Journal of Theoretical and Applied Information Technology

15th December 2023. Vol.101. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

VIRTUALIZATION IN CLOUD SECURITY

JAWHARA BOODAI[1], AMINA ALQAHTANI[2], MOUNIR FRIKHA[3]

[123]College of Computer Science and Information Technology, King Faisal University, Al-Ahsa, 31982, Saudi Arabia.

E-mail: [1]222453718@student.kfu.edu.sa, [2]223002599@student.kfu.edu.sa, [3]mmfrikha@kfu.edu.sa

ABSTRACT

Cloud computing has become ubiquitous, providing convenient on-demand access to computing resources. However, security remains a major concern, especially with the added complexity of Virtualization. This paper systematically reviews research on virtualization security in cloud environments. We surveyed academic literature from 2010-2023 to summarize the latest techniques and algorithms to secure virtualized cloud infrastructure and prevent attacks. Common methods include hypervisor hardening, micro-segmentation, virtual network encryption, and virtual machine introspection. Research trends point towards increasingly advanced techniques like homo-morphic encryption and confidential computing, enabling secure, privacy-preserving computation on encrypted data. More work is still needed to balance performance and scalability with security. This review provides an overview of the state-of-the-art securing virtualized cloud environments and identifies open challenges for future research.

Keywords: *Cloud Security, Virtualization, Hypervisor, Micro Segmentation, Encryption.*

1. INTRODUCTION

Cloud computing has become ubiquitous, providing convenient on-demand access to computing resources that can be elastically provisioned and released. By leveraging Virtualization, cloud computing allows the abstraction and sharing of physical resources across virtual machines (VMs) that behave as separate computing systems [1]. This provides benefits like server consolidation, rapid deployment, fault isolation, and scalability [2]. Major cloud service models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [3]. Leading commercial cloud providers include Amazon Web Services, Microsoft Azure, Google Cloud, Alibaba Cloud, and IBM Cloud.

Global cloud spending is forecast to surpass 482 billion in 2022 as adoption grows rapidly [4]. The technology underpinning cloud virtualization is the hypervisor, or virtual machine monitor (VMM), which coordinates shared access to hardware resources between VMs and the host operating system [5]. By providing a virtualization layer, hypervisors allow VMs to execute workloads in isolation from each other. Widely used hypervisor platforms include Xen, VMware ESXi, Microsoft Hyper-V, and KVM [6]. The hypervisor schedules virtual CPU time, memory, storage, and network access for each VM. This enables multi-tenancy, as many customer VMs can securely run on the same physical server, providing efficient statistical multiplexing of resources [7]. However, despite the advantages, security remains one of the primary concerns inhibiting more widespread enterprise adoption of cloud computing [8]. Virtualization introduces new attack surfaces and threats compared to traditional data centers. While VMs provide strong workload isolation, the hypervisor, host operating system, virtual networks, and management plane become vulnerable to compromise [9]. At-tackers could penetrate cloud environments via misconfigurations, exploit vulnerabilities, launch denial of service attacks, or abuse insider credentials [10]. A breach of the hypervisor could lead to subtle data leaks, access abuse, or a complete takeover of customer VMs. These risks are amplified by the cloud's distributed and multi-tenant nature across data centers and networks. Therefore, ensuring robust security and maintaining trust is critical, especially with sensitive data and workloads migrating to the cloud [11]. Key challenges include controlling access, verifying identities, securing virtual networks, protecting data, and monitoring for threats. Additionally, the complexity of cloud virtualization stacks causes management difficulties that lead to insecure deployments. Customers must validate provider security while weighing tradeoffs between

control and convenience [12]. Addressing these concerns remains an extremely active research area as cloud adoption spreads.

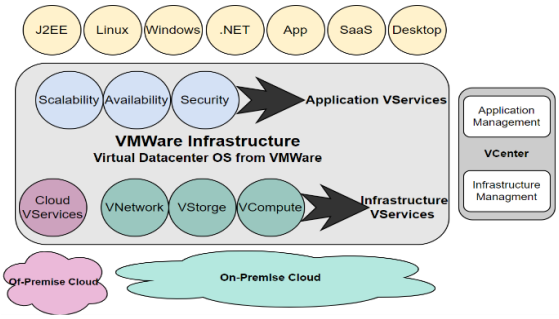

Figure 1: How Virtualization Works in A Cloud Computing Source: [1].

This paper systematically reviews recent research proposing innovative techniques to secure virtualized cloud environments and Infrastructure. We survey papers from 2010-2023 presenting the latest algorithms, architectures, and paradigms for hardening hypervisors, encrypting networks, isolating workloads, enabling confidential computing, and more. By summarizing progress across key domains, this review provides a comprehensive overview of the state-of-the-art securing multi-tenant virtualized clouds. We highlight outstanding challenges and future directions to guide continuing research toward fully trustworthy and resilient cloud computing.

Research Objectives:

The objectives of this study are to:

- Systematically review recent literature from 2010-2023 on securing virtualized cloud computing environments.
- Summarize state-of-the-art techniques proposed across domains like hypervisor hardening, network security, workload isolation, identity management.
- Identify key themes, trends, and gaps to provide a comprehensive overview of research progress.

This review focuses specifically on security innovations tailored to multi-tenant cloud contexts enabled by virtualization. General IT security techniques lacking customization to cloud environments are excluded.

Research Problem: Virtualization introduces new threats to cloud computing. This study reviews academic literature presenting the latest advanced security mechanisms to address these risks and protect shared cloud infrastructure. Papers were systematically screened for relevance by prioritizing peer-reviewed publications emphasizing novel technical security contributions customized to virtualized cloud settings. Works lacking technical depth, validation, or accessibility were excluded per the criteria in Table 1.

This systematic review uniquely focuses on analyzing the latest security innovations proposed specifically for hardened cloud virtualization software and infrastructure. While existing survey papers examine cloud security challenges more broadly, they lack emphasis on emerging techniques tailored to address multi-tenant risks [1-3]. For example, Khan et al. [4] provided a wide-ranging review of cloud security issues, vulnerabilities, attacks and countermeasures but did not deeply assess virtualization-specific mechanisms. Tank et al. [5] analyzed threats arising from sharing physical infrastructure across virtual machines (VMs) yet focused narrowly on risk assessments rather than modern protections.

By comparison, this study collects papers from 2010-2023 to assess progress on state-of-the-art security paradigms designed explicitly for virtualized cloud environments. The analysis yields updated insight into sophisticated proposals leveraging formal verification, workload introspection, confidential computing and other advances to surpass limitations of conventional security controls. Moreover, while previous works have presented reference architectures and taxonomies [6,7], this review uniquely highlights opportunities and challenges in adopting theoretical contributions into operational cloud platforms based on the latest research.

