Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos

Security in cloud computing: Opportunities and challenges

HanJung Youn
Seoultech 2015

Table of Contents

1. Introduction
2. Cloud computing architectural framework
3. Cloud security challenges
4. Security solutions in literature
5. Security issues in MCC
6. Discussion and open issues
7. Conclusions

1. Introduction

- the cloud computing paradigm has gained the widespread popularity in the industry and academia.
- Security is one of the biggest obstacles that hamper the widespread adoption of cloud computing

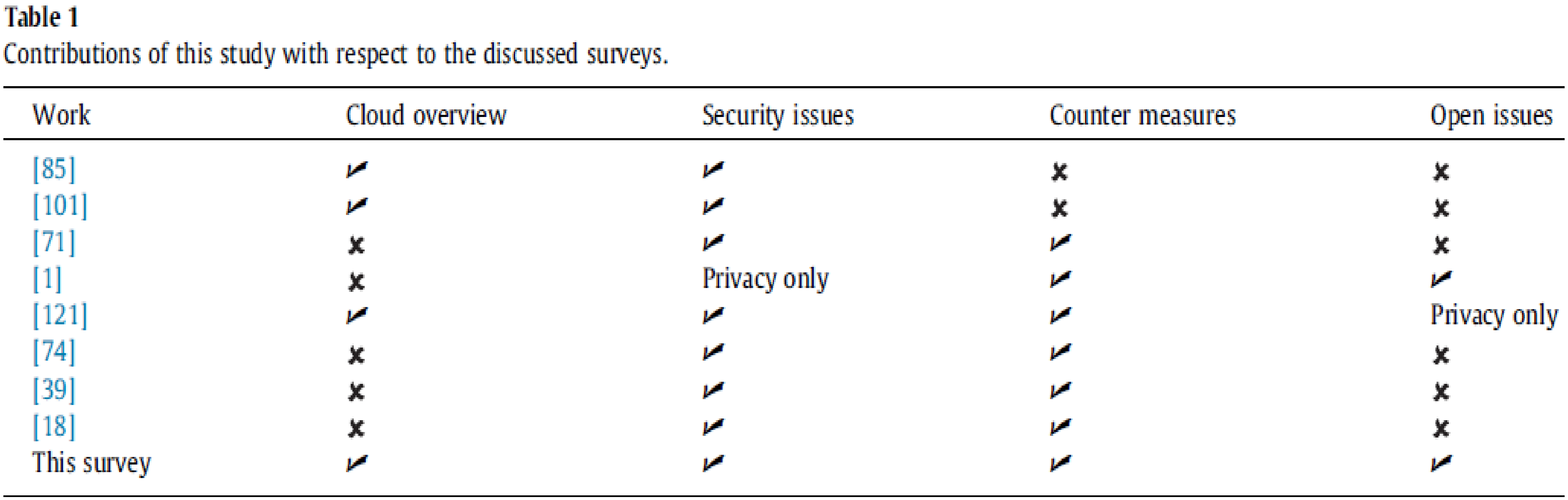


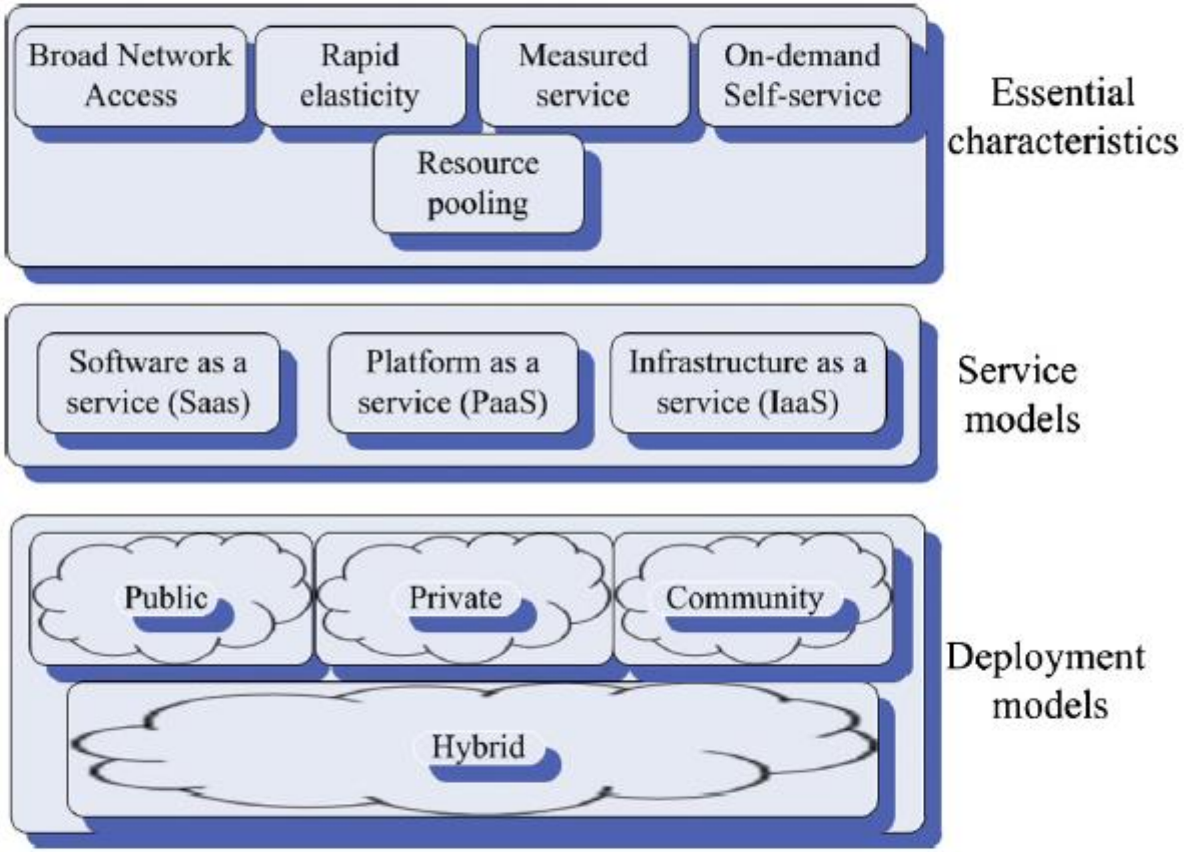
Table 1
Contributions of this study with respect to the discussed surveys.

Work	Cloud overview	Security issues	Counter measures	Open issues
[85]	✓	✓	✗	✗
[101]	✓	✓	✗	✗
[71]	✗	✓	✓	✗
[1]	✗	Privacy only	✓	✓
[121]	✓	✓	✓	Privacy only
[74]	✗	✓	✓	✗
[39]	✗	✓	✓	✗
[18]	✗	✓	✓	✗
This survey	✓	✓	✓	✓

2. Cloud computing architectural framework

- NISTs definition of cloud computing is widely accepted.
- The model comprising with three concepts
  - Essential characteristics
  - Service models
  - Deploying models

2. Cloud computing architectural framework



2.1 Essential characteristics

- On-Demand self-service
  - Customer can manage the services without human interaction.
- Broad network access
  - Services must be accessible to the customers using the standard mechanisms and protocols: ubiquitous network access.
- Resource pooling
  - The cloud's resources are shared among multiple customers by pooling in a multi-tenant environment.
- Rapid elasticity
  - The resources can be rapidly and elastically scaled as per customer's demands.
- Measured service
  - To optimize service provision, the usage and performance are metered and reported to customer and Cloud Service Provider(CSP).
- Multi-tenancy
  - Additional feature added by Cloud Security Alliance(CSA)
  - Single resource is shared by multiple customers

2.2 Service models

- Cloud service model is referred to as SPI(software, platform, infrastructure).
- Software as Service(SaaS)
  - it only provides software through internet.
- Platform as Service(PaaS)
  - It provide framework as IDE, OS, runtime engine for application.
- Infrastructure as Service(Iaas)
  - It refers to the hardware infrastructure as network, storage, memory, processor.

2.3 Deployment models

- Private cloud
  - Only for a single organization.
- Public cloud
  - Cloud`s infrastructure is owned by CSP and opend to general public and organization.
- Community cloud
  - It shared by a number of organizations and/or customers forming a community.
- Hybrid cloud
  - Mix of two or more clouds

3. Cloud security challenges

- Cloud models are supposed to use various technologies. This leads various security risk and vulnerabilities.

- This chapter is about security challenges at abstract level in
  - Communication security
  - Architectural security
  - Contractual and legal aspects

3.1 Challenges at communication level

- There are communications between the customers and cloud(external), cloud and infrastructure(internal).

