Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.044304

ARTICLE

# Performance Comparison of Hyper-V and KVM for Cryptographic Tasks in Cloud Computing

**Nader Abdel Karim[1,*], Osama A. Khashan[2,*], Waleed K. Abdulraheem[3], Moutaz Alazab[1], Hasan Kanaker[4], Mahmoud E. Farfoura[5] and Mohammad Alshinwan[5,6]**

[1]Department of Intelligent Systems, Faculty of Artificial Intelligence, Al-Balqa Applied University, Al-Salt, 1705, Jordan

[2]Research and Innovation Centers, Rabdan Academy, P.O. Box 114646, Abu Dhabi, United Arab Emirates

[3]Department of Information Systems and Networks, The World Islamic Sciences and Education University, Amman, 11947, Jordan

[4]Department of Cyber Security, Isra University, Amman, 1162, Jordan

[5]Faculty of Science and Information Technology, Al-Zaytoonah University of Jordan, Amman, 11733, Jordan

[6]Middle East University Research Unit, Middle East University, Amman, 11831, Jordan

*Corresponding Authors: Nader Abdel Karim. Email: nader.salameh@bau.edu.jo; Osama A. Khashan. Email: okhashan@ra.ac.ae

Received: 27 July 2023 Accepted: 15 November 2023 Published: 27 February 2024

## ABSTRACT

As the extensive use of cloud computing raises questions about the security of any personal data stored there, cryptography is being used more frequently as a security tool to protect data confidentiality and privacy in the cloud environment. A hypervisor is a virtualization software used in cloud hosting to divide and allocate resources on various pieces of hardware. The choice of hypervisor can significantly impact the performance of cryptographic operations in the cloud environment. An important issue that must be carefully examined is that no hypervisor is completely superior in terms of performance; Each hypervisor should be examined to meet specific needs. The main objective of this study is to provide accurate results to compare the performance of Hyper-V and Kernel-based Virtual Machine (KVM) while implementing different cryptographic algorithms to guide cloud service providers and end users in choosing the most suitable hypervisor for their cryptographic needs. This study evaluated the efficiency of two hypervisors, Hyper-V and KVM, in implementing six cryptographic algorithms: Rivest, Shamir, Adleman (RSA), Advanced Encryption Standard (AES), Triple Data Encryption Standard (TripleDES), Carlisle Adams and Stafford Tavares (CAST-128), BLOWFISH, and TwoFish. The study's findings show that KVM outperforms Hyper-V, with 12.2% less Central Processing Unit (CPU) use and 12.95% less time overall for encryption and decryption operations with various file sizes. The study's findings emphasize how crucial it is to pick a hypervisor that is appropriate for cryptographic needs in a cloud environment, which could assist both cloud service providers and end users. Future research may focus more on how various hypervisors perform while handling cryptographic workloads.

## KEYWORDS

Cloud computing; performance; virtualization; hypervisors; Hyper-V; KVM; cryptographic algorithm

## 1 Introduction

Authors are required to adhere to this Microsoft Word template in preparing their manuscripts for submission. It will speed up the review and typesetting process. In recent years, various sectors have adopted cloud computing, making it more and more common. These sectors include governments, financial markets, businesses, and industries. This is primarily because cloud computing offers cost-effective and scalable solutions for storing, handling, and administering data. It also allows collaboration and remote access to resources from anywhere. The growing number of smartphone devices, the Internet of Things, and big data analytics have raised the need for cloud computing to process and manage enormous amounts of data in a timely and efficient manner. Cloud computing provides an affordable solution for companies and individuals with varying computing needs by enabling remote computing devices to collaborate on data processing tasks [1].

Cloud computing is thoroughly described by the National Institute of Standards and Technology (NIST), including key features, service models, and deployment options. According to [2], cloud computing is a model that allows access to a shared pool of reconfigurable computing resources from anywhere and at any time that is most convenient for you. With the idea of cloud computing, users and companies have access to a model that makes it easier to provision and release a variety of resources, including networks, servers, storage, applications, and services, without putting a lot of management work into it or requiring direct contact with service providers. This approach offers several advantages, including the ability to quickly scale up or down the number of resources and a pay-per-use model that is effective and affordable [3,4]. The most notable characteristics of cloud computing include on-demand self-service, widespread network access, resource pooling, quick elasticity, and measured service. These features all contribute to the scalability, effectiveness, and cost-effectiveness of cloud computing. Additionally, the NIST lists private, public, community, and hybrid clouds as the top four cloud computing deployment options [3,5]. Private clouds are only available to one company, whereas many companies share public, community, and hybrid clouds with similar goals. Users can access cloud computing resources in a way that satisfies their preferences, needs, and requirements due to the numerous service models and deployment options available.

Cloud computing has developed to the point where it is an essential component of the computing infrastructure. Numerous advantages, including adaptability, affordability, and flexibility, come with cloud computing. With over 90% of global enterprises using cloud computing in some form, these advantages have helped to accelerate its adoption [6]. A survey conducted in 2020 found that 83% of business applications were hosted in the cloud, with 41% of enterprise workloads employing public cloud platforms [7]. In addition, there are 7.5 million active internet users every second, 3.5 million active smartphone users every second, and more than 2 billion mobile game players who save their data in the cloud [8].

Governments have also been quick to adopt cloud computing [9]. The United States federal government is making significant efforts to increase cloud computing adoption through policies and programs such as the Cloud Smart plan, which aims to accelerate the transition to cloud computing across all government agencies [10]. Significant advancements in cloud computing usage have also been undertaken by major countries such as the United Kingdom, Australia, New Zealand, and Canada [9]. Governments using cloud computing are expected to stimulate innovation and enhance the quality of services supplied to citizens.

Virtualization is a fundamental concept in cloud computing, Virtualization is creating a virtual version of something at the same abstraction level, including virtual computer hardware platforms,

storage devices, and computer network resources. It allows for more efficient utilization of physical computer hardware and is the foundation of cloud computing [11,12].

