H. Electromagnetic torque ripple minimization of slotted doubly-salient-permanent-magnet generator for wind turbine applications. *Prog. Electromagn. Res. M* **2019**, *83*, 181–190. [[CrossRef](#)]
70. Lee, J.Y. A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Bus. Horiz.* **2019**, *62*, 773–784. [[CrossRef](#)]
71. Khan, S.; Amin, A.; Hossain, H.; Noor, N.; Sadik, W. A pragmatical study on blockchain empowered decentralized application development platform. In Proceedings of the International Conference on Computing Advancements, New York, NY, USA, 10–12 January 2020. [[CrossRef](#)]
72. Falazi, G.; Khinchi, V.; Breitenbücher, U.; Leymann, F. Transactional properties of permissioned blockchains. *SICS Softw. Intensive Cyber-Phys. Syst.* **2019**, *35*, 49–61. [[CrossRef](#)]
73. Ismail, L.; Hameed, H.; Alshamsi, M.; Alhammadi, M.; Aldhanhani, N. Towards a blockchain deployment at UAE University: Performance evaluation and blockchain taxonomy. In Proceedings of the 2019 International Conference on Blockchain Technology, Honolulu, HI, USA, 15–18 March 2019; pp. 30–38. [[CrossRef](#)]
74. Sarfraz, U.; Alam, M.; Zeadally, S.; Khan, A. Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions. *Comput. Netw.* **2019**, *148*, 361–372. [[CrossRef](#)]
75. Oswald, E.; Fischlin, M. (Eds.) Advances in Cryptology—EUROCRYPT 2015. In Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 26–30 April 2015; Volume 9057.
76. Lone, A.H.; Mir, R.N. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digit. Investig.* **2019**, *28*, 44–55. [[CrossRef](#)]
77. Khan, M.Y.; Zuhairi, M.F.; Ali, T.; Alghamdi, T.; Marmolejo-Saucedo, J. An extended access control model for permissioned blockchain frameworks. *Wirel. Netw.* **2019**, *26*, 4943–4954. [[CrossRef](#)]
78. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A survey on blockchain for information systems management and security. *Inf. Process. Manag.* **2021**, *58*, 102397. [[CrossRef](#)]

79. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [[CrossRef](#)]
80. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in distributed blockchain: Analysis, requirements and open issues. *Future Gener. Comput. Syst.* **2019**, *100*, 325–343. [[CrossRef](#)]
81. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R. P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. *Comput. Secur.* **2020**, *88*, 101629. [[CrossRef](#)]
82. Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [[CrossRef](#)]
83. Bertin, E.; Hussein, D.; Sengul, C.; Frey, V. Access control in the Internet of Things: A survey of existing approaches and open research questions. *Ann. Telecommun.* **2019**, *74*, 375–388. [[CrossRef](#)]
84. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [[CrossRef](#)]
85. Blockchain Threat Report-Mcafee.com. Available online: [www.mcafee.com/enterprise/enus/assets/reports/rp-blockchain-security-risks.pdf](http://www.mcafee.com/enterprise/enus/assets/reports/rp-blockchain-security-risks.pdf) (accessed on 15 April 2021).
86. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [[CrossRef](#)]
87. Uddin, M. Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *Int. J. Pharm.* **2021**, *597*, 120235. [[CrossRef](#)]