- In external case is similar as any other communication over the internet.
  - Denial of service, spoofing, eavesdropping…
- Solution is also same
  - SSL, IPSec, IDS, IPS, certificate, encryption…

3.1 Challenges at communication level

- Internal communication generates cloud specific challenges because of its features and structure.

- Shared communication infrastructure
- Virtual network
- Security misconfiguration

3.1.1 Shared communication infrastructure

- Resource pooling not only results sharing of resources, but also allow the sharing of network infrastructure[28].

- This provides attacker the window of cross-tenant attack[39].

- Usually scanning is not allowed because it is hard to distinguish that attacker access or customer access on components.

- The user on cloud granted as super-user to manage their VMs.
- [12,28,39]

3.1.2 Virtual network

- Virtual network is a logical network built over a physical network [116]. The software-based components support the networking of VMs over the same host.
- Security mechanisms on physical network cannot monitor the traffic over virtualized network.
- Virtual network shared on multiple VMs that cause the possibility of attacks, such as DoS, traffic monitoring, sniffing, spoofing.
- The data transit of users can suffer from costly breaches.

- [33,47,116]

3.1.3 Security misconfigurations

- A small misconfiguration can break the security of system.
- Most misconfiguration occur when administrator choose familiar configuration tool with not necessarily covers all the security requirements.
- When migrating system, or changing traffic pattern or topology, the configuration must be dynamically managed to ensure security.
- any weakness in session configurations and protocol configurations can be exploited for session hijacking and to gain user sensitive data.
- [24,26,101]

3.2 Challenges at architectural level

- Virtualization issues
- Data/storage issues
- Web application and application programming interface (API) security
- Identity management and access control

3.2.1 Virtualization issues(1/3)

- Virtualization allows the use of same physical resources by multi users.
- Several VMs can be mapped to the same physical resources allowing the resource pooling in multi-tenant environment.
- VM image sharing [39,47]
  - Users can upload and download images from the repository.
  - Malicious user can analysis the code of the image to look for probable attack point. Or they can upload image that contains malware.
- VM isolation [33,101]
  - Each VMs in same physical hardware need to be isolated from each other. Although logically isolated each other, the access to same physical resources can lead to data breach and cross-VM attacks.

3.2.1Virtualization issues(2/3)

- VM escape [47,73,97]
  - It is a situation in which malicious user or VM escapes from the control of VMM or hypervisor. This can provides attacker access to other VMs or let VMM(VM monitor) down, or access on computing, storage hardware.
- VM migration [20,39,47,128]
  - It is the process of relocating a VM to another physical machine without shutting down.
  - There are many reasons of migration, such as load balancing, fault tolerance, and maintenance.
  - The data and code of VM become vulnerable to attackers during migration.

3.2.1Virtualization issues(3/3)

- VM rollback [39, 90, 116]
  - Rollback can revert previous vulnerability, security.
- Hypervisor issues [102, 106, 128]
  - The VMs management and isolation is the responsibility of the VMM. Compromised VMM can cause huge attack.
- VM sprawl [80, 97]
  - It is a situation where a number of VMS on the host system is continuously increasing and instantiated VMs are in idle state. This causes the resources of the host machine to be wasted.

3.2.2 Data/storage issues

- The cloud computing model does not deliver users with full control over data.
- Data privacy and integrity [39,47,65,93,99,110]
  - In a shared environment, the security strength of the cloud equals the security strength of its weakest entity.
  - A successful attack on a single entity will result in unauthorized access to the data of all the users.
  - The cryptographic key generation and management for cloud computing paradigm is still not standardized.

3.2.2 Data/storage issues

- Data recovery vulnerability [10,17,28]
  - In case of memory and storage resources, a malicious user can employ data recovery techniques to obtain the data of previous users.
- Improper media sanitization[28,47,107]
  - If the CSP does not sanitize the device properly, the data can be exposed to risks.
- Data backup [101]
  - A regular backup is needed at the CSP side. Moreover, the backup storage also needs to be protected from attacks.

3.2.3 Web application and API security

- Top ten risk in the web applications
  - Injection (SQL, OS, and LDAP)
  - Broken Authentication and Session Management
  - Cross-Site Scripting (XSS)
    - It occurs when an application takes untrusted data and sends it to a web browser without proper validation or escaping.
  - Insecure Direct Object References
  - Security Misconfiguration
  - Sensitive Data Exposure
  - Missing Function Level Access Control

3.2.3 Web application and API security

- Cross-Site Request Forgery (CSRF)
  - It forces a logged-on victim`s browser to send a forged HTTP request, including victim`s session cookie and other authentication information to hazard web application with confusing that is legal.
- Using Known Vulnerable Components
- Invalidated Redirects and Forwards

- The traditional security solutions are not suitable for the cloud environment because the risks of web application in cloud is much greater and complex issues.

3.2.3 Web application and API security

- The CSP can publish their APIs to market the features of their cloud.

- At one hand, it helps the users to know the details about components and functions of cloud.
- On the other hand, the cloud architecture is exposed to the attackers.

3.2.4 Identity management and access control

- A cloud needs a dynamic, fine-grained, and strict access control mechanisms to control unauthorized operations within the cloud.

- Also it needs management system to quickly update access control policies in case of newly joining or leaving.

- Weak identity management example, denial of service by account lock-out, weak credential reset mechanisms, insufficient authorization checks.

3.3. Challenges at contractual and legal levels

- Adopting the cloud computing, results in moving the organizations data and applications to the administrative control of CSP.

- This brings many issues to the front which are related to the service level agreement (SLA), legalities, and physical locations of the data.

3.3.1 Service level agreements(SLA)

- The SLA is a document that specifies the terms and conditions between the user and CSP.
- It indicates
  - minimum performance level that CSP has to provide.
  - counteractive actions.
  - consequences in case of breach of the agreement between user and CSP.
- There are many issues about conflict between user and CSP, such as monitoring, statistic report.
- It is kind of technical issues

3.3.2 Legal issues

- There are case of local difference of legal issue.

- Sometime, the data may be present in more than one location having different laws about digital security.

- Moreover, in case of a dispute the issue of jurisdiction arises as to which laws would be applicable.

3.3.2 Legal issues

- The E-discovery refers to an issue when the hardware of the CSP gets seized for investigations related to particular customer according to the laws of geographic location.

- Such a case, results in risk of privacy breach of other users.

4. Security solutions

- This section discusses various approaches proposed in the literature to counter the security issues discussed in Section 3.

- The counter measures for communication issues and architectural issues which was explained in many paper.

- Each solutions are compared and analyzed in table form.

4.1 Counter measures for communication issues

- In [21], the CSA guidelines recommend the use of a combination of virtual LANs, IDS, IPS, and firewalls to protect the data in transit.
- In [67],the authors proposed Advanced cloud protection system (ACPS), which aim at providing greater security to the cloud resources. The ACPS is divided into multiple modules located at the host platform. The interceptor module is responsible for detecting any suspicious activities at the host. The detected suspicious activities are recorded by the warning recorder module and are stored in the warning pool.[84]
- In [59], A security tool for the cloud computing, called CyberGuarder is proposed to provide virtual network security through the deployment of virtual network devices. It implemented isolation by utilizing virtual private network(VPN). CyberGuarder also provide VM security through the integrity verification of applications and by monitoring of system calls invoked by the applications.

4.1 Counter measures for communication issues

- In [116],a virtual network model that safeguards the virtual networks against sniffing and spoofing attacks is proposed. In bridge mode the hypervisor attaches the VM directly to the virtual Ethernet bridge. The bridge in turn connects to the physical network. The route mode creates a P2P link between the VM and the VM management domain. This model is divided into three layers: routing, firewall, and shared network layer.

- In [42], the author presented a cloud network security solution by implementing a novel tree-rule firewall instead of conventional list-rule firewall to increase performance and security.

4.1 Counter measures for communication issues

- Authors in [72] presented a technique named DCPortalsNg for isolation of virtual networks for various VMs. It also prevents the cross VM denial of service (DoS).

- In [120], system called SnortFlow for intrusion prevention within cloud environment is proposed. It utilizes the features of Snort and OpenFlow systems.