Virtualization is critical to cloud computing since it enhances workloads by making traditional computing more efficient, flexible, and cost-effective [5]. Cloud computing virtualization implementations include virtual servers, hardware virtualization, and operating system virtualization [13]. To reap the full advantages of virtualization, system administrators must select the best hypervisor for their organization's needs among various commercial and open-source alternatives based on diverse underlying technologies. This selection procedure should consider several critical variables: performance, features, and cost. For instance, Amazon Web Services virtualizes its Elastic Compute Cloud (EC2) machines using the XEN hypervisor platform. In contrast, Microsoft Azure uses the Hyper-V hypervisor platform for its Infrastructure as a Service (IaaS) cloud. Google's recent entry into the IaaS cloud market is based on the KVM hypervisor platform. Multiple hypervisors' availability enables customers to select the one that best meets their organization's needs while using its services [14].

Hypervisor performance plays a crucial role in cloud computing since it has a vital effect on the performance of the running virtual machines (VMs) [15,16]. It acts as a bottleneck affecting performance in the cloud computing environment [17]. Hence, Numerous studies have been conducted to investigate the impact of hypervisor performance on VMs. Regarding architecture, Kernel-based Virtual Machine (KVM) is better than Hyper-V regarding VMs performance, such as Central Processing Unit (CPU), memory, disk, and network, since KVM runs as a Linux kernel, so it gets the full capabilities of the hardware infrastructure. In addition, KVM is open-source, and its open-source nature allows the whole community to improve the product regarding software security and performance [18]. KVM is supported by Linux vendors such as RedHat and the open-source community [19]. At the same time, Hyper-V is a Windows-based kernel that requires more abstraction layers which reduces the overall performance [18–20]. The authors in [19,21] compared the performance of different hypervisors such as KVM, Hyper-V, Xen, and vSphere. They found that no hypervisor is superior in terms of performance, and each hypervisor should be examined to meet a particular need. Moreover, some studies show that performance for VMs, while deploying Hyper-V is better than KVM in some processes, such as in [22–24]. Studies like [25,26] compare KVM and Hyper-V hypervisors (see Table 1). Comparing the performance of the VMs processes between KVM and Hyper-V, especially in the virtualization performance, is related to CPU, time, network, and memory as in [18,24].

**Table 1:** Comparison between KVM and Hyper-V

| | KVM | Hyper-V |
|---|---|---|
| Version and base OS | Linux (+QEMU) | Windows server |
| Architecture | Bare-Metal; Full, Para and H/W–Assisted virtualization | Bare-Metal; Full, Para and H/W–Assisted virtualization |
| CPU and memory features | Linux schedulers (fair queuing scheduler, round-robin, fair queuing, proportionally) | Scheduling control with VMs reservation, VMs limit, and relative weigh |
| License | Open-source | Commercial |
| High availability | Yes | Yes |

(Continued)

**Table 1 (continued)**

| | KVM | Hyper-V |
|---|---|---|
| Virtual CPUs per VM | 64 | 64 |
| Memory per VM | 2 TB | 1 TB |
| Maximum VMs | 4000 | 4000 |
| Active VMs per Host | 512 | Unlimited |

Businesses that utilize cloud computing services must implement privacy and security protocols as an essential requirement [27,28]. As a result of an increasing amount of cyberattacks and data breaches, security is a vital part of cloud usage and acceptance for both cloud service providers and customers [29]. Cloud computing provides a dependable and practical multipurpose solution that allows businesses to access, store, and manage data from anywhere, anytime, using any device. However, the advantages of cloud computing are vulnerable to being attacked by the dangers posed by hacking attempts, which can include unauthorized access, the loss of data, and the compromise of security systems. Therefore, cloud security measures such as encryption, authentication, and access control are vital for maintaining the confidentiality, integrity, and availability of sensitive data and services [24,30–32].

Cryptography is one of the oldest and most widely used methods for protecting sensitive digital data in computers, and cloud computing environments. In cloud environments, where data is transmitted and stored across multiple servers and networks, cryptography is essential in securing the data against unauthorized access, tampering, or theft [33]. Employing various cryptographic technologies, including symmetric and asymmetric encryption, aids in maintaining data confidentiality, integrity, and authenticity and can be used to lower the danger of data breaches and cybercrimes. Additional security measures such as access control, monitoring, and audit trails are also necessary to maintain cloud computing. While Hyper-V and KVM are considered two of the most used hypervisors, this research examined the capabilities of the Hyper-V and KVM hypervisors while adopting six different cryptographic algorithms in this research. Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), Triple Data Encryption Algorithm (TripleDES), Carlisle Adams and Stafford Tavares (CAST-128), BLOWFISH, and TwoFish are among these algorithms. Martin et al. [34] presented comparisons between these six popular algorithms as shown in Table 2.

**Table 2:** Comparison of six common cryptographic algorithms

| Algorithm | Type | Key size | Speed | Security |
|---|---|---|---|---|
| RSA | Asymmetric | 1024–4096 | Slow | High |
| AES | Symmetric | 128, 192, or 256 | Fast | High |
| TripleDES | Symmetric | 128, 192, or 256 | Medium | Good |
| CAST-128 | Symmetric | 128 | Medium | Good |
| BlowFish | Symmetric | 128, 192, or 256 | Fast | Good |
| TwoFish | Symmetric | 128, 192, or 256 | Medium | Good |

In this research, the main objective is to assess the above algorithms' performance in terms of cloud security and establish how effectively they work. Furthermore, the study aims to resolve the debate on which hypervisor performs better for VMs, KVM, or Hyper-V.

This study is expected to provide the following contributions:

- Examine the performance of the two most prominent hypervisors, KVM as an open-source and Hyper-V, when using six cryptographic algorithms.
- Compare CPU usage and the time required for encryption and decryption methods with different key sizes, data sizes, and core counts.
- Add substantial new information to virtualization by evaluating the impact of cryptographic algorithms on KVM and Hyper-V's overall performance (CPU and Time).
- Present advice for identifying the best hypervisor and cryptographic method for specific use scenarios based on performance measurements.

The subsequent sections of this manuscript are organized as follows: Section 2 offers related works; Section 3 demonstrates the evaluation method; Section 4 presents the results and discussion. Finally, the conclusion with some future recommendations is presented in Section 5.

## 2 Related Works

This section of the research summarizes previous studies that examined diverse types of hypervisors, especially KVM and Hyper-V, and their impact on improving the performance of VMs in the cloud environment. Moreover, studies exploring ways to enhance cloud computing security were reviewed. Additionally, this section explored the latest encryption techniques used in cloud computing, as encryption plays a vital role in protecting cloud computing.