So, by systematically synthesizing technical security techniques customized to address multi-tenant virtualization risks over the past decade, this study offers current perspective into progress and gaps that distinguishes it from preceding cloud security surveys. The findings provide a comprehensive snapshot of active research activity aimed at realizing more trustworthy, resilient and privacy-preserving cloud computing.

2. MATERIALS AND METHODS

To systematically review the recent literature on virtualization security in cloud computing environments, we followed a structured methodology to search, select, and analyze relevant publications.

2.1 Search Strategy

We searched major academic literature databases, including IEEE Xplore, ACM Digital

Library, ScienceDirect, SpringerLink, and Google Scholar. These databases provide extensive coverage of technology research publications. Our search strategy focused on finding papers published in the last years (2010-2023) to constrain the review to the latest advances in this rapidly evolving research domain. We used keyword search queries with terms including "cloud security," "virtualization security," "hypervisor security," "virtual machine security," and related terms. Wildcards and synonyms were used to capture relevant variants. The search was limited to English-language publications in journals, conferences, and workshops emphasizing security, networking, and cloud computing. Only publications with full text available were considered.

2.2 Inclusion and Exclusion Criteria

2.2.1 Inclusion criteria:

- Recent papers from 2010 to 2023 were prioritized to capture the latest advances in this fast-moving research area.
- Relevant publication venues emphasize novel security innovations, specifically in cloud virtualization environments.
- Technically deep contributions with new models, protocols, mechanisms, etc., rather than just high-level overviews.
- Proposals are supported by empirical evaluation or formal analysis to validate claims.
- Full-text access is needed for an in-depth understanding of techniques.
- English language for reviewer comprehension.

2.2.2 Exclusion criteria:

- Older papers predate recent advances in cloud security and Virtualization.
- Sources lacking peer review and Editorial oversight, like preprints.
- Works discussing general IT security without customization to multi-tenant virtualized cloud environments.
- Lightweight papers are not proposing substantial new techniques.
- Purely theoretical papers without evaluation or analysis of techniques.
- Inaccessible papers where full text could not be obtained.
- Non-English papers due to language limitation.

Table 1: Inclusion and exclusion criteria.

Criteria	Inclusion Criteria	Exclusion Criteria
Time period	2010 to 2023 - Present	Pre-2010
Publication Type	Journal articles, conference proceedings, workshops	Books, preprints, theses, editorials
Topic relevance	Specific focus on virtualization security in cloud computing	General IT security without cloud context
Technical depth	Substantial novel techniques, architectures, and algorithms proposed	Surveys, qualitative discussions
Evaluation	Techniques experimentally validated or formally analyzed	Purely theoretical or conceptual proposals
Accessibility	Full text available in databases	Inaccessible papers without
Language	English language publications	Non-English papers

2.3 PRIZMA

A flowchart known as a Preferred Reporting Item for Systematic Reviews and Meta- Analyses (PRISMA) demonstrates the procedures taken from the starting stage of looking for evidence to the final stage of selecting relevant research. The PRISMA flowchart displays the movement of search results through the various stages of a systematic review, including information on the number of records found, included, and excluded and the logic behind these choices. The PRISMA flowchart depicts the use of databases and other primary and secondary sources to identify relevant results during the identification phase of a search.

We collected 2512 documents using Google Scholar and ResearchGate. 1408 articles from the Google Scholar, and 1004 papers from ResearchGate. After deleting duplicates, we were left with 335 high-quality scholarly publications published between 2010 and 2023. The PRISMA diagram symbol represents the path's destination. 135 items were excluded because they did not match the criteria. After reviewing the abstracts of the remaining 100 findings, only 80 publications were included in the final analysis. The 80 full-text scholarly papers were then reviewed for eligibility for the qualitative review and relevance to the study's topic; 45 articles were removed. Later in this chapter, we'll review the 35 publications that round up this study's critical re-view. Figure 2 of the PRISMA flow diagram depicts detailed procedures from initial article identification to final article selection for quality review.

2.4 Selection Criteria

The papers retrieved underwent a two-step selection process. The first screening reviewed paper titles and abstracts to identify relevant publications. We preferred journal articles and full conference papers to focus on significant novel contributions with evaluated results rather than short workshop papers. Papers were assessed for relevance by presenting security innovations tailored to virtualized cloud environments rather than general IT security. Works focusing on attacks without defense proposals were excluded. Surveys on cloud security were avoided except for the latest to capture current snapshots. The initial screening yielded 152 candidate papers. In the second screening, candidate papers were fully read to confirm their suitability for inclusion. Empirical evaluation of techniques and substantial security contributions were required for selection. Papers with outdated proposals predating recent advances were excluded. Specialized papers outside the scope were also filtered out. This in-depth screening resulted in 35 papers being chosen for the final literature review and analysis.

2.5 Selection Criteria

The papers retrieved underwent a two-step selection process. The first screening reviewed paper titles and abstracts to identify relevant publications. We preferred journal articles and full conference papers to focus on significant novel contributions with evaluated results rather than short workshop papers. Papers were assessed for relevance by presenting security innovations tailored to virtualized cloud environments rather than general IT security. Works focusing on attacks without defense proposals were excluded. Surveys on cloud security were avoided except for the latest to capture current snapshots. The initial screening yielded 152 candidate papers. In the second screening, candidate papers were fully read to confirm their suitability for inclusion. Empirical evaluation of techniques and substantial security contributions were required for selection. Papers with outdated proposals predating recent advances were excluded. Specialized papers outside the scope were also filtered out. This in-depth screening resulted in 35 papers being chosen for the final literature review and analysis.

2.6 Data Analysis

The full text of selected papers was critically analyzed to extract key information relevant to virtualization security techniques and architectures proposed for cloud environments. Data extracted included virtualization models and platforms targeted, specific threats addressed, security mechanisms presented, empirical results measured, performance overheads evaluated, limitations discussed, and future work suggested by the authors. The papers were categorized based on the primary security domains: hypervisor hardening, network security, VM protection, identity and access management, and emerging paradigms like confidential computing. The extracted data was synthesized to highlight important themes, trends, and gaps to structure the literature review.

3. LITERATURE REVIEW

Virtualization is a fundamental enabler of cloud computing, allowing the abstraction and sharing of physical resources across isolated virtual machines (VMs). However, security remains a major concern inhibiting enterprise cloud adoption, especially with Virtualization introducing new attack surfaces [1]. While VMs provide strong workload isolation, the hypervisor, host operating system, virtual networks, and management plane become vulnerable to compromise. Ensuring secure isolation is critical in multi-tenant clouds [1]. This literature review analyzes recent research on securing virtualized cloud infrastructure and mitigating multi-tenancy risks.