4.1 Counter measures for communication issues

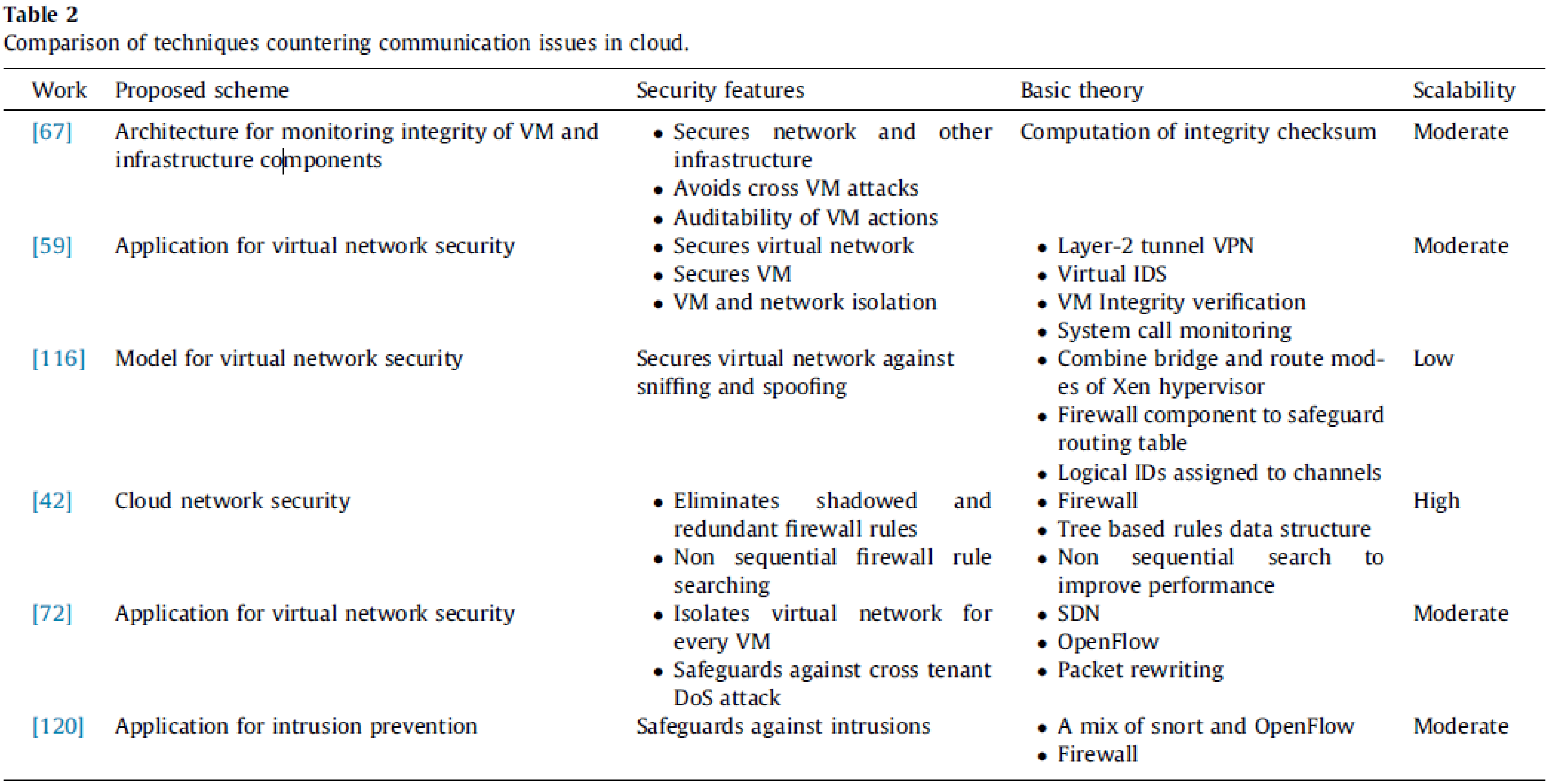


Table 2
Comparison of techniques countering communication issues in cloud.

Work	Proposed scheme	Security features	Basic theory	Scalability
[67]	Architecture for monitoring integrity of VM and infrastructure components	• Secures network and other infrastructure • Avoids cross VM attacks • Auditability of VM actions	Computation of integrity checksum	Moderate
[59]	Application for virtual network security	• Secures virtual network • Secures VM • VM and network isolation	• Layer-2 tunnel VPN • Virtual IDS • VM Integrity verification • System call monitoring	Moderate
[116]	Model for virtual network security	Secures virtual network against sniffing and spoofing	• Combine bridge and route modes of Xen hypervisor • Firewall component to safeguard routing table • Logical IDs assigned to channels	Low
[42]	Cloud network security	• Eliminates shadowed and redundant firewall rules • Non sequential firewall rule searching	• Firewall • Tree based rules data structure • Non sequential search to improve performance	High
[72]	Application for virtual network security	• Isolates virtual network for every VM • Safeguards against cross tenant DoS attack	• SDN • OpenFlow • Packet rewriting	Moderate
[120]	Application for intrusion prevention	Safeguards against intrusions	• A mix of snort and OpenFlow • Firewall	Moderate

4.2. Counter measures for architectural issues

- Measures about virtualization[21]
  - The implementers should secure each virtualized OS in each of the guest VMs.
  - Built in security measures should be adopted for virtualized OS.
  - Third party security technology should be used to cut down dependency on the CSP.
  - The VMs at rest should be encrypted.
  - Security vulnerability assessment tools should cover the virtualized environment.
  - VM images at rest should be patched with the latest fixes as soon as required. Moreover, the protection mechanism should be in place until VMs are patched.
  - Virtualization aware security tools should be implemented and used in the cloud computing environment

Virtual image security

- Wie et al. [113] proposed Mirage, an image management system for the cloud environment. It provides a fourfold security to the VM images.
- In [51], the authors proposed encrypted virtual disk images in cloud (EVDIC) that exploits encryption to secure the VM images on the disk. It uses advanced encryption standard (AES) with a key size of 256 bits.
- [90] proposed an approach that checks for the outdated software and vulnerabilities in the VM images. Two modules work in the proposed scheme : update checker and Online penetration suite(OPS)
- The ImageElves in [48] targeted at providing updated software installs, and patches for the VMs in the cloud.
- An Offline Patching Scheme (OPS-offline) is introduced in [27] to identify and rectify images with outdated software and malware vulnerabilities.