Regarding the studies that dealt with hypervisors, authors [24] compared two hypervisors, Xen and Hyper-V, in terms of the performance of the VMs while using eight different cryptosystems. He found that Xen is better than Hyper-V regarding CPU and time response in most processes, while Hyper-V is better in some results and algorithms. di Pietro et al. [35] analyzed the advantages and drawbacks of using virtualization technologies, including Xen, KVM, VMWare ESX, Hyper-V, and VirtualBox in cloud environments. The authors discussed the benefits of virtualization technology, including better resource use, flexibility, scalability, and potential security issues. Studies [15] investigated the performance of the hypervisor. They stated that it plays an essential role in cloud computing since it has a vital effect on the performance of the running VMs. Several studies [18] that dealt with hypervisor performance within cloud environments specifically, KVM and Hyper-V, and their distinctive characteristics are already discussed in the introduction section.

The existing literature proposed various defense methodologies, such as encryption, access control, and data obfuscation, to protect sensitive data from unauthorized access and potential threats to improve the security and privacy of cloud-based data storage and processing. Multiple studies have offered innovative approaches, including homomorphic encryption, attribute-based encryption, and secure multi-party computing. Thabit et al. [36] investigated the security and performance features of a unique lightweight cryptographic algorithm for cloud computing. The findings showed that the suggested method outperforms standard cryptographic algorithms and provides adequate protection against various security risks. Bhandari et al. [37] proposed a model approach for creating a cloud-based client relationship management (CRM) service employing independent encryption and decryption procedures using the Blowfish algorithm to improve the security and privacy of client

data. The study's findings indicated that the suggested strategy considerably decreases the risks of data breaches and illegal access, resulting in a safe and dependable CRM solution for enterprises.

The healthcare sector has great hope for the future of cloud computing in terms of improving the standard and effectiveness of healthcare services. Cloud computing can assist healthcare organizations in streamlining their operations, reducing expenses, and improving patient outcomes by facilitating simple access to medical data and fostering collaboration among healthcare providers. However, implementing resilient regulatory and governance frameworks that protect patient information privacy, confidentiality, and security is necessary to successfully integrate cloud computing in healthcare. In this regard, various access control and encryption schemes have been proposed to enhance the security and privacy of patient data in healthcare clouds. Chinnasamy et al. [38] proposed a novel access control scheme that combines hybrid cryptographic techniques with attribute-based access control to secure the retrieval of electronic health records in healthcare clouds. On the other hand, Dwivedi et al. [39] proposed a secure healthcare monitoring sensor cloud system that utilizes attribute-based elliptical curve cryptography for data protection. Both proposed schemes exhibit better performance than existing techniques, and their adoption is recommended for enhancing data security and privacy in healthcare cloud systems.

Other studies have focused on key management systems in cloud cryptography. Vinothkumar et al. [40] employed a systematic literature review methodology to analyze the current state-of-the-art in the field of cryptography and key management-based security in cloud computing to support cloud cryptography client and key management service interoperability. Their results highlight the importance of key management protocols, encryption algorithms, and the need for secure key storage mechanisms to ensure data confidentiality and integrity in cloud computing environments.

Several studies have also suggested hybrid cryptographic solutions to the security issues with cloud computing. A method for improving data protection in cloud computing was put forth by Suresha et al. [41] using key derivation. This cryptographic technique creates three secret keys from a single master key, each used for a particular purpose. To protect the confidentiality and integrity of their data, the authors advise organizations to adopt key derivation techniques as part of their cloud computing security strategy. To preserve users' privacy and security in the cloud, Orobosade et al. [42] examined the effectiveness of hybrid encryption by implementing symmetric and asymmetric cryptography techniques using elliptic curve cryptography and AES. According to their research, hybrid encryption can improve the confidentiality and integrity of cloud-based applications, hence enhancing security.

A research study on enhancing cloud data security with hybrid encryption and steganography techniques was published by Abbas et al. [43]. The authors in this research combined the AES symmetric encryption algorithm and the RSA asymmetric encryption algorithm to create hybrid encryption. The encrypted data was then embedded in an image using the LSB technique, and the data's authenticity was verified using the SHA hashing method. Before hiding the data in the image, they suggested compressing it using the LZW method. They also suggested employing a hybrid approach in cloud-based systems to increase the security of sensitive data. To evaluate the effectiveness of cryptographic and hybrid security measures for cloud computing systems, Chaudhary et al. [44] suggested a thorough methodology. The study provides in-depth information and findings demonstrating how hybrid solutions offer more security than cryptography. By demonstrating the effectiveness of hybrid solutions compared to cloud computing cryptography security implementation in algorithm execution, their research study solves the security issues associated with cloud computing.

Zaineldeen et al. [45] offered an overview of cloud computing cryptography, comparing various methods, tools, and conclusions. The authors investigate several cloud computing cryptography techniques, including homomorphic encryption, symmetric and asymmetric key encryption, and proxy re-encryption. They discuss issues like key management, data confidentiality, and data integrity arising when incorporating cryptography with cloud computing. They contend that even though cryptography might improve cloud computing security, significant challenges must be overcome. The findings give a thorough picture of the state of cryptography in cloud computing and emphasize the need for more research, mainly focusing on the difficulty of encryption implementation at the hypervisor layer.

Ogiela [46] developed hybrid CAPTCHA codes employing a hybrid techniques approach to examine the possibilities of cognitive cryptography. The results of the study indicated that cognitive cryptography has the potential to improve the security and integrity of cloud data.

Singh et al. [47] proposed a novel authentication approach based on mutual authentication for secure data-sharing in a federated cloud services environment. The proposed method combines cryptography and machine learning techniques ensemble voting classifier to achieve an essential level of security and privacy, as demonstrated by the experimental results.

An innovative AI-based encryption method for cloud computing, known as AI-Enc, was developed by Wang et al. in a report published in 2021 [48]. AI-Enc uses deep neural networks to encrypt and decode data safely and effectively. The authors asserted that traditional encryption techniques cannot match AI-Enc's ability to deliver more robust security and lower computational overhead, nor can it be integrated with existing hypervisors. In 2020, Mrbullwinkle et al. introduced the RL-Hyper framework, which uses reinforcement learning to optimize the performance of hypervisors. Throughput, latency, and energy consumption can all be significantly improved because of the framework's ability to dynamically modify hypervisor parameters based on workload factors and system conditions [49].

Table 3 summarizes some of the collected literature within three sections: reference, description, and results.