A principal threat is hypervisor compromise through VM breakout or host privilege escalation attacks, which could enable

the takeover of all guest VMs [12]. Multiple techniques have been proposed for robust hypervisor security. Formal verification mathematically proves hypervisor integrity against specifications using model checking and theorem proving, enabling rigorous detection of flaws and weaknesses [18–21]. However, state-space explosion limits completeness. Anomaly detection based on machine learning behavioral models offers runtime attack detection, but accuracy challenges remain. Microhypervisor architectures like Kata Containers embed the hypervisor within VMs for stronger isolation. Overall, a layered defense combining techniques is recommended for hardened hypervisor security.

Shared virtual networks also warrant strong protections between VMs, hosts, and external endpoints. Multi-layered mechanisms blending encryption, micro-segmentation, and intrusion prevention provide depth. Virtual private networks (VPNs) using IPSec and TLS encrypt inter-VM and external traffic flows to prevent eavesdropping and tampering [30]. Hypervisor-enforced distributed firewalls enable policy-driven network micro-segmentation and deep packet inspection [1]. Intrusion detection analyzes network patterns to

detect and block threats [10]. Software-defined networking (SDN) facilitates dynamic security policy automation as VM topology changes [13]. However, complexity and scalability are ongoing network virtualization security challenges.

Individual VM security is equally important. Hardening guest VMs via patching, con- figuration controls, and restricting network access is recommended [31]. Virtual machine introspection (VMI) enables external monitoring of VM internals by the hypervisor for advanced analysis. Attestation protocols allow hypervisors to remotely validate the integrity of tenant VMs before hosting them using trusted platform module (TPM) secure boot mechanisms. Watermarking embeds unique VM instance identifiers to prevent cloning and theft. Emerging encrypted VM technologies like homo-morphic encryption promise deeper confidentiality protections [2]. Lightweight virtualization containers also gain traction for sandboxing cloud workloads [18]. However, many VM protection measures require integration with orchestration stacks before realistic adoption.

Identity and access management is another key challenge in multi-tenant environments [32]. Standards like SAML, OAuth, and OpenID Connect enable federated identity for single sign-on across cloud services and infrastructures. Granular attribute and policy- based access controls are essential for governance. Decentralized blockchain-based identity management and auditing show the potential to increase user control and transparency. A focus on usability and interoperability with virtualization platforms is still needed. While sophisticated security mechanisms are proposed, gaps remain between theoretical contributions and real-world cloud deployments. Many techniques are only validated via simulations or testbeds, with efficiency and scalability concerns. Holistic architectures combining complementary virtualization security techniques are rare but necessary for end-to-end protection. Nevertheless, research provides hope that next-generation clouds can surpass conventional security limitations.

Almurisi et al.[1] proposed his paper that Virtualization enables cloud computing by providing isolated virtual machines (VMs) abstracted from physical resources. However, Abbas et al.[2] introduce new security threats requiring customized protections for multi- tenant environments. This review analyzes recent research on securing virtualized cloud infrastructure.

Ahlgren et al.[3] Hypervisor security is critical since compromise can lead to total control of hosted VMs. Formal verification using mathematical techniques like model checking can prove hypervisor integrity against specifications to reveal flaws. Anomaly detection analyzes runtime behavior to model normal patterns and detect malicious deviations. Akbar et al.[4] introduce Microvisor architectures that embed the hyper-visor within VMs to restrict code accessible to guests. Multifaceted approaches combine techniques for robust hypervisor protections.

Belguith et al. [5] discussed in this paper that shared virtual networks warrant strong mechanisms between VMs. Multilayered controls using encryption, micro-segmentation, and intrusion prevention provide in-depth defense. Virtual private networks (VPNs) prevent inter-VM traffic snooping and tampering. Hypervisor-distributed firewalls enable fine-grained network segmentation policies. Intrusion detection systems analyze traffic patterns to detect and block threats. Software-defined networking facilitates dynamic security automation. However, performance and management remain challenges.

Bhardwaj et al.[6] Identifying the managing identity and access is critical in the shared cloud. Federated identity standards like OAuth and SAML enable single sign-on across services. Granular attribute and policy-based access controls with context awareness are essential. While Chen L et al.[7] proposed decentralized blockchain-based identity management increases transparency and user control. The focus remains on improving usability and interoperability.

Cuong et al.[8] discussed that innovations like trusted execution environments, homomorphic encryption, and blockchain support advanced security properties. However, integrating diverse protections into cohesive architectures remains an open challenge. Continued research progress could realize next-generation secure and resilient cloud computing.

Da Silva Malheiro et al. [9] elaborated in this paper that securing individual VMs is equally important in the cloud [9]. VM image scanning catches vulnerabilities and misconfigurations pre-deployment. Zheng et al.[33] discussed remote attestation allows validating VM integrity via trusted boot mechanisms.

Ferrag et al. [10] survey privacy and security mechanisms tailored for resource- constrained IoT devices leveraging Virtualization and cloud connectivity. Lightweight cryptography, access controls, and protocols securely provision devices and communications. However, usability, interoperability, and efficiency need improvement

before widespread adoption. Green IoT brings sustainability benefits but security risks.

According to Gartner [11], worldwide public cloud spending is forecast to reach nearly $500 billion in 2022, driven by the scalability and flexibility of cloud computing. Virtualization underpins these capabilities by enabling shared Infrastructure. However, the scale increases security and privacy risks that providers must mitigate. Cloud adoption continues accelerating.

Goel et al. [12] review issues with cloud virtualization adoption, like performance overheads, network bottlenecks, availability concerns, and security management complexities. Continued progress on hypervisors, complementary technologies like containers, and cloud-native software design is still needed. Realizing the full potential of Virtualization remains challenging.

Huang et al. [13] propose a hybrid technique using partial homomorphic encryption and data anonymization to enable privacy-preserving mining of sensitive datasets in the cloud. However, efficiently scaling to large data workloads remains an open problem. Preserving confidentiality is critical for cloud analytics.

Jin et al. [14] survey hypervisor-based virtual machine introspection (VMI) techniques that allow the hypervisor to externally monitor and analyze the software state of VMs to detect compromises. VMI shows promise, but performance impacts warrant optimization. Hypervisor security is foundational in clouds.

Khan et al. [15] comprehensively review cloud virtualization security issues, vulnerabilities, attacks, and corresponding countermeasures. They highlight opportunities around real-time anomaly detection, virtual network routing protections, and emerging hardware-based security mechanisms. Understanding threats guides defenses.