Virtual image security

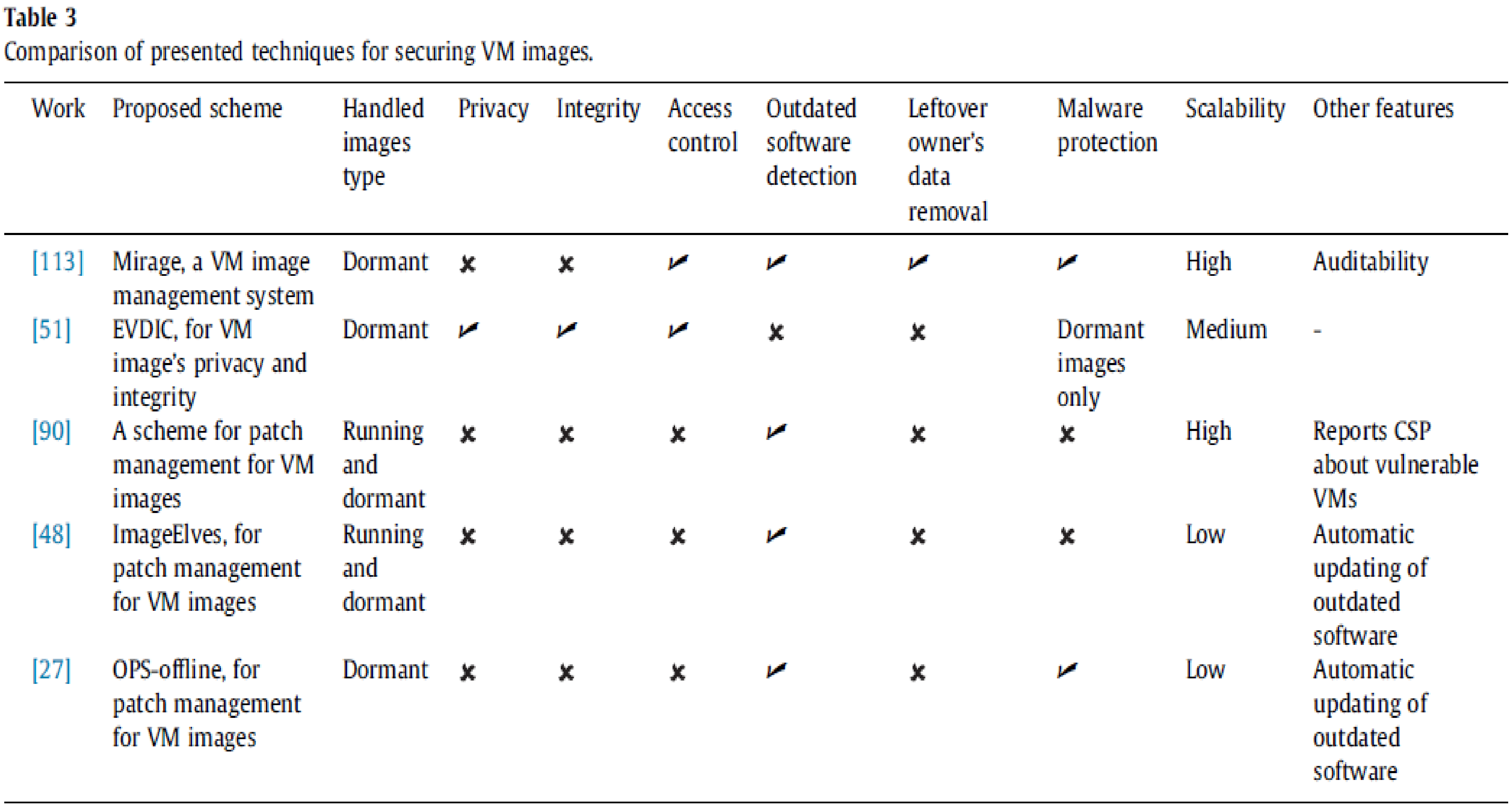
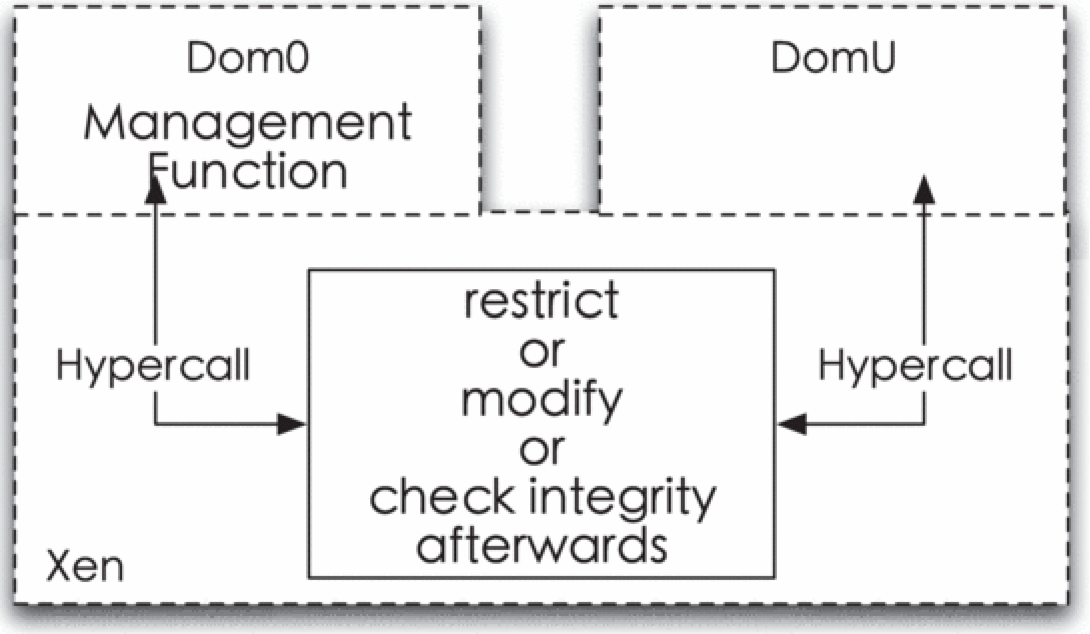


Table 3
Comparison of presented techniques for securing VM images.

Work	Proposed scheme	Handled images type	Privacy	Integrity	Access control	Outdated software detection	Leftover owner's data removal	Malware protection	Scalability	Other features
[113]	Mirage, a VM image management system	Dormant	✗	✗	✓	✓	✓	✓	High	Auditability
[51]	EVDIC, for VM image's privacy and integrity	Dormant	✓	✓	✓	✗	✗	Dormant images only	Medium	-
[90]	A scheme for patch management for VM images	Running and dormant	✗	✗	✗	✓	✗	✗	High	Reports CSP about vulnerable VMs
[48]	ImageElves, for patch management for VM images	Running and dormant	✗	✗	✗	✓	✗	✗	Low	Automatic updating of outdated software
[27]	OPS-offline, for patch management for VM images	Dormant	✗	✗	✗	✓	✗	✓	Low	Automatic updating of outdated software

VM security during execution(1)

- In [58],the architecture prohibit memory access from management domain to user domain using foreign mapping. Hypervisor is always monitoring memory access and ensures encryption of information of user domain.



VM security during execution(2)

- [129], CloudVisor is a light weight security module, intercept every control transitions between VMM and VMs. It also monitors the address translation to enforce memory isolation. The integrity is ensured by using Merkle tree, MD5 hash and Trusted Platform Module(TPM).
- [118], HyperCoffer only trusts the processor and consider everything else as the untrusted components. The Address Independent Seed Encryption (AISE) and Merkle tree are used for encryption and integrity checking. Like [129], it monitors the control transition between VMM and VMs.

VM security during execution(3)

- [46], CloudSec monitors the VMs physical memory by using VM inspection technique. After VM launching, it identifies the memory layout of the VMs hardware by inspecting the control registers of the VMs CPU. And it requests for Kernel Structure Definition through the hypervisor. It maps the physical memory to the KSD that generates the OS view of the live VM

- [31], Exterior, dual VM architecture that launches a Secure Virtual Machine (SVM) for executing a guest virtual machine (GVM). The kernel data rootkit attacks and intrusions are detected by introspection of code in the SVM.

VM security during execution(3)

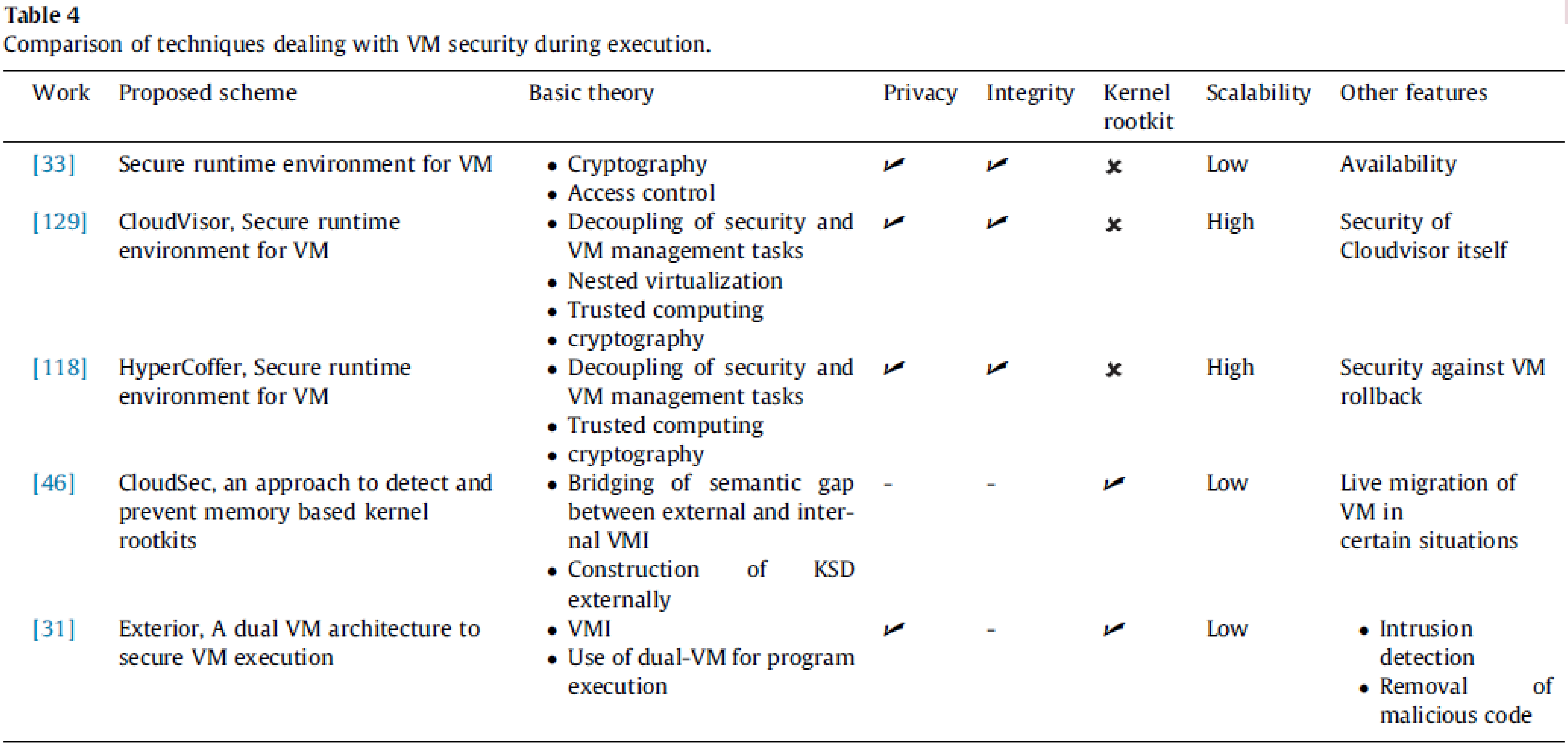


Table 4
Comparison of techniques dealing with VM security during execution.