**Table 3:** Summary of related literature

| Ref. | Description | Results |
|---|---|---|
| [15–17] | In these papers, the authors attempt to assess the maturity of different types of hypervisors and study their impact on VMs. | The results showed that the performance of VMs and the cloud computing environment may be directly impacted by hypervisor performance. The VMs and the overall cloud computing environment may experience a slowdown if the hypervisor is underperforming. This may occur if the hypervisor is not set up correctly or if it is underpowered to manage the workload. But in most cases, virtualization just slightly increases the workload on the CPU, memory, storage, and network. |

(Continued)

**Table 3 (continued)**

| Ref. | Description | Results |
|---|---|---|
| [18–20] | In these papers, the authors studied the properties and implementation of KVM and Hyper-V hypervisors. | The authors state that KVM is, theoretically, better than Hyper-V because of its lightweight kernel and open-source nature. |
| [19,21] | In these papers, the authors compared the performance of different hypervisor types such as KVM, Hyper-V, Xen, and vSphere. | Researchers have not found any hypervisor that is superior in terms of performance, and each hypervisor should be tested to meet a specific need. Choosing the right hypervisor will continue to be an important challenge for proper virtualization management. |
| [21,23] | In these papers, the authors compare KVM and Hyper-V as well as other hypervisors using various criteria, such as responsiveness to SQL workloads, file server workloads, and web server workloads. | The researchers noted that there was a difference in the performance of hypervisors for different applications and workloads under different test conditions, but that Hyper-V performed better than KVM during the tests. Choosing the right hypervisor will increase energy efficiency during cloud workload. |
| [24] | In this paper, the author compares the performance of the Xen and Hyper-V hypervisors while running eight cryptographic algorithms: RSA, AES, RC4, CAST-128, TripleDES, DES, TwoFish, and BlowFish. The author used different key sizes, data sizes, and numbers of cores to test the performance of the algorithms. | The results show that Xen outperforms Hyper-V by 15% in terms of time and 6.1% in terms of CPU utilization, except for CPU utilization using AES, where Hyper-V outperforms Xen. |
| [25,26] | In these papers, the authors compare and describe the properties of KVM and Hyper-V hypervisors. | Each hypervisor has its properties and abilities. Both are Type 1 hypervisors; KVM and Hyper-V are supported on various platforms. Although they both provide a comparable set of functionalities, Hyper-V is a commercial product, whereas KVM is open-source and free to use. Compared to Hyper-V, KVM requires more configuration and management work. |

(Continued)

**Table 3 (continued)**

| Ref. | Description | Results |
|---|---|---|
| [30–32] | In these papers, the authors investigate the techniques used to ensure security and privacy in cloud environments, such as encryption, authentication, and access control. | Researchers have shown that there are different ways to ensure the security of the cloud, whether it is symmetric (such as AES), asymmetric (such as RSA), or hashing algorithms (e.g., SHA 256). The use of multi-factor authentication is also vital to ensure the security of the cloud to achieve a high degree of security and achieve what is called defense in depth (layers). |
| [38,39,41,42] | In these papers, the authors proposed schemes to ensure the security of the cloud in the health sector based on cryptography. | Using various encryption algorithms, the authors proposed a scheme that ensures data integrity, confidentiality, and precise control of access. The proposed scheme also reduces computational overheads, which increases system performance. |
| [43–46] | In these papers, the authors proposed using various hybrid techniques with cryptography, such as steganography, homomorphic, and CAPTCHA code in the cloud computing environment. | The authors state that encryption can be combined with other technologies to build a robust technology that ensures data security in the cloud. For example, encryption and steganography can be combined to provide dual security for data stored in the cloud. |
| [47–49] | In these papers, the authors propose using cryptography in the cloud in combination with machine learning and AI to offer methods and schemes for ensuring security. | The authors state that AI and machine learning can be used to secure the cloud and provide better performance to the hypervisor. The use of AI, as well as machine learning, is vital to ensuring hypervisor performance and cloud computing security in the future. |

## 3 Evaluation Method

In this research, authors examined the average response time for encryption and decryption of different encryption algorithms to verify the correlation between time and performance, evaluated the effect of changes in the number of CPU cores, examined the impact of varying key sizes, and finally, evaluate the effect of data size on performance.

As shown in Fig. 1, the proposed evaluation method involves deploying two servers, each utilizing a distinct hypervisor: Hyper-V and KVM. A VM running Windows 7 is instantiated on each server, and six cryptographic algorithms, including RSA, TripleDES, AES, CAST-128, TwoFish, and Blowfish,

are implemented using tools on each VM instance to evaluate the different cryptographic algorithms' performance.

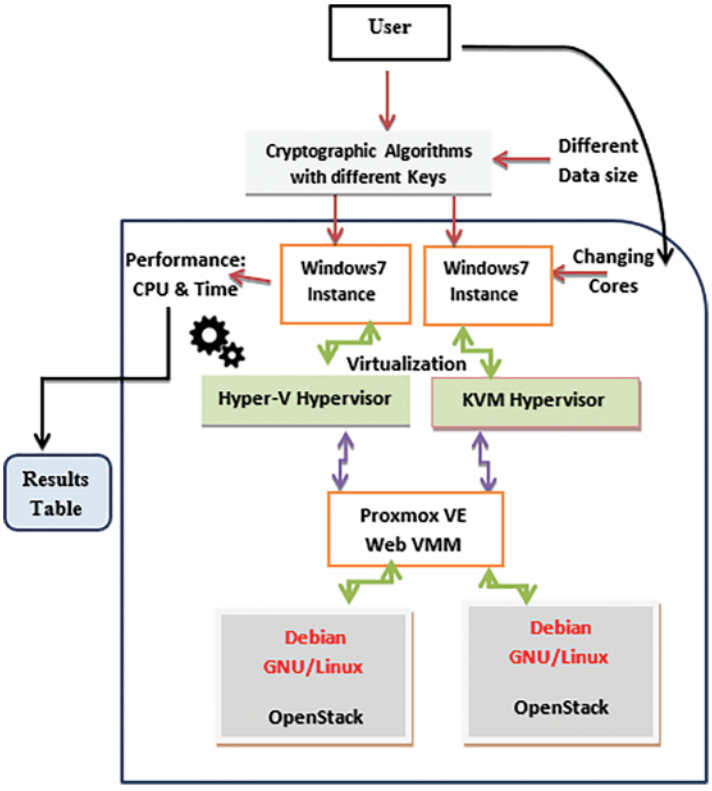


**Figure 1:** Evaluation method

### *3.1 Environment Setup*

The proposed environment in this study includes two different data centers (i.e., servers), both of which have an i7 CPU at 2.7 GHz and 16 GB of DDR RAM. For each server, the VM is implemented using Windows 7. The VM is allocated 4 GB of DDR RAM and a variable number of cores, depending on the experiment. Additionally, the VMs were deployed with the following subsequent software tools:

1. HsCipherSDK v2.1 tool that provides RSA, CAST-128, TwoFish, and Blowfish cryptographic algorithms while encryption and decryption with different keys using Python programming.
2. Rijndael tool that provides AES cryptographic algorithm.
3. PyCryptodome tool that provides TripleDES cryptosystem using Python programming language.
4. Windows 7 Performance Monitor is used to measure CPU usage over a specific period of time and is measured in percentage %.
5. Time is measured by minutes and seconds m:s using a stopwatch.

### *3.2 Performance Metrics and Dataset*

In this research, authors used HsCipherSDK v2.1 as a cryptographic tool to encrypt RSA, DES, TripleDES, CAST-128, TwoFish, and Blowfish algorithms. In contrast, the Rijndael tool is used to encrypt and decrypt the AES algorithm. For both tools, a different key can be chosen among various data. Meanwhile, other file types are selected from among the algorithms, such as PDF files, Images, and compressed files. The file sizes differ from 1 KB in RSA to 5 GB in AES.

CPU core in cloud computing can be changed among different VMs. So, the authors used two different cores during experiments 2 and 4.

Based on [50], the following equation (Eq. (1)) is used to calculate the overall ratio performance of the results:

$$Rat = \left| \frac{Average\,(Hyper - V) - Average\,(KVM)}{Average\,(KVM)} \right| \times 100\% \tag{1}$$

## 4 Result Analysis

This study investigates the performance of six popular encryption algorithms: RSA, TripleDES, AES, CAST-128, TwoFish, and Blowfish. Experiments were conducted several times for each algorithm in different contexts to ensure that the results were accurate and reliable. Below is a brief description of the algorithms used in the study, along with their evaluation results:

### *4.1 RSA*

The RSA algorithm is a cornerstone of modern cryptography and offers a safe way to send sensitive data over open networks. Because RSA fundamentally depends on the difficulty of factoring large numbers, it is a vital instrument for data encryption. The algorithm is based on a mathematical equation involving two large prime numbers, p and q, and their product, n. The selection of public and private key exponents, e and d, respectively, involves using Euler's totient function of n. RSA encryption involves raising the message to the power of e modulo n, while decryption requires raising the encrypted message to the power of d modulo n. The strength of RSA lies in its asymmetry, which makes it computationally infeasible to derive the private key from the public key. The recommended key size for RSA by NIST in 2015 was 2048 bits [51], and it is widely used in cloud computing [52].

Table 4 compares the performance of the Hyper-V and KVM hypervisors in terms of duration time, and CPU usage among different key sizes during the encryption and decryption operations. The first experiment indicates that with a key size of 64 and one core with a file size of 606 k, the Hyper-V hypervisor required 40.3 and 51 s, respectively, for encryption and decryption, and a CPU use was 61% for both encryption and decryption. The KVM hypervisor required 26.2 and 29.2 s for encryption and decryption, with CPU use of 59% and 60%, respectively. Since KVM consumes less time duration and CPU usage while encryption and decryption than Hyper-V, the results indicate that KVM outperformed Hyper-V regarding both response time and CPU utilization.

**Table 4:** RSA experimental results

| Experiment no. | Hypervisor type | Key size | No. of CPU cores | File size | Encryption time m:s | CPU encryption % | Decryption time m:s | CPU decryption % |
|---|---|---|---|---|---|---|---|---|
| 1 | Hyper-V | 64 | 1 | 606 k | 40.3 | 61 | 51 | 61 |
| | KVM | 64 | 1 | 606 k | 26.2 | 59 | 29.2 | 60 |

(Continued)

**Table 4 (continued)**

| Experiment no. | Hypervisor type | Key size | No. of CPU cores | File size | Encryption time m:s | CPU encryption % | Decryption time m:s | CPU decryption % |
|---|---|---|---|---|---|---|---|---|
| 2 | Hyper-V | 1024 | 1 | 12.2 k | 14.5 | 56 | 23.1 | 54 |
| | KVM | 1024 | 1 | 12.2 k | 14.4 | 54 | 21.5 | 53 |
| 3 | Hyper-V | 2048 | 1 | 1 k | 5.4 | 54 | 10.3 | 55 |
| | KVM | 2048 | 1 | 1 k | 4.6 | 53 | 10.5 | 53 |
| 4 | Hyper-V | 256 | 1 | 12.2 k | 2.3 | 64 | 3.1 | 64 |
| | KVM | 256 | 1 | 12.2 k | 2 | 61 | 2.1 | 55 |
| 5 | Hyper-V | 1536 | 1 | 12.2 k | 34 | 64 | 60.2 | 62 |
| | KVM | 1536 | 1 | 12.2 k | 35.5 | 56 | 60 | 52 |
| 6 | Hyper-V | 2048 | 1 | 12.2 k | 67.2 | 52 | 106.4 | 56 |
| | KVM | 2048 | 1 | 12.2 k | 77.2 | 51 | 120.1 | 52 |
| 7 | Hyper-V | 1024 | 2 | 12.2 k | 15.5 | 100 | 26.4 | 89 |
| | KVM | 1024 | 2 | 12.2 k | 9.4 | 95 | 9.4 | 87 |
| 8 | Hyper-V | 1024 | 2 | 2.25 M | 51.5 | 95 | 78.2 | 87 |
| | KVM | 1024 | 2 | 2.25 M | 25 | 85 | 32.2 | 82 |
| 9 | Hyper-V | 2048 | 2 | 1 K | 4.1 | 96 | 7.5 | 96 |
| | KVM | 2048 | 2 | 1 K | 3.5 | 94 | 7 | 94 |
| 10 | Hyper-V | 2048 | 2 | 2 K | 7.6 | 94 | 15 | 93 |
| | KVM | 2048 | 2 | 2 K | 7.6 | 94 | 13.5 | 93 |

Table 5 compares the average response time and CPU utilization of two hypervisors, KVM and Hyper-V, during the encryption and decryption processes using the RSA cryptographic algorithm. The results reveal that KVM outperforms Hyper-V regarding time and CPU consumption for encryption and decryption operations. Specifically, KVM demonstrates a 3.7 and 3.4 difference in time and CPU utilization for encryption and a 7.6 and 3.6 difference for decryption. These results show that KVM is a more efficient and effective hypervisor for cryptographic operations using the RSA algorithm, even when changing the key, data size, or core numbers. It can be helpful for companies and individuals looking to improve their performance and security.