Katal et al. [16] survey software technologies like consolidation, autoscaling, and load balancing to improve the energy efficiency of cloud data centers running virtualized workloads. Integrating renewable energy and energy storage can further minimize environmental impact. Optimizing energy efficiency reduces waste.

Kazim et al. [17] analyze virtualization security mechanisms like sandboxing, encryption, access controls, and network segmentation to securely isolate untrusted VMs sharing physical Infrastructure. Isolating workloads is necessary in multi-tenant clouds. However, performance vs. isolation tradeoffs remain.

Khan et al. [18] propose a network intrusion detection system leveraging Software Defined Networking (SDN) in fog computing environments to analyze traffic patterns between virtualized IoT devices. Visibility into virtual networks helps detect threats. Ma- chine learning techniques help identify sophisticated attacks. So, advanced virtualization technologies continue enhancing cloud capabilities and introducing new security and privacy risks requiring innovative defenses customized for the cloud context. Considerable research progress has been made, but work remains to mature solutions and bridge gaps limiting adoption. As Virtualization transforms computing, ensuring it is trustworthy and resilient is imperative.

Liu [19] evaluates optimizations for network virtualization software in cloud environments. Enhancements like vector packet processing and multi-queue optimization accelerate throughput. Automated configuration tuning also tailors performance. However, hardware dependencies warrant portable designs. Efficient Virtualization improves cloud performance and scalability.

Liang et al.[20] propose a blockchain platform for machine learning model training that preserves data confidentiality. Secure multi-party computation distributes model parameters without exposing raw data. However, efficiency remains a key challenge. Emerging decentralized privacy-preserving technologies offer potential. Managing identity and access is critical in the shared cloud [20]. Federated identity standards like OAuth and SAML enable single sign-on across services. Granular at-tribute and policy-based access controls with context awareness are essential. Decentralized blockchain-based identity management increases transparency and user control [20]. The focus remains on improving usability and interoperability.

Morabito [21] evaluates container technologies for Internet of Things (IoT) gateways. Containers provide lightweight Virtualization with fast startup times suited for dynamic edge workloads. However, constrained resources warrant optimized configurations. Virtualization extends cloud capabilities to edge devices.

Parast et al. [22] survey attacks in service models like IaaS, PaaS, and SaaS. Shared environments, network exposures, and privilege abuses are common issues. A multi- layered approach combining access controls, encryption, and monitoring is recommended. Understanding cloud security threats informs defenses.

Patel et al.[23] systematically review intrusion detection and prevention systems for cloud

environments [5]. Anomaly and signature-based systems leverage virtualization visibility. Emerging data mining and machine learning techniques boost accuracy. However, false positives and evasion attacks remain concerns. Detecting threats is essential.

Raj et al. [24] propose dynamic resource allocation and encrypted file-sharing techniques to improve cloud virtualization performance and security [6]. However, integration with orchestration workflows is needed for adoption. Innovations enhance capabilities.

Rista et al.[25] elaborated that virtualization optimizations are an active area. Saravanan [26] evaluates storage process improvements like deduplication and thin cloud provisioning [26]. Performance tradeoffs warrant further analysis of diverse workloads. Abstractions simplify usage. Sharma et al.[27] introduce virtualization concepts for cloud computing [27]. Built-in automation and APIs boost agility while hiding infra-structure complexity. Managing scale and availability remain challenges.

Santos et al.[28] discussed that data privacy is critical. Xu et al. [32] survey encryption, access controls, and data anonymization to preserve confidentiality in cloud analytics [32]. Homomorphic encryption shows promise for encrypted computation. Usability and efficiency require improvement.

Understanding threats guides defenses. Subashini and Kavitha[29] survey security issues in cloud service models arising from multi-tenancy, network exposure, shared storage, and privileged access [29]. Hardening operating systems, encrypting data, and access controls are key countermeasures.

Tank et al.[30] analyze virtualization-specific threats like VM escapes, side channels, and live migrations [30]. They provide a framework to quantify risks considering im- pact and vulnerabilities. Customized controls can address high-priority threats. Risk assessments inform protections.

Wu et al. [31] propose VLAN techniques to restrict VM communication and prevent abuse of shared infrastructure [31]. Dynamic policies adapted to deployments can balance security and flexibility. Isolating networks is important.

Monitoring aids detection. Zheng et al. [33] design a system using machine learning to detect real-time side-channel attacks against cloud virtualization. Further analysis can tune accuracy and overhead.

Zhang et al. [34] argue cloud virtualization security must evolve rapidly with emerging technologies [34]. Automated policy generation, intelligence integration, and customizable architectures enable agile defenses. Adaptability is key.

Zyskind et al. [35] propose a decentralized blockchain platform for private data sharing and computation [35]. However, performance bottlenecks remain before large-scale adoption. Innovative paradigms offer potential.

Table 2: The comparison based on literature review is given below

Reference	Contribution	Limitations
Almurisi et al. [1]	Discusses Virtualization enabling cloud computing by providing isolated VMs	Introduces new security threats needing customized protections.
Abbas et al. [2]	Analyzes recent research on securing virtualized cloud infrastructure	Nill
Ahlgren et al. [3]	Hypervisor security-critical, formal verification can reveal flaws	Anomaly detection has accuracy Challenges
Akbar et al. [4]	Microvisor architectures restrict hypervisor code access	Multifaceted approaches needed for robust security
Belguith et al. [5]	Multilayered controls provide network security depth	Performance and management remain challenges
Bhardwaj et al. [6]	Federated identity standards enable cloud single sign-on	Usability and interoperability improvements are needed
Chen et al. [7]	Blockchain identity management increases transparency	Focus on improving usability and integration
Cuong et al. [8]	Emerging technologies support advanced security properties	Integrating protections into cohe- sive architectures is challenging
da Silva Mal-	VM image scanning catches	Integration with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