Work	Proposed scheme	Basic theory	Privacy	Integrity	Kernel rootkit	Scalability	Other features
[33]	Secure runtime environment for VM	• Cryptography • Access control	✓	✓	✗	Low	Availability
[129]	CloudVisor, Secure runtime environment for VM	• Decoupling of security and VM management tasks • Nested virtualization • Trusted computing • cryptography	✓	✓	✗	High	Security of Cloudvisor itself
[118]	HyperCoffer, Secure runtime environment for VM	• Decoupling of security and VM management tasks • Trusted computing • cryptography	✓	✓	✗	High	Security against VM rollback
[46]	CloudSec, an approach to detect and prevent memory based kernel rootkits	• Bridging of semantic gap between external and internal VMI • Construction of KSD externally	-	-	✓	Low	Live migration of VM in certain situations
[31]	Exterior, A dual VM architecture to secure VM execution	• VMI • Use of dual-VM for program execution	✓	-	✓	Low	• Intrusion detection • Removal of malicious code

VM migration(1)

- Aslam et al.[9], presented a VM migration technique that allows migration only if the destination platform is secure up to the user defined level. A Trusted Assurance Level is introduced that specifies the trust level of the cloud platform.
- [109], the author used a Virtual TPM bound with a VM that certifies the integrity of the VM. Property based remote attestation is used to verify the integrity and security conditions of the remote host before migration.
- Authors in [22] also utilized trusted computing for secure VM-vTPM migration. The security for migration is provided by using the key hierarchy of vTPM in [22].

VM migration(2)

- [7], The authors used trusted computing is used for attestation and integrity verification of source and destination platforms. Its framework also used role based access control policies to ensure security against VM hopping and useless migrations.
- [105], the authors proposed a framework that migrate not only the VM but the security context is also migrated to the destination host. The security context manager module migrates the static security context state, followed by the migration of VM state information by the VM state migrator module. The final phase is the migration of the dynamic security context to the destination host by the security context migrator.

VM migration(3)

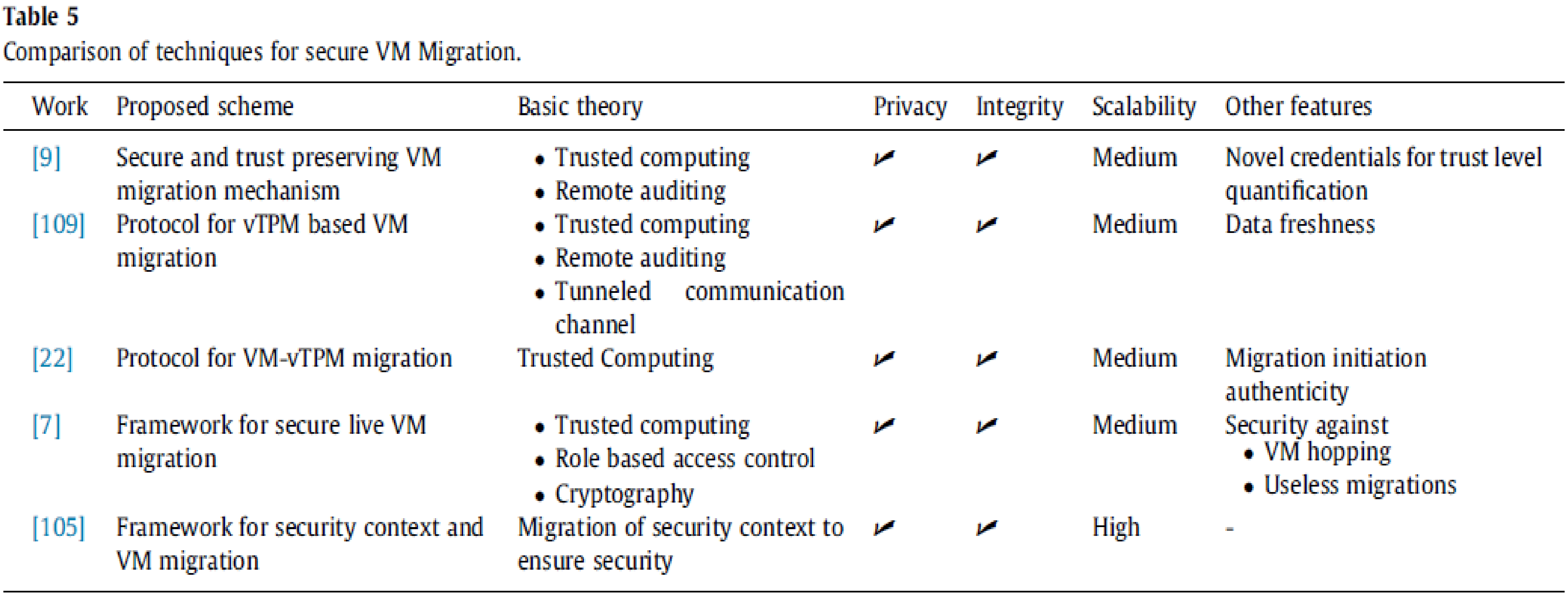


Table 5
Comparison of techniques for secure VM Migration.

Work	Proposed scheme	Basic theory	Privacy	Integrity	Scalability	Other features
[9]	Secure and trust preserving VM migration mechanism	• Trusted computing • Remote auditing	✓	✓	Medium	Novel credentials for trust level quantification
[109]	Protocol for vTPM based VM migration	• Trusted computing • Remote auditing • Tunneled communication channel	✓	✓	Medium	Data freshness
[22]	Protocol for VM-vTPM migration	Trusted Computing	✓	✓	Medium	Migration initiation authenticity
[7]	Framework for secure live VM migration	• Trusted computing • Role based access control • Cryptography	✓	✓	Medium	Security against • VM hopping • Useless migrations
[105]	Framework for security context and VM migration	Migration of security context to ensure security	✓	✓	High	-

Secure hypervisor (VMM)(1)

- Zhang et al,[130] presented HyperCheck to ensure a secure execution of the hypervisor. It is a hardware assisted framework using the CPU system management mode(SMM). Registers and network card is utilized to detect and monitor.
- [115], The authors proposed scheme divides the hypervisor into two major components. The de-privileged DeHype component, that is decoupled from the OS and is executed in the user mode. This separation make hypervisor secure at attacks.
- [111], HyperLock provides an isolated address space than the host OS and with the limited instruction set. Authors proposed hypervisor shadowing technique to further safeguard the VMs running on the host system.

Secure hypervisor (VMM)(2)

- Pan et al.[76] reduce the trusted computing base and restrict the functionality of hypervisor in root mode for securing the hypervisor and running VMs. The authors divide the functionality of hypervisor into sub modules, namely: (a) Guestvisor, non-root mode and (b)Splitvisor, which is executes in root mode and is responsible for isolating multiple Guestvisors.

- [102], NoHype is based on the following key ideas, (a) pre-allocation of the memory and cores, (b) use of virtualized I/O devices only, (c) system discovery process at the boot time of VM OS, and (d) avoiding indirections. It propose hypervisor elimination

Secure hypervisor (VMM)(3)