**Table 5:** RSA performance

| RSA | Encryption | | Decryption | |
|---|---|---|---|---|
| | Time | CPU | Time | CPU |
| Hyper-V | 24.2 | 73.6 | 38.1 | 71.7 |
| KVM | 20.5 | 70.2 | 30.5 | 68.1 |
| Differences | 3.7 | 3.4 | 7.6 | 3.6 |

### *4.2 AES*

Modern cryptographic systems frequently use the symmetric block cipher known as the AES [53]. The Data Encryption Standard (DES) was chosen as its replacement by the National Institute of Standards and Technology (NIST) in 2001. AES is developed to be secure against various attacks, such as side-channel attacks, differential and linear cryptanalysis, and brute-force attacks. AES utilizes a key that is either 128, 192, or 256 bits long and operates on fixed block sizes of 128 bits [53]. The algorithm comprises rounds with several smaller steps, including substitution, permutation, and XOR operations. The key schedule is the same for all rounds except the final round, which differs slightly

from the earlier rounds. The overall strength of AES comes from its use of a substitution-permutation network (SPN) structure and the extensive diffusion of input bits throughout the rounds.

Galois field arithmetic, especially the finite field GF (2 ^ 8), is the foundation of the mathematical formula utilized in AES [54]. This finite field consists of 256 elements and represents bytes in the input block and elements of the key schedule. The AES algorithm uses a set of standard operations, including the substitution of bytes, shift rows, mixing columns, and adding round keys. The substitution step involves replacing each byte of the input block with another byte based on a fixed lookup table called the S-box. The shift rows step involves cyclically shifting the bytes in each row of the input block by a fixed amount. The mix columns step involves multiplying each column of the input block by a fixed matrix, resulting in a diffusion of input bits throughout the block. The add-round key step involves XORing the input block with a key schedule derived from the encryption key. Together, these steps create a highly secure cloud security environment and efficient encryption algorithm widely used in applications ranging from secure communication to data storage. This paper presents a detailed analysis of the AES algorithm using (128, 192, and 256), CPU core numbers (2 to 4), and its performance in ten repeated experiments as in Table 6 below.

**Table 6:** AES experimental results

| Experiment no. | Hypervisor type | Key size | No. of CPU cores | File size | Encryption time m:s | CPU encryption % | Decryption time m:s | CPU decryption % |
|---|---|---|---|---|---|---|---|---|
| 1 | Hyper-V | 128 | 2 | 2 G | 2.4 | 67 | 2.4 | 69 |
| | KVM | 128 | 2 | 2 G | 2.4 | 60 | 2.4 | 55 |
| 2 | Hyper-V | 128 | 4 | 2 G | 3.1 | 34 | 2.5 | 40 |
| | KVM | 128 | 4 | 2 G | 2.6 | 30 | 2.3 | 34 |
| 3 | Hyper-V | 128 | 4 | 5 G | 7.2 | 35 | 7.1 | 38 |
| | KVM | 128 | 4 | 5 G | 6.3 | 30 | 6.1 | 33 |
| 4 | Hyper-V | 128 | 4 | 3 G | 3.4 | 35 | 3.5 | 36 |
| | KVM | 128 | 4 | 3 G | 3.4 | 30 | 3.2 | 32 |
| 5 | Hyper-V | 192 | 2 | 2 G | 2.6 | 67 | 2.6 | 71 |
| | KVM | 192 | 2 | 2 G | 2.5 | 62 | 2.6 | 56 |
| 6 | Hyper-V | 192 | 4 | 2 G | 2.5 | 37 | 3.2 | 37 |
| | KVM | 192 | 4 | 2 G | 2.5 | 33 | 2.4 | 34 |
| 7 | Hyper-V | 256 | 2 | 3 G | 4.2 | 70 | 4.0 | 69 |
| | KVM | 256 | 2 | 3 G | 3.5 | 63 | 3.2 | 64 |
| 8 | Hyper-V | 256 | 2 | 2 G | 3.3 | 63 | 3.3 | 67 |
| | KVM | 256 | 2 | 2 G | 2.5 | 61 | 2.5 | 61 |
| 9 | Hyper-V | 256 | 4 | 2 G | 3 | 37 | 3.3 | 38 |
| | KVM | 256 | 4 | 2 G | 2.6 | 34 | 2.6 | 34 |
| 10 | Hyper-V | 256 | 4 | 1 G | 1.1 | 34 | 1.1 | 32 |
| | KVM | 256 | 4 | 1 G | 1.1 | 32 | 1 | 32 |

Table 7 compares the average response time and CPU utilization of two hypervisors, KVM and Hyper-V, during the encryption and decryption processes using the AES cryptographic algorithm. The results reveal that KVM outperforms Hyper-V regarding time and CPU consumption for encryption and decryption operations. Specifically, KVM demonstrates a 0.4 and 4.4 difference in time and CPU utilization for encryption and a 0.5 and 4.8 difference for decryption. These findings suggest that KVM is a more efficient and effective hypervisor for performing cryptographic tasks using the AES algorithm, even when changing the key, data size, or core numbers. It can significantly benefit organizations and individuals seeking to enhance their security and performance capabilities.

**Table 7:** AES performance

| AES | Encryption | | Decryption | |
|---|---|---|---|---|
| | Time | CPU | Time | CPU |
| Hyper-V | 3.5 | 45.4 | 3.5 | 47.4 |
| KVM | 3.1 | 41 | 3 | 42.6 |
| Differences | 0.4 | 4.4 | 0.5 | 4.8 |

### *4.3 TripleDES*

The Triple Data Encryption Standard (TripleDES) is a cryptographic technique that uses a symmetric block cipher. Three DES keys comprise a key bundle, also known as a key [55].

The authors have performed ten different experiments for both Hyper-V and KVM hypervisors. Different CPU core numbers (2 and 4) and file sizes with fixed key size (192-bit) were used. Table 8 shows the average time and CPU usage while encryption and decryption using TripleDES cryptographic algorithm.