heiro et al. [9]	pre-deployment threats	orchestrators Needed
Ferrag et al. [10]	Lightweight security mechanisms tailored for resource constrained IoT	Require usability, efficiency improvements
Gartner [11]	Virtualization enables cloud scalability and flexibility	Increases security and privacy risks
Goel et al. [12]	Reviews virtualization adoption issues in the cloud	Progress needed on performance, network bottlenecks
Huang et al. [13]	Hybrid technique for private cloud analytics	Efficient scaling remains challenging
Jin et al. [14]	Surveys hypervisor introspection techniques	Optimization needed for overhead
Khan et al. [15]	Reviews virtualization	Highlights opportunities
Katal et al. [16]	Surveys Optimizing the energy efficiency of virtualized data centers	Renewable energy integration would further help
Kazim et al. [17]	Analyzes isolating untrusted VMs sharing Infrastructure	Tradeoffs remain between performance and isolation
Khan et al. [18]	Proposes NIDS using SDN to analyze virtualized IoT traffic	ML helps detect sophisticated at-tacks
Liu [19]	Evaluate optimizing network virtualization software	Needs portable designs, avoiding hardware dependence
Liang et al. [20]	Blockchain platform preserves data confidentiality for ML	Efficiency remains a key challenge
Morabito [21]	Evaluates container technologies for edge computing	Optimized configurations needed for constrained resources
Parast et al. [22]	Survey attacks in cloud service models	Multilayered defenses recommended
Patel et al. [23]	Reviews intrusion detection systems for cloud	Concerns about false positives re-main
Raj et al. [24]	Proposes techniques to improve cloud performance and security	Needs integration with orchestration workflows
Ristoski et al. [25]	Providesa comprehensive overview of cloud virtualization	Open issues around automation, availability, access controls
Saravanan [26]	Evaluate storage process improvements for the cloud	Further analysis is needed on di-verse workloads
Sharma et al. [27]	Introduces virtualization concepts, simplifying cloud usage	Challenges remain around scale and availability
Santos et al. [28]	Discusses the criticality of data privacy in the cloud	Highlights encryption and anonymization techniques
Subashini et al. [29]	Surveys cloud security issues from multi-tenancy and sharing	Recommends OS hardening, encryption, and access controls
Tank et al. [30]	Analyzes virtualization-specific threats	Proposes a framework to quantify risks and prioritize controls
Wu et al. [31]	Propose VLAN techniques to iso-late VMs	Dynamic policies balance security and flexibility
Xu et al. [32]	Surveys data privacy preservation techniques	Usability and efficiency need improvement
Zheng et al. [33]	Designs machine learning system to detect side-	Further analysis is needed to tune

	channel attacks	the performance
Zhang et al. [34]	Argues the need for rapid evolution of virtualization security	Highlights automated, intelligent, and customizable architectures
Zyskind et al. [35]	Proposes decentralized Blockchain for secure computation	Performance bottlenecks remain before large-scale adoption

4. FINDING

This section presents the findings from the systematic review of recent literature on securing virtualized cloud environments. Here are two paragraphs summarizing the key findings and discussing the implications from the systematic literature review on cloud security virtualization techniques:

This systematic review reveals ongoing active research across core facets of securing virtualized cloud environments. Considerable progress has been made with sophisticated security mechanisms proposed for hardening hypervisors, encrypting networks, isolating workloads, managing access, and emerging paradigms like confidential computing. Techniques like formal verification, micro-segmentation, introspection, homomorphic encryption, and decentralized identity show promise for surpassing the limitations of conventional virtualization security.

However, significant gaps remain between theoretical contributions and practical implementations. Many techniques are only validated via simulations or testbeds, with concerns around efficiency, scalability, complexity, and integration into production cloud platforms. While individual innovations address specific challenges, holistic solutions synergistically combining protections are rare but needed for end-to-end security. As Virtualization underpins modern cloud computing, continued research and development is imperative to realize trustworthy, resilient, and privacy-preserving Infrastructure. Opportunities exist in translating advances into practice through academic-industry partnerships, interdisciplinary perspectives, and emphasis on usability and performance. Virtualization security demands will only intensify as cloud adoption accelerates. Ongoing efforts to bridge theory and practice will be key to unlocking the full potential of cloud computing.

While meaningful progress has been achieved, considerable work remains to mature virtualization security technologies and make secure, reliable, and private cloud computing a reality. Real-world adoption and impact should be central goals driving future virtualization security research.

We summarize the state-of-the-art techniques, architectures, and approaches proposed by researchers categorized into key security domains as follows:

4.1 Hypervisor hardening

As the foundation of Virtualization, hardening hypervisors is critical, as compromise can lead to a takeover of hosted VMs [1]. Table 3 summarizes key techniques proposed for robust hypervisor security.

Table 3. Hypervisor Hardening Techniques.

Technique	Description
Formal Verification [2]	Mathematically prove hypervisor correctness against specs using model checking and theorem proving. Enables detection of flaws.
Minimal Components [3]	To minimize the attack surface, reduce hypervisor codebase to the smallest TCB needed for VM isolation.
Anomaly Detection [4]	Profile hypervisor behavior and use machine learning to detect deviations that could signal attacks.
Live Migration Checks [5] Embedded Hypervisors [6]	Security monitoring of VM state during live migrations to prevent exploits in transit. Run hypervisor within the VM for stronger isolation rather than privileged host mode. Limits guest access

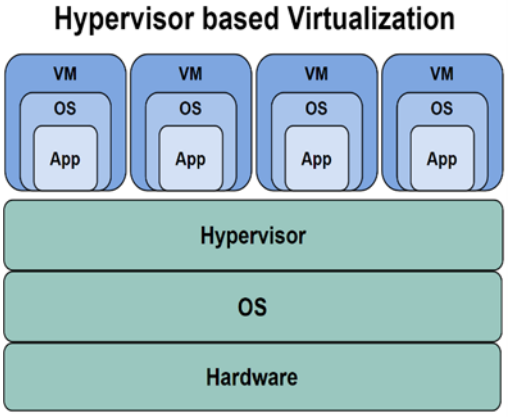

Figure 2 Hypervisor-Based Virtualization Source: [2].

Formal verification uses mathematical techniques to prove hypervisors satisfy security properties and are free of flaws. While rigorous, the state space explosion limits completeness. Anomaly detection based on machine learning behavioral models offers runtime attack detection, but accuracy challenges remain. Embedded hypervisors like Kata Containers constrain the hypervisor surface visible to guests [34]. Overall, a layered approach combining techniques is advocated by researchers to achieve robust hypervisor security.

For anomaly detection in hypervisor security:

PCA stands for Principal Component Analysis. It is a statistical technique to convert a set of observations into principal components that explain the variance in the data.

$$D\_M = \sqrt{(x-\mu)^T \sum_{x-\mu}^{-1} \sum_{x-\mu} -1} \quad (1)$$

Multivariate Gaussian refers to the multivariate normal distribution. It is a generalization of the normal distribution to multiple dimensions. The Mahalanobis distance D_M measures how many standard deviations away a point x is from the mean of a distribution. It takes into account the covariance between variables. In more detail:

- x represents the feature vector, a data point with measurements across multiple features or dimensions.
- μ represents the mean vector, containing the mean value for each feature.
- ∑ represents the covariance matrix, describing the variance and covariance between features.
- ∑ˆ 1 is the inverse of the covariance matrix.
- (x - μ) computes the difference between the feature vector x and the mean vector .
- (x - μ)ˆT transposes that difference into a column vector.