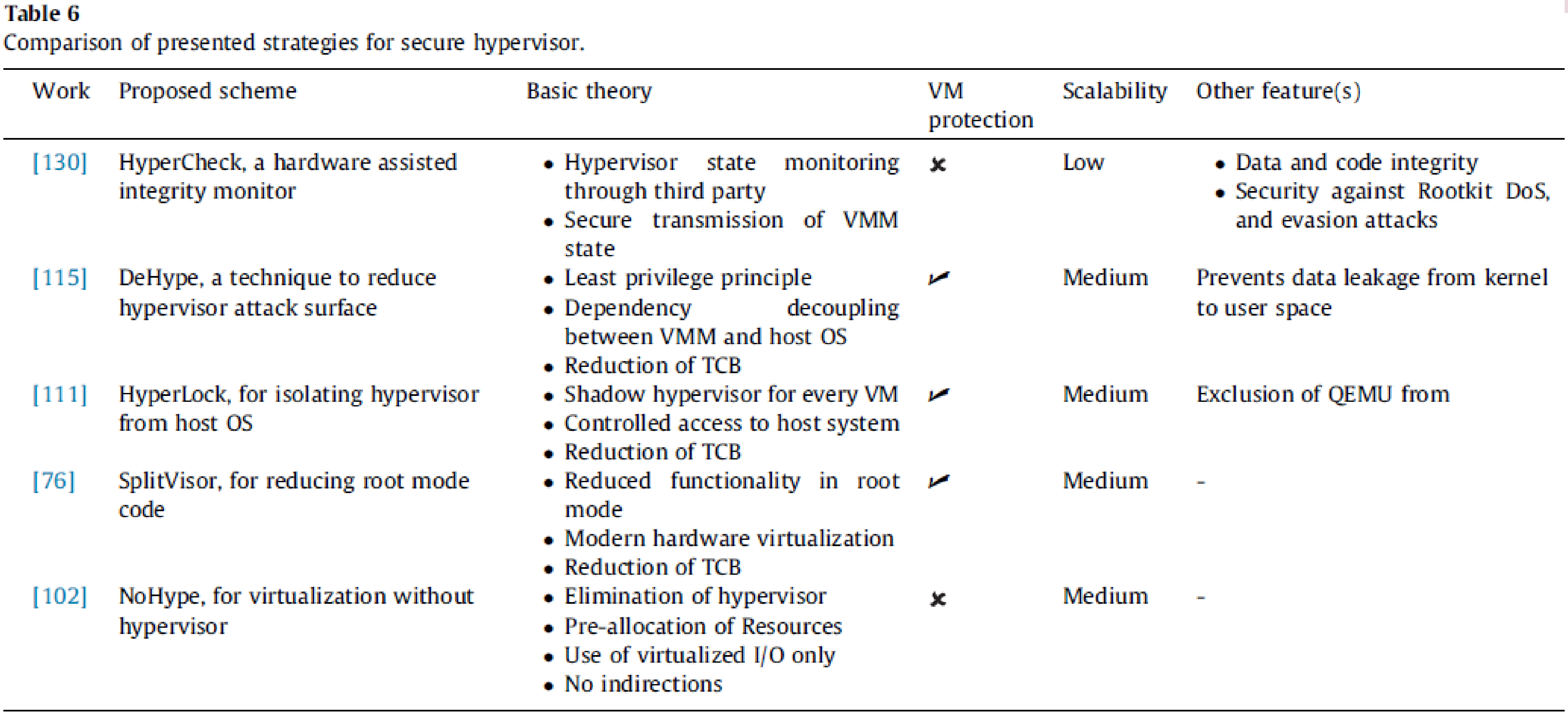


Table 6
Comparison of presented strategies for secure hypervisor.

Work	Proposed scheme	Basic theory	VM protection	Scalability	Other feature(s)
[130]	HyperCheck, a hardware assisted integrity monitor	• Hypervisor state monitoring through third party • Secure transmission of VMM state	✗	Low	• Data and code integrity • Security against Rootkit DoS, and evasion attacks
[115]	DeHype, a technique to reduce hypervisor attack surface	• Least privilege principle • Dependency decoupling between VMM and host OS • Reduction of TCB	✓	Medium	Prevents data leakage from kernel to user space
[111]	HyperLock, for isolating hypervisor from host OS	• Shadow hypervisor for every VM • Controlled access to host system • Reduction of TCB	✓	Medium	Exclusion of QEMU from
[76]	SplitVisor, for reducing root mode code	• Reduced functionality in root mode • Modern hardware virtualization • Reduction of TCB	✓	Medium	-
[102]	NoHype, for virtualization without hypervisor	• Elimination of hypervisor • Pre-allocation of Resources • Use of virtualized I/O only • No indirections	✗	Medium	-

4.2. Counter measures for architectural issues

- Data/storage security solution’s recommendations [21]
  - The key management should be performed by either the organizations/users themselves or by a trusted cryptographic service from a credible source.
  - The best practices regarding the key management and encryption products from reliable sources should be used.
  - It is recommended to use off-the-shelf-technology where possible.
  - The key scope should be maintained at the individual or group level.
  - The use of standard algorithms is recommended and proprietary encryption algorithms are discouraged.

Cloud data/storage security(1)

- [114] SecCloud secures the user data in cloud and computations performed on that. It use bilinear Deffie Hellman for key management. The computational security is ensured about partial computation and use of invalid data. It also using Merkle tree to get more security.
- [98], The data is encrypted with 128-bit SSL encryption and MAC is appended afterwards. Based on the Sensitivity Rating(SR value), user`s security requirement rating. the data is allotted space in one of the three proposed partitions in the cloud. The proposed partitions are public, private. The data and index are sent to the cloud where they are stored depending on the SR value.

Cloud data/storage security(2)

- [110], authors proposed methodology conducting the verification of the cloud data correctness without explicit knowledge of the whole data. The erasure correcting code and homomorphic tokens are used for the aforesaid purpose. Also, the proposed scheme performs error localization by detecting misbehaving server.
- [103], The File Assured Deletion (FADE) is light weight protocol use both sym-asym encryption. It works with a group of key managers(KM) that act as a trusted 3rd party. The data key is used to encrypt file of client, and another key is used to encrypt data key. it is using Shamirs scheme and RSA to manage key.

Cloud data/storage security(2)

- Liu et al, [64] proposed TimePRE, a time based proxy re-encryption combined with Attribute Based Encryption (ABE) to support secure data sharing with fine grained access control. Unlike other proxy re-encryption schemes, it does not require the data owner to be online for user revocation and generation of new re-encryption keys. The access control is ensured by use of ABE that identifies user by set of attributes rather than identity.

Cloud data/storage security

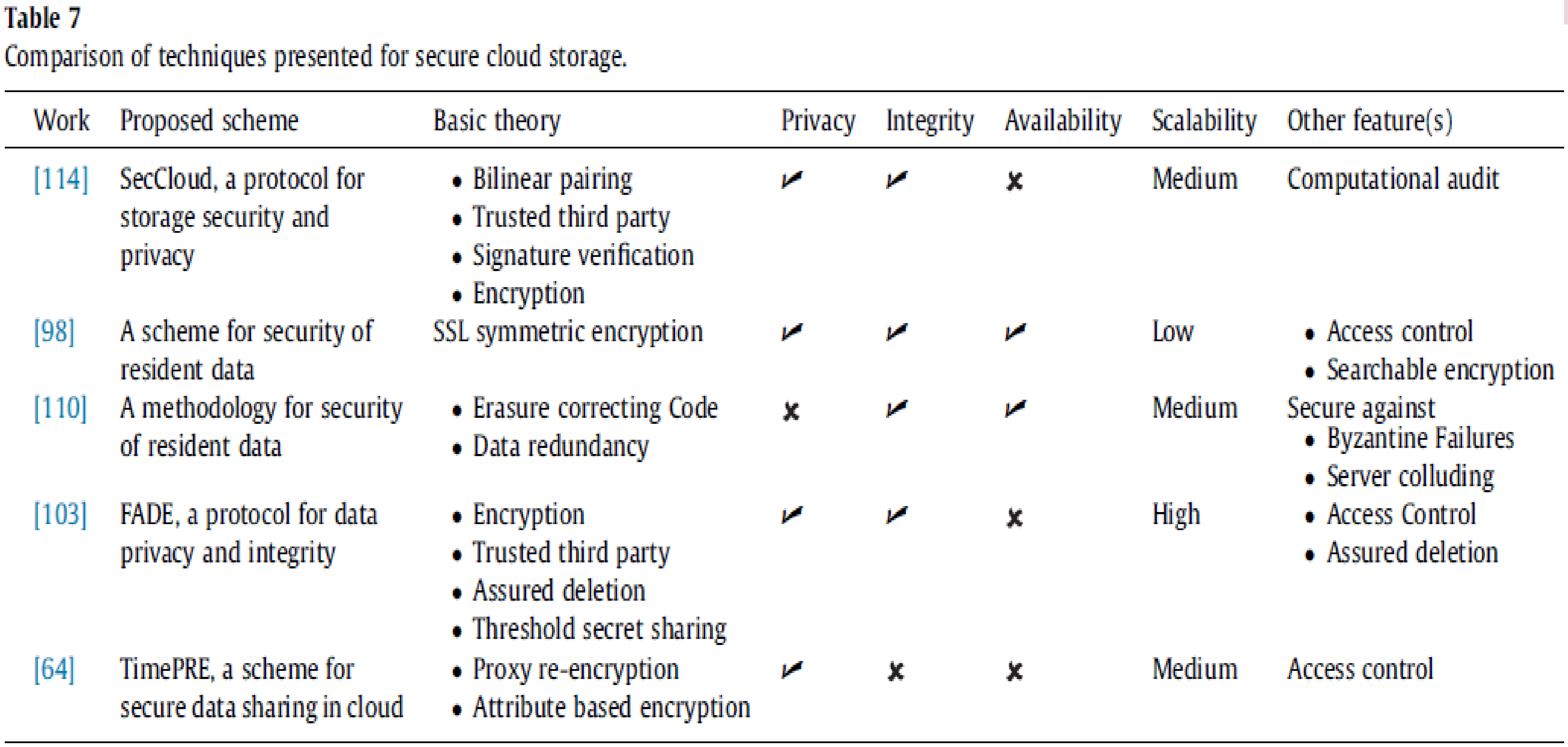


Table 7
Comparison of techniques presented for secure cloud storage.