**Table 8:** TripleDES performance

| TripleDES | Encryption | | Decryption | |
|---|---|---|---|---|
| | Time | CPU | Time | CPU |
| Hyper-V | 11.9 | 48.2 | 12.1 | 49.1 |
| KVM | 11.6 | 44.9 | 11.7 | 46.4 |
| Differences | 0.3 | 3.3 | 0.4 | 2.7 |

As presented in Table 8, the performance of two hypervisors, KVM and Hyper-V, was evaluated during the encryption and decryption processes using the TripleDES cryptographic algorithm. The analysis indicates that KVM has superior CPU performance for encryption compared to Hyper-V, but Hyper-V exhibits better encryption response time. On the other hand, KVM has better CPU utilization and time response for decryption than Hyper-V.

### *4.4 CAST-128*

CAST-128, often known as CAST5, is a 1996-designed member of the CAST family. The technique is based on a traditional Feistel/DES network with 16 rounds, 64-bit block, and up to 128-bit keys. CAST-128 has 16 subkey pairs, three types of round functions, and eight distinct S-boxes [56].

The authors have performed ten different experiments for both Hyper-V and KVM hypervisors. The key (128-bit), CPU core numbers (2 and 4), and different file sizes were used. Table 9 shows the average time and CPU usage while encryption and decryption using the CAST-128 cryptographic algorithm.

**Table 9:** CAST-128 performance

| CAST-128 | Encryption | | Decryption | |
|---|---|---|---|---|
| | Time | CPU | Time | CPU |
| Hyper-V | 2.1 | 46.3 | 2 | 48.3 |
| KVM | 1.9 | 40.3 | 1.9 | 41 |
| Differences | 0.2 | 6 | 0.1 | 7.3 |

Table 9 compares the average response time and CPU utilization of two hypervisors, KVM and Hyper-V, during the encryption and decryption processes using the CAST-128 cryptographic algorithm. The results reveal that KVM outperforms Hyper-V regarding time and CPU consumption for encryption and decryption operations. Specifically, KVM shows a 0.2 and 6 difference in time and CPU utilization for encryption and a 0.1 and 7.3 difference for decryption. These findings suggest that KVM is a more efficient and effective hypervisor for performing cryptographic tasks using the CAST-128 algorithm, even when changing the key, data size, or core numbers. It can significantly benefit organizations and individuals seeking to enhance their security and performance capabilities.

### *4.5 BLOWFISH*

Blowfish is a symmetric block cipher designed to provide secure encryption of digital data. Bruce Schneier created it in 1993, and it gained popularity due to its flexibility and high level of security. Blowfish is a cipher well-suited for encrypting enormous amounts of data owing to its block length of 64 bits. It utilizes four substitution boxes, often known as "S-Boxes," and eighteen permutation arrays, or "P-Boxes,". Blowfish is appropriate for applications requiring high-speed encryption since it supports various keys ranging from 32 bits to 448 bits [56]. The Feistel network, a prominent topology used in many block ciphers, is the basis for Blowfish's mathematical formula. Blowfish encrypts data in rounds or iterations, including a replacement step, a permutation step, and a key mixing step. The substitution step is performed using the S-Boxes, which replace blocks of data with other blocks according to a predetermined table. The permutation step is performed using the P-Boxes, which scramble the order of the data. Finally, the key mixing step involves XORing the data with a portion of the secret key. This process is repeated for several rounds, resulting in encrypted data. The strength of Blowfish lies in its complex key schedule, which ensures that each key bit affects many parts of the encryption process, making it highly resistant to attacks.

The authors have performed ten different experiments for both Hyper-V and KVM hypervisors. A 64-bit key size, CPU core numbers (2 and 4), and different file sizes were used.

Table 10 compares the average response time and CPU utilization of two hypervisors, KVM and Hyper-V, during the encryption and decryption processes using the BLOWFISH cryptographic algorithm. The results reveal that KVM outperforms Hyper-V regarding time and CPU consumption for encryption and decryption operations. Specifically, KVM demonstrates a 1.1 and 4.8 difference in time and CPU utilization for encryption and a 1.1 and 4.5 difference for decryption. These findings suggest that KVM is a more efficient and effective hypervisor for performing cryptographic tasks using the BLOWFISH algorithm, even when changing the key, data size, or core numbers. It can significantly benefit organizations and individuals seeking to enhance their security and performance capabilities.

**Table 10:** BLOWFISH performance

| BLOWFISH | Encryption | | Decryption | |
|---|---|---|---|---|
| | Time | CPU | Time | CPU |
| Hyper-V | 7.4 | 50.5 | 7.1 | 51.5 |
| KVM | 6.3 | 45.7 | 6 | 47 |
| Differences | 1.1 | 4.8 | 1.1 | 4.5 |

### *4.6 TwoFish*

Twofish is a symmetric block encryption algorithm developed in 1998 [56,57]. The algorithm works with fixed-size data blocks with a key length of 128, 192, or 256 bits. Twofish's design combines several characteristics to make it secure and efficient. Using the Feistel cipher structure, a popular method for block ciphers is one such aspect. TwoFish employs four S-boxes, which replace input bits with output bits based on the key and round number. The S-boxes are developed from extended Rijndael S-boxes, which depend on the properties of finite fields.

The authors performed ten tests for the Hyper-V and KVM hypervisors using various keys (128, 192, and 256-bit), CPU core counts (2 and 4), and file sizes. Table 11 compares the average response time and CPU usage of two hypervisors, KVM and Hyper-V, during encryption and decryption. The findings show that KVM consumes fewer CPU for encryption and takes the same time for Hyper-V. KVM surpasses Hyper-V regarding both time and CPU use for decryption operations. KVM reveals a 3.3 difference in CPU use for encryption and a 0.1 in time. These results imply that KVM is a more efficient and effective hypervisor for completing cryptographic operations using the TWOFISH technique, even if the key, data size, or core counts are modified.

**Table 11:** TWOFISH performance

| TwoFish | Encryption | | Decryption | |
|---|---|---|---|---|
| | Time | CPU | Time | CPU |
| Hyper-V | 5.6 | 48.1 | 5.6 | 48.6 |
| KVM | 5.6 | 44.8 | 5.5 | 46.3 |
| Differences | 0 | 3.3 | 0.1 | 3.3 |

### *4.7 Overall Results*

The overall performance time and CPU utilization during encryption and decryption for both Hyper-V and KVM hypervisors of all cryptosystems and all previous tables are presented in Table 12 and Fig. 2.