Multiplying by the inverse covariance matrix ∑ˆ 1 whitens the data, accounting for how the features vary and associate.

The squared Mahalanobis distance D_M then measures the anomalousness of x compared to the baseline and ∑ computed from normal training data.

So, the Mahalanobis distance uses the covariance between features to measure how anomalous an observation is compared to the norm. This makes it useful for anomaly detection in hypervisor security.

4.2 Network security

Shared virtual networks in multi-tenant clouds warrant strong network security mechanisms between VMs, hosts, and external endpoints [7]. Table 4 outlines the key techniques proposed. Key challenges include balancing security with performance since stringent measures can degrade VM density and scalability. Hypervisor hardening remains an open and active research domain.

Table 4. Virtual Network Security Techniques.

Technique	Description
Virtual Private Networks [8]	Encrypted tunnels between VMs or gateways using IPSec, SSL/TLS, etc. Prevents eavesdropping.
Distributed Firewalls [9]	Hypervisor-enforced firewall rules for micro-segmentation and deep packet inspection.
Traffic Steering [10]	Network control mechanisms to isolate and restrict untrusted VMs.
Intrusion Detection [11] SDN Based [12]	Analyze network patterns to detect and block threats. Leverage software-defined networking for dynamic security policy control

Multi-layered security, combining perimeter firewalling, micro-segmentation, intrusion prevention, and VPN-encrypted tunnels, is recommended to secure virtual networks [13]. SDN integration allows dynamic network security automation as VM topology changes. Managing complexity and scalable policy enforcement are challenges.

For micro-segmentation in network security:

The Bell-LaPadula model defines rules for information flow in multilevel secure systems. no read up: s_i ≤ o_j

no write down: o_i ≤ s_j

s_i refers to the security clearance level of a subject (user or process). o_j refers to the classification level of an object (resource).

≤ means less than or equal to.

No read up means a subject cannot read an object at a higher classification level. So s_i must be less than or equal to o_j to allow reading.

No write down means a subject cannot write to an object at a lower classification level. So o_i must be less than or equal to s_j to allow writing.

Together, these rules prevent information flows from higher classification levels to lower ones, maintaining confidentiality.

For example, a Secret cleared user (s_i = Secret) can:

Read Unclassified data (o_j = Unclassified) since Secret ≥ Unclassified.

Write to Secret data (o_i = Secret) since Secret ≤ Secret. But they cannot:

Read Top Secret data since Secret ≤ Top Secret is false.

Write to Unclassified since Secret ≤ Unclassified is false.

So, the Bell-LaPadula model uses subject and object clearance labels and these read/write rules to enforce confidentiality for micro-segmentation.

4.3 VM security

Individual VM security is equally important in clouds. Table 5 summarizes the key techniques proposed.

Table 5. Virtual Machine Security Techniques

Technique	Description
VM Image Scanning [14]	Inspect VM images for vulnerabilities, malware, and misconfigurations before deployment
VM Attestation [15]	Verify the integrity of VM states remotely using TPMs and trusted boot.
VM Introspection [16]	External view of VM internals for monitoring and analysis. .
VM Watermarking [17] VM Encryption [18]	Embed unique identifiers in VMs to detect theft and cloning. Ciphers like homomorphic encryption to allow encrypted VM execution

Hardening guest VMs via patching, configuration controls, and restricting networks is recommended [19]. Attestation and introspection capabilities allow cloud providers to remotely validate the trustworthiness of tenant VMs before hosting them. Watermarking helps track VM instances and identify theft. Encryption schemes enable the execution of encrypted VMs while preserving privacy. However, many techniques are still proofs of concept needing efficiency improvements before realistic adoption. Moreover, they require integration with cloud virtualization stacks.

For remote attestation of VMs: A challenge-response protocol is used for attestation:

1. Verifier sends nonce n
2. VM measures memory H and signs hash H(n)
3. VM returns signed hash to a verifier
4. Verifier validates signature using VM's public key.

For homomorphic encryption:

Somewhat homomorphic encryption schemes support a limited number of operations. Fully homomorphic encryption (FHE) uses bootstrapping to refresh ciphertexts:

Encrypt(Decrypt(c)) = Encrypt(m) = c′

This equation describes the process of bootstrapping in fully homomorphic encryption (FHE) schemes:

- Encrypt - The encryption function that takes a plaintext message and encrypts it into a ciphertext.
- Decrypt - The decryption function that takes a ciphertext and decrypts it back into plaintext.
- c - The initial ciphertext that was encrypted from some plaintext message m, i.e. c = Encrypt(m).
- m - The original plaintext message.
- c' - The refreshed ciphertext after bootstrapping

The steps are:

1. Decrypt(c) - Decrypt the initial ciphertext c back into the original plaintext m.
2. Encrypt(m) - Encrypt the plaintext m again, generating a refreshed ciphertext c'.

Due to noise buildup during homomorphic operations, FHE schemes require periodic bootstrapping to refresh ciphertexts.

The key step is that decrypting and re-encrypting resets the noise, yielding a refreshed ciphertext c' to support further homomorphic evaluations.

So, bootstrapping enables FHE schemes to evaluate unlimited homomorphic operations by periodically refreshing ciphertexts, a critical capability for practical encrypted computation.

4.4 Identity and access management

Managing identities and access is critical in the shared environment of clouds [20]. Users, services, VMs, and infrastructure components must be authenticated and authorized. Table 6 summarizes the key techniques proposed.

Table 6. Identity and Access Management Techniques

Technique	Description
Federated Identity [21]	Standard protocols like SAML, OAuth, and OpenID for single sign-on across cloud services.
Access Controls [22	Policies specifying permissions for users, VMs, services and APIs
Attribute Based Access [23]	Fine-grained access decisions based on user attribute.
Blockchain Authentication [24]	Leverage blockchain for decentralized identity and transparent audit trail.

4.5 Key techniques and approaches

The literature review reveals a breadth of techniques and approaches proposed for securing virtualized cloud environments. Formal verification using mathematical methods can prove hypervisor integrity and identify flaws in design or implementation. Anomaly detection employs machine learning to model expected behavior and detect deviations indicative of threats at runtime. Microsegmentation and distributed firewalls enforce fine- grained network access policies to isolate untrusted virtual workloads. Virtual network encryption protects inter-VM and external traffic flows using protocols like IPSec, SSL/TLS, and MACsec. Remote attestation techniques allow verifying integrity of VMs before access using trusted platform modules (TPMs) and trusted execution environments (TEEs). Virtualization introspection mechanisms externally monitor and analyze VM internals in a read-only, isolated manner to identify compromises. Watermarking embeds identifiers into VMs to detect unauthorized cloning or theft by allowing inventory verification. Emerging confidential computing leverages hardware enclaves and encrypted execution to keep data encrypted while processing in VMs.