Work	Proposed scheme	Basic theory	Privacy	Integrity	Availability	Scalability	Other feature(s)
[114]	SecCloud, a protocol for storage security and privacy	• Bilinear pairing • Trusted third party • Signature verification • Encryption	✓	✓	✗	Medium	Computational audit
[98]	A scheme for security of resident data	SSL symmetric encryption	✓	✓	✓	Low	• Access control • Searchable encryption
[110]	A methodology for security of resident data	• Erasure correcting Code • Data redundancy	✗	✓	✓	Medium	Secure against • Byzantine Failures • Server colluding
[103]	FADE, a protocol for data privacy and integrity	• Encryption • Trusted third party • Assured deletion • Threshold secret sharing	✓	✓	✗	High	• Access Control • Assured deletion
[64]	TimePRE, a scheme for secure data sharing in cloud	• Proxy re-encryption • Attribute based encryption	✓	✗	✗	Medium	Access control

Security solutions for cloud applications and APIs

- Cloud applications and APIs recommendations[21]
  - Security and privacy requirements should be defined in accordance to the needs of the cloud development and deployment. The defined requirements should also be in the order based on the impact and possibility.
  - The risks and attack vectors specific to the cloud computing must be explored and assimilated into the security requirements. The risk models and attack models should be continuously built and maintained.
  - The secure software development life cycle and software architecture should be developed and maintained.
  - The re-useable software components that are known to alleviate the known security and breach scenarios should be used.
  - Regular penetration testing for web applications should be carried out.
  - Manual tests must be carried out periodically to ensure secure session management of web applications.

Security solutions for cloud applications and APIs

- [91], author proposed the use of Diameter-AAA protocol. It employs network based access control to filter the illegal access request to the cloud applications.
- [6], authors proposed the use of TPM and ECC to provide a secure platform for application execution in the cloud.
- [45], authors proposed the provision of Security as a Service (SECaaS) in cloud, provided by different clouds, and in dependent cloud, which works in all levels.
- [117], proposed an API management platform for the cloud, with Open Authorization which is token based access control mechanism. The consumer calls the API by using the token signed with its private key. The
- provider sends the token to the API management platform for validation. If valid, the access is granted to the consumer.

Security solutions for cloud applications and APIs

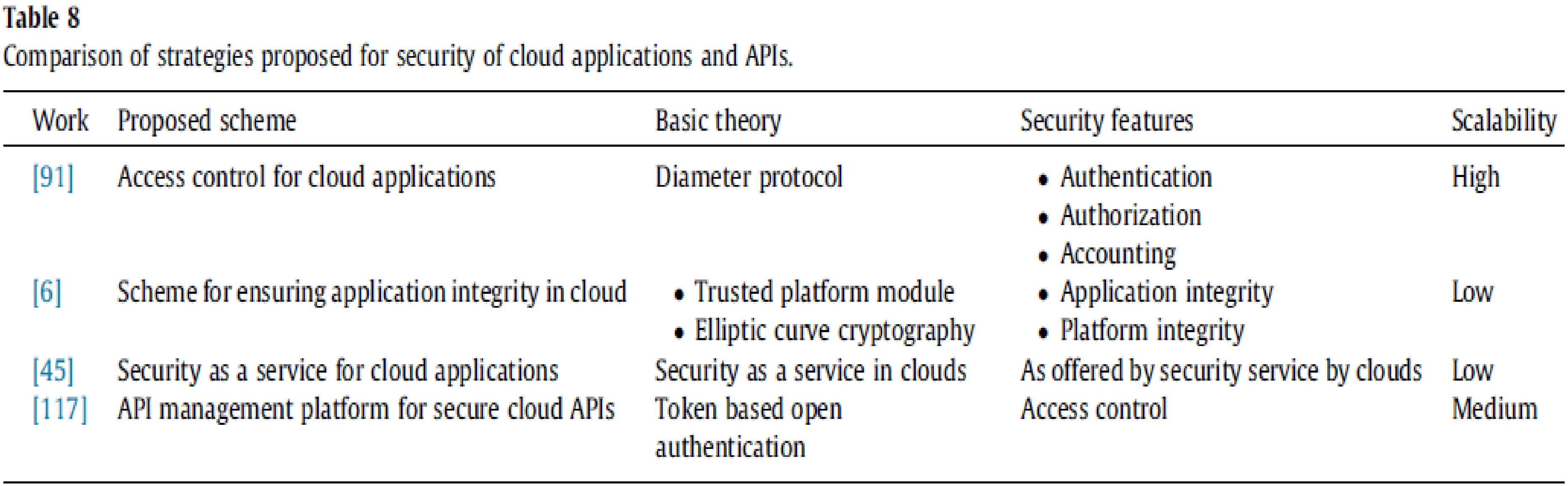


Table 8
Comparison of strategies proposed for security of cloud applications and APIs.

Work	Proposed scheme	Basic theory	Security features	Scalability
[91]	Access control for cloud applications	Diameter protocol	• Authentication • Authorization • Accounting	High
[6]	Scheme for ensuring application integrity in cloud	• Trusted platform module • Elliptic curve cryptography	• Application integrity • Platform integrity	Low
[45]	Security as a service for cloud applications	Security as a service in clouds	As offered by security service by clouds	Low
[117]	API management platform for secure cloud APIs	Token based open authentication	Access control	Medium

4.2. Counter measures for architectural issues

- Identity management and access control requirement
  - Open standard federations, for example, SAML and OAuth, should be preferred if possible.
  - The source of the attributes should be as close to master source as possible.
  - The attributes should be validated at master source or as close as possible.
  - All characteristics of the entities should have an identified trust level.
  - Bi-directional trust should be ensured for secure relationship and transactions.
  - The services should have import/export function into standards such as XACML and OASIS.

Identity management and access control

- [108], authors extended Attribute Set Based Encryption (ASBE) to present Hierarchical ASBE that utilize hierarchical user structure. In HASBE, Root authority is trusted by the domain level, and domain is trusted by subdomain level authorities or users. The access control is also defined as a hierarchical tree structure.

- [86], author proposed use of ABE and the Attribute Based Signature (ABS) for access control and anonymous authentication.

- [122], Role Based Multi-tenancy Access Control (RB-MTAC) scheme that combines identity management and role based access control. The scheme requires the users to register with the cloud and obtain unique ID and password. And user is directed to the role assignment module that connects to the DB and assign roles based on information.

Identity management and access control

- [19], Simple Privacy-preserving Identity-Management for Cloud Environment (SPICE). It exploits the concept of group signature and randomization for providing the anonymous authentication, delegatable authentication, unlinkability, accountability, and user centric access control.

- [23], an identity management framework for the cloud networking infrastructure that is centered on User Managed Access (UMA) protocol. The infrastructure in the proposed scheme is seen as the Authorization Manager (AM). The service and users identities are managed by AM.