After applying Eq. (1) to compare Hyper-V and KVM, the results show that KVM performs better than Hyper-V in terms of encryption time by 10.5% ((8.1 − 7.3)/7.3) and decryption time by 15.4% ((9.7 − 8.4)/8.4), resulting in an overall average of 12.95%. Similarly, KVM shows lower CPU utilization than Hyper-V during encryption with a ratio of 10.5% ((51.4 − 46.5)/46.5) and 9.9% ((51.8 − 47.1)/47.1) during decryption, resulting in an overall average of 10.2%.

**Table 12:** Overall algorithms

| Overall algorithms | Time | | CPU | |
|---|---|---|---|---|
| | Encryption | Decryption | Encryption | Decryption |
| KVM | 7.3 | 8.4 | 46.5 | 47.1 |
| Hyper-V | 8.1 | 9.7 | 51.4 | 51.8 |

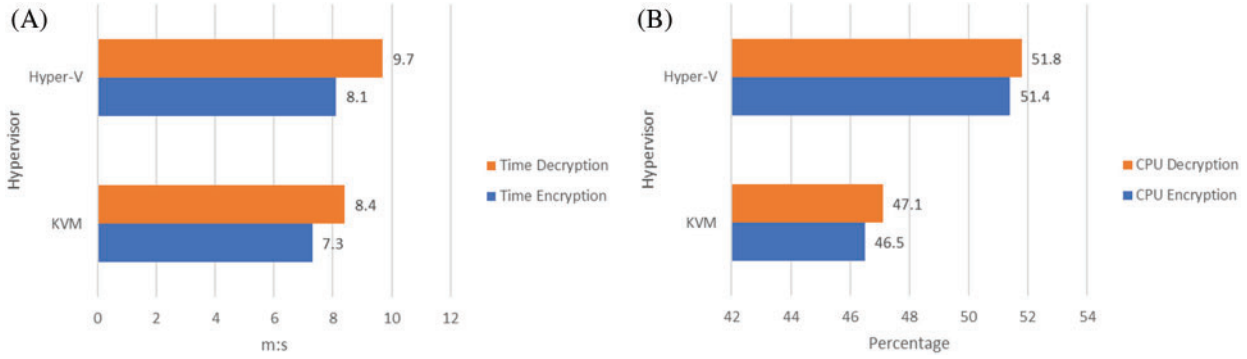


**Figure 2:** Performance of all algorithms in terms of time (A), and CPU usage (B)

Moreover, Table 13 demonstrates a performance comparison of the six cryptography algorithms being compared (i.e., RSA, AES, TripleDES, CAST-128, BlowFish, and TwoFish Algorithms) using KVM and Hyper-V. Fig. 3 shows the overall time performance in m:s for each algorithm while encryption and decryption, and Fig. 4 shows the CPU utilization in % while encryption and decryption.

**Table 13:** Performance of cryptographic algorithms on KVM and Hyper-V

| | Time | | | | CPU | | | |
|---|---|---|---|---|---|---|---|---|
| | Encryption | | Decryption | | Encryption | | Decryption | |
| | KVM | Hyper-V | KVM | Hyper-V | KVM | Hyper-V | KVM | Hyper-V |
| RSA | 20.5 | 24.2 | 30.5 | 38.1 | 70.2 | 73.6 | 68.1 | 71.7 |
| AES | 3.1 | 3.5 | 3 | 3.5 | 41 | 45.4 | 42.6 | 47.4 |
| TripleDES | 11.6 | 11.9 | 11.7 | 12.1 | 44.9 | 48.2 | 46.4 | 49.1 |
| CAST-128 | 1.9 | 2.1 | 1.9 | 2 | 40.3 | 46.3 | 41 | 48.3 |
| BlowFish | 6.3 | 7.4 | 6 | 7.1 | 45.7 | 50.5 | 47.1 | 51.5 |
| TwoFish | 5.6 | 5.6 | 5.5 | 5.6 | 44.8 | 48.1 | 46.3 | 48.6 |

To compare our results with other studies, we choose the paper [24] published in 2022 as a relevant reference, because it also investigated the performance of different cryptographic algorithms on VMs. In [24], the authors studied eight different cryptographic algorithms; RSA, AES, RC4, CAST-128, TripleDES, DES, TwoFish, and BlowFish, while this study excluded the DES and RC4 algorithms because they are no longer safe. The authors in [24] compared Xen and Hyper-V, while this study compares Hyper-V and KVM, as they are the most commonly used hypervisors. In [24], they found

that Hyper-V outperforms Xen for most results during encryption and decryption operations, while this study shows that KVM outperforms Hyper-V in terms of time duration and CPU usage for all encryption and decryption operations. Table 14 shows the comparison of this study with [24]:

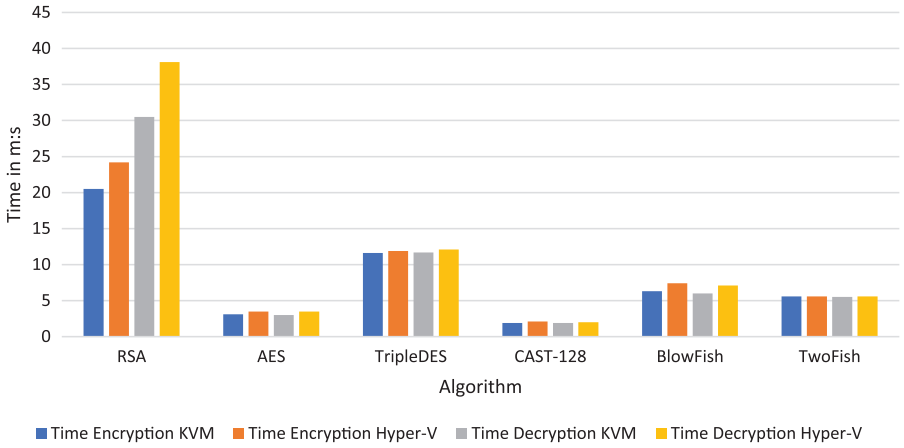


**Figure 3:** Overall time performance of cryptography algorithms in m:s during encryption and decryption