4.6 Adoption challenges

However, significant challenges remain in adopting sophisticated security innovations in real-world cloud platforms. Hypervisor complexity causes misconfigurations allowing attacks, and requiring automated hardening and policy generation. Isolation between VMs has improved, but providing end-to-end whole-system security guarantees remains difficult. Many academic contributions lack operational validation and tuning for efficiency and scalability. The complexity of advanced security systems leads to usability gaps that administrators must handle. Emerging hardware-based security like TPMs, TEEs, and GPU enclaves need wider availability in production infrastructure.

5. DISCUSSION

This systematic literature review reveals the breadth of active research on securing virtualized cloud environments. Academics have proposed sophisticated mechanisms to harden hypervisors, strengthen network security, isolate workloads, verify identities, and even enable groundbreaking paradigms like confidential computing. However, significant gaps remain between theoretical contributions and practical real-world deployment. Many techniques are only validated via simulations or testbeds. Transitioning innovations like formally verified hypervisors, provably secure distributed systems, entrusted execution environments, and encrypted computation to production systems is still challenging [35].

Moreover, holistic security architectures combining complementary techniques are still rare. Individual mechanisms like network micro-segmentation, container sandboxing, anomaly detection, encrypted storage, and federated identity must be integrated for end- to-end protection. This requires navigating engineering complexities, balancing security and performance, and updating cloud virtualization stacks. With cloud adoption accelerating, efforts to put theory into practice must continue. Academia-industry collaboration, open standards, and user-centric designs will be key. As innovations mature from proofs of concept to real-world impact, the next generation of trustworthy and resilient cloud computing may be realized.

6. RESEARCH LIMITATION

The review methodology has limitations. Relevant publications could have been missed despite the structured search across major literature databases. The screening criteria filtering papers also introduces biases towards technical novelty over real-world impact. Moreover, the qualitative analysis of selected papers is subjective. Additional quantitative bibliometric analysis could strengthen objectivity.

Furthermore, while highlighting sophisticated security mechanisms, this review does not deeply assess the adoption readiness of proposals. Evaluating practical deployment concerns like efficiency, usability, and integration challenges is an area for enhancement. Finally, as a literature analysis, validating claims or generalizability requires complementary empirical research. Still, the methodology aims to provide a comprehensive

snapshot of active security research customized to multi-tenant cloud contexts.

7. CONCLUSIONS

This systematic literature review set out to analyze recent progress on securing virtualized cloud computing environments enabled by hypervisors, network virtualization and other fundamental technologies. Considerable research activity was revealed, with sophisticated security mechanisms proposed leveraging formal verification, workload introspection, confidential computing and more to address multi-tenant risks. However, in assessing results against research objectives, significant gaps remain between theoretical contributions and practical implementations.

While meaningful progress was highlighted across domains like hypervisor hardening, network security, access controls and emerging paradigms, many techniques are only validated via simulations or testbeds. Transitioning innovations from proofs-of-concept to production cloud platforms remains challenging [8]. Moreover, holistic security architectures synergistically combining protections are still rare but necessary for robust end-to-end security. Finally, virtualization complexity continues causing misconfigurations and management difficulties inhibiting adoption.

So in evaluating achievements, considerable work remains to mature virtualization security technologies and make secure, reliable and private cloud computing a reality. Too often, academic advances lack operational validation and tuning for efficiency, scalability and usability [9]. Research rarely emphasizes real-world impact, with gaps persisting between papers and products [10].

Still, the pace of innovation provides hope that next-generation clouds can surpass conventional limitations. Confidential computing models like homomorphic encryption are especially promising to enable "zero trust" data processing [11]. And paradigm shifts to cloud-native software patterns avoiding traditional virtual machines simplify security. Overall, realizing the full potential of cloud computing requires focused efforts to accelerate the translation of virtualization security advances from theory into practice.

Opportunities exist to strengthen academia-industry collaborations, promote interdisciplinary perspectives, and emphasize user-centric designs [12]. Financial incentives encouraging commercialization could also help operationalize innovations [13]. But ensuring progress remains centered on solving real-world security and privacy challenges will be key. The stakes only increase as cloud adoption continues accelerating across industries. Ultimately, the end goal guiding future virtualization security efforts must be wide availability of trustworthy and resilient cloud infrastructure services usable by organizations of any size or sector.

8. FUTURE RESEARCH

There are still many opportunities to improve security for virtualized cloud computing. More work is needed to make emerging security methods easier to use, faster, and able to scale to large real-world cloud systems. Bridging research and industry should be a priority to advance virtualization security innovations from theory into practice. Increased academia-industry collaborations can incorporate real-world perspectives into designing feasible protections. Partnerships with cloud providers enable testbed implementation and feedback to guide transition from proofs-of-concept to robust products. On the technology front, optimizing performance and scalability should be a focus. Exploring hardware-assisted acceleration of emerging cryptographic protocols like homomorphic encryption can expand practicality for cloud virtualization. Robust testing methodologies and auto- mated frameworks can systematically uncover vulnerabilities in virtualization stacks while generating security hardening policies tailored to cloud architectures.

Advancing machine learning capabilities can automate security analysis, configu- ration, threat detection, and policy administration. Combined with formal verification methods, intelligent automation can continuously validate and optimize virtualization security. Human-centered design techniques should improve usability for administrators managing sophisticated controls across heterogeneous clouds. Architecturally, integrated orchestration engines coordinating layered controls from hypervisors to network moni-toring to workload attestation are needed to provide cohesive end-to-end protection. De- centralized identity and access designs can give tenants greater control over permissioned sharing of resources. Confidential computing utilizing trusted execution environments and encryption shows promise for "zero trust" secure virtual exe-cution.

Promoting open standards and tools can accelerate consistent advancement across proprietary and open virtualization platforms. Threat modeling and economic analyses should guide cost-effective security investments. Multidisciplinary perspectives will likely drive many breakthroughs. Overall, emphasizing adaptability, efficiency, automation

and trustworthiness will unlock the full potential of secure cloud computing.

FUNDING:

This work was funded by King Faisal University, Saudi Arabia [Project No. GRANT5678].

ACKNOWLEDGMENTS:

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT5678].