Identity management and access control

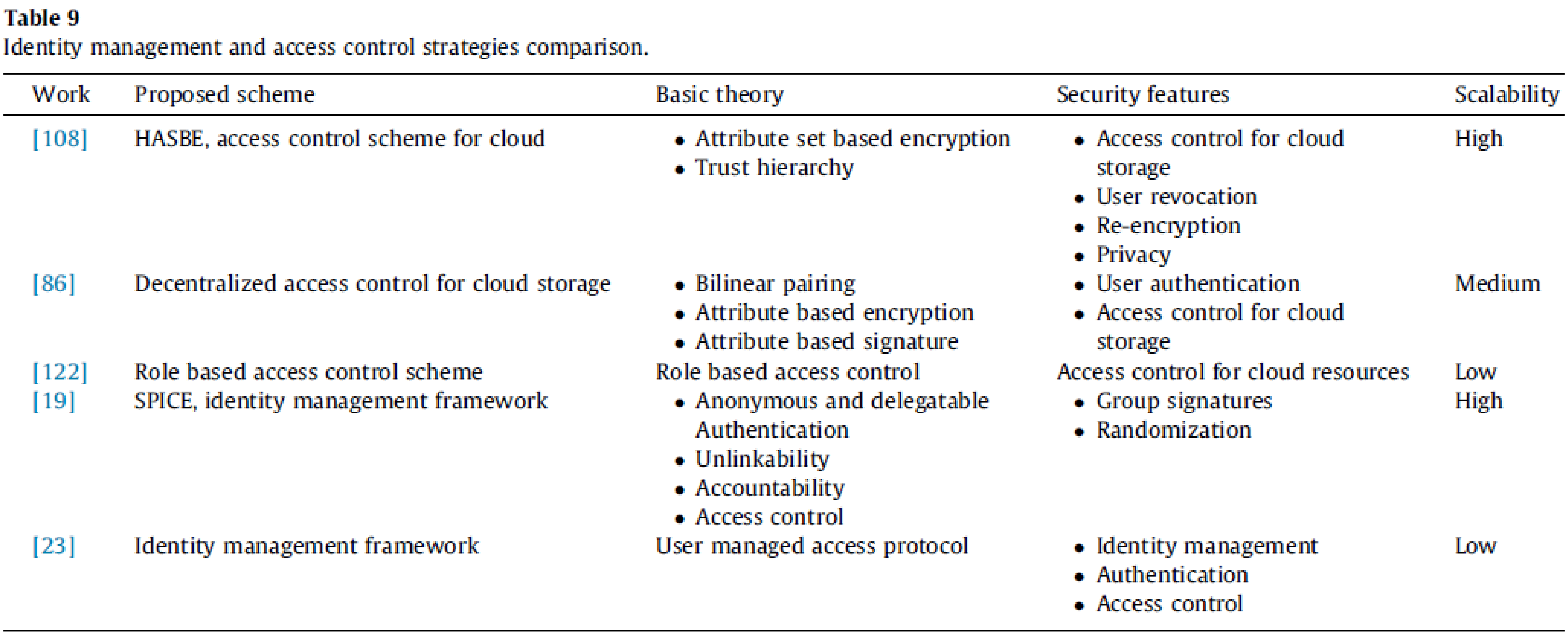


Table 9
Identity management and access control strategies comparison.

Work	Proposed scheme	Basic theory	Security features	Scalability
[108]	HASBE, access control scheme for cloud	• Attribute set based encryption • Trust hierarchy	• Access control for cloud storage • User revocation • Re-encryption • Privacy	High
[86]	Decentralized access control for cloud storage	• Bilinear pairing • Attribute based encryption • Attribute based signature	• User authentication • Access control for cloud storage	Medium
[122]	Role based access control scheme	Role based access control	Access control for cloud resources	Low
[19]	SPICE, identity management framework	• Anonymous and delegatable Authentication • Unlinkability • Accountability • Access control	• Group signatures • Randomization	High
[23]	Identity management framework	User managed access protocol	• Identity management • Authentication • Access control	Low

Contractual and legal issues

- [36], SecAgreement that articulates the security parameters and services for provision in the SLA. It extends the template of the wel service agreement to incorporate seciriry constraints and metrics into the terms of SLA.
- [37], a methd react to the SLA violations or service cancelation to reduce the security risk
- [79], SPECS, SLA-based approach to security as a service. It divede the SLA life cycle in three stage, (a) negotiation, (b) enforcement, and (c) monitoring.
- [38], A solution for embedding security controls in cloud SLA, it is concentrating on vocabulary of SLA, with XML schema. The vocabulary allows the organizations to compare different secure services.

Contractual and legal issues

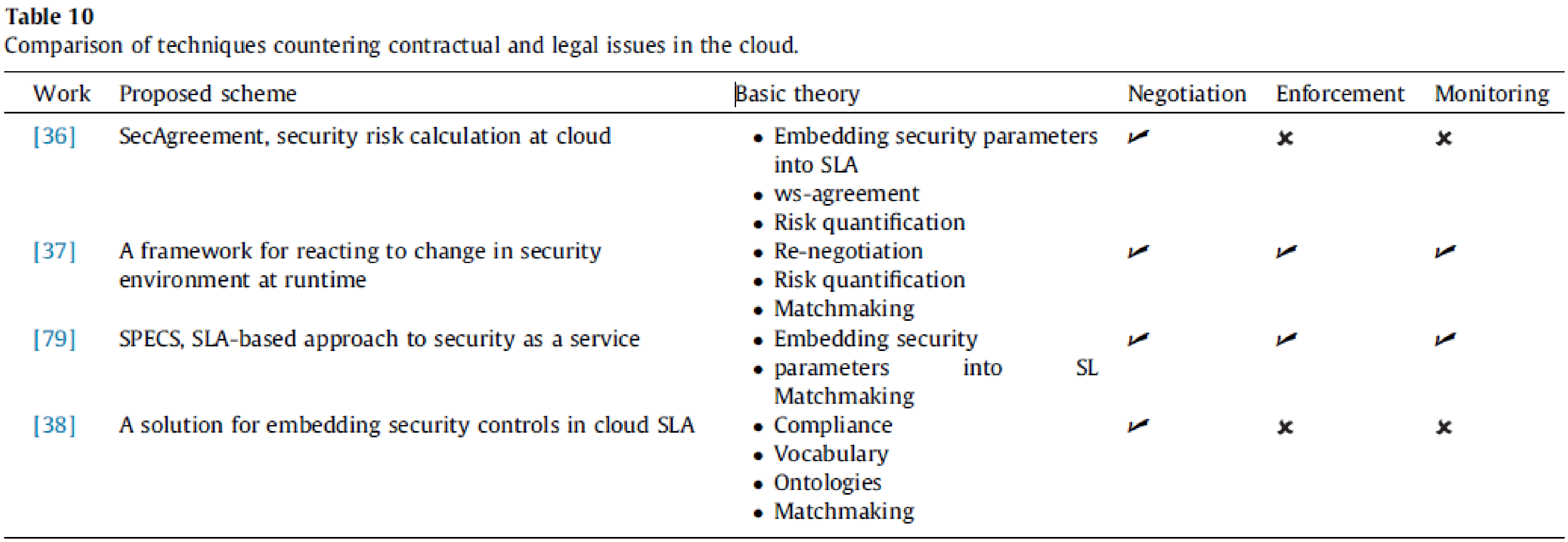


Table 10
Comparison of techniques countering contractual and legal issues in the cloud.

Work	Proposed scheme	Basic theory	Negotiation	Enforcement	Monitoring
[36]	SecAgreement, security risk calculation at cloud	• Embedding security parameters into SLA • ws-agreement • Risk quantification	✓	✗	✗
[37]	A framework for reacting to change in security environment at runtime	• Re-negotiation • Risk quantification • Matchmaking	✓	✓	✓
[79]	SPECS, SLA-based approach to security as a service	• Embedding security • parameters into SL Matchmaking	✓	✓	✓
[38]	A solution for embedding security controls in cloud SLA	• Compliance • Vocabulary • Ontologies • Matchmaking	✓	✗	✗

5. Security issues in MCC(1/3)

- Mobile cloud computing inherit security issues that aforementioned.
- However, MCC has constraint about resources such as low processing power, less storage capacity, limited energy, and capricious internet connectivity.
- These make interruptions to adapt cloud computing security solution in MCC.

5. Security issues in MCC(2/3)

- Mobile application security
  - The traditional security software like antivirus and IDS are not possible to run continuously on the mobile device.
  - The basic concept of offloading computation can also be used to run heavy security programs on mobile.
- User privacy
  - The mobile device can be the source of user location leakage especially due to location based services
  - The concept of location cloaking can be used to preserve user location privacy by concealing the user exact geographic position

5. Security issues in MCC(3/3)

- Authentication
  - Dynamic credential generation can be used for secure authentication. The credential generation can be offloaded to a trusted third party due to low processing power of the mobile device.
- Data security
  - Computation intensive encryption algorithms with large keys are not feasible to be run at the mobile device.
  - The compute intensive tasks of encryption / decryption can be moved to trusted third party for securing the user data.

6. Discussion and open issues

- The cloud not only retains the orthodox security concerns but also entails the novel issues arising due to the use of new technologies and practices.
  - Such as shared pool of resources, multi tenancy, agreement and legal issues.
  - But also integrity, confidentiality, authority, privacy show critical issues.
- The first and the foremost need is to develop a comprehensive and integrated security solution that includes most of the major security requirements in the cloud environment.
- there is a need to find security solutions that create a balance between the security requirements and performance to overcome constraints.

7. Conclusions

- There was many conventional security issues for, and cloud computing`s own specific issues based on different system.
- Understanding the security threats and counter measures will help organizations to carry out the cost benefit analysis and will urge them to shift to the cloud.
- Tabulated analysis will greatly help the readers to compare and analyze the pros and cons of the research endeavors.
- This survey presented the security issues that arise due to the shared, virtualized, and public nature of the cloud computing paradigm.