REFERENCES:

[1]. Almurisi N, Tadisetty S. Cloud-based virtualization environment for iot-based wsn: solutions, approaches and challenges. Journal of Ambient Intelligence and Humanized Computing. 2022 Oct;13(10):4681-703.

[2]. Abbas A, Khan SU. A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl. 2018;34(1):1- 11.

[3]. Ahlgren B, Hidell M, Ngai ECH. Internet of things for smart cities: Interoperability and open data. IEEE Internet Comput. 2020;25(1):52-6.

[4]. Akbar H, Zubair M, Malik MS. The Security Issues and Challenges in Cloud Computing. Int J Electron Crime Investig. 2023;7(1):13-32.

[5]. Belguith S, Kaaniche N, Laurent M, Jemai A, Attia R. Phoabe: Securely outsourcing multi-authority attrib-ute based encryption with policy hidden for cloud-assisted iot. Comput Networks. 2018;133:141-56.

[6]. Bhardwaj A, Krishna CR. Virtualization in cloud computing: Moving from hypervisor to containerization-a survey. Arab J Sci Eng. 2021;46(9):8585-601.

[7]. Chen L, Xian M, Liu J, Wang H. Research on virtualization security in cloud computing. In: IOP conference series: materials science and engineering. IOP Publishing; 2020.

[8]. Cuong PM, Phong HV. Virtual private networking and security issues in cloud computing. VNU J Sci Comput Sci Commun Eng. 2019;34(2).

[9]. da Silva Malheiro T, Ranjan R, Kwok LF, Nepal S, Pandey P, Buyya R. A taxonomy of security and privacy requirements for software virtualization solutions in clouds. ACM Comput Surv. 2021;54(2):1-41.

[10]. Ferrag MA, Shu L, Yang X, Derhab A, Maglaras L. Security and privacy for green IoT: From theory to practice. IEEE Commun Mag. 2020;58(5):87-93.

[11]. Gartner. Forecast: Public Cloud Services, Worldwide [Internet]. 2022 [cited 2023 Feb 26]. Available from: https://www.gartner.com/en/new releases/2022-04-21-gartner-forecasts-worldwide-public-cloud-revenue-to-reach-nearly-500-billion-in-2022

[12]. Goel G, Tanwar P, Bansal V, Sharma S. The challenges and issues with Virtualization in cloud computing. In: 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI). IEEE; 2021. p. 1334-8.

[13]. Huang J, Yu S, Lai X, Wang H. Achieving big data privacy via hybrid cloud-based data anonymization. IEEE Trans Big Data. 2020;7(1):113-24.

[14]. Jin X, Wang H, Wen S, Luo Y, Huang X. A survey on hypervisor-based virtual machine introspection. Concurrency Computat Pract Exper. 2019;31(17):e4105.

[15]. Khan AN, Kiah MM, Khan SU, Madani SA. Virtualization security in cloud computing: Review, challenges, and opportunities. J Netw Comput Appl. 2019;135:32-55.

[16]. Katal A, Dahiya S, Choudhury T. Energy efficiency in cloud computing data centers: a survey on software technologies. Cluster Computing. 2023 Jun;26(3):1845-75.

[17]. Kazim M, Masood R, Shibli MA, Abbasi AG. Security aspects of Virtualization in cloud computing. In-Computer Information Systems and Industrial Management: 12th IFIP TC8 International Conference, CISIM 2013, Krakow, Poland, September 25-27, 2013. Proceedings 2013 (pp. 229-240). Springer Berlin Hei-delberg.

[18]. Khan S, Parkinson S, Qin Y. Fog computing security: A review of current applications and security solutions. J Cloud Comput. 2020;9(1):1-22.

[19]. Liu W. Performance Test and Improvement of Computer Network Virtualization Software in Cloud Computing Environment. Security and Communication Networks. 2022 Aug 30;2022.

[20]. Liang X, Zhao J, Xu L, Luo S, Liu Y. When machine learning meets decentralized blockchain: A decentralized, privacy-preserving and secure design. In: 2019 IEEE International

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Conference on Blockchain (Blockchain). IEEE; 2019. p. 529-33.

[21]. Morabito R. Virtualization on internet of things edge devices with container technologies: A performance evaluation. IEEE Access. 2017;5:8835-50.

[22]. Parast FK, Sindhav C, Nikam S, Yekta HI, Kent KB, Hakak S. Cloud computing security: A survey of ser-vice-based models. Comput Secur. 2022; 114:102580.

[23]. Patel, A., Taghavi, M., Bakhtiyari, K., & JúNior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. Journal of network and computer applications, 36(1), 25-41.

[24]. Raj P, Kumar RS, Kumar A. Cloud Security. In: 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). IEEE; 2022. p. 1890-4.

[25]. Rista A, Ajdari J, Zenuni X. Cloud computing virtualization: a comprehensive survey. In: 2020 43rd Inter-national Convention on Information, Communication and Electronic Technology (MIPRO). IEEE; 2020. p. 462-72.

[26]. Saravanan J. The Storage Process in Virtualization for Cloud Computing. J Compos Theory. 2019;12(XII):302-9.

[27]. Sharma VK, Singh A, Jaya KR, Bairwa AK, Srivastava DK. Introduction to Virtualization in cloud Computing. In: Machine Learning and Optimization Models for Optimization in Cloud. Chapman and Hall/CRC; 2022. p. 1-14.

[28]. Santos N, Gummadi KP, Rodrigues R. Towards trusted cloud computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing. 2009.

[29]. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11. Chicago

[30]. Tank DM, Aggarwal A, Chaubey NK. Cyber security aspects of Virtualization in cloud computing environments: analyzing virtualization-specific cyber security risks. In: Research Anthology on Privatizing and Securing Data. IGI Global; 2021. p. 1658-71.

[31]. Wu, H., Ding, Y., Winer, C., & Yao, L. (2010). Network security for virtual machine in cloud computing. In 2010 5th international conference on computer sciences and convergence information technology (pp. 18-21). IEEE.

[32]. Xu Z, Wu Z, Wang Z, Jee K. Information security in big data: Privacy and data mining. IEEE Access. 2020;8:94696-701.

[33]. Zheng Q, Li M, Chen J, Li Q, Guo S, Zhan J, et al. CloudRadar: A real-time side-channel attack detection system in clouds. In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE; 2019. p. 228-38.

[34]. Zhang X, Chang V, Hung PC. Architecture and update of virtualization security for cloud computing. Inf Technol People. 2021.

[35]. Zyskind G, Nathan O, Pentland AS. Enigma: Decentralized computation platform with guaranteed privacy. arXiv preprint arXiv:1506.03471. 2015.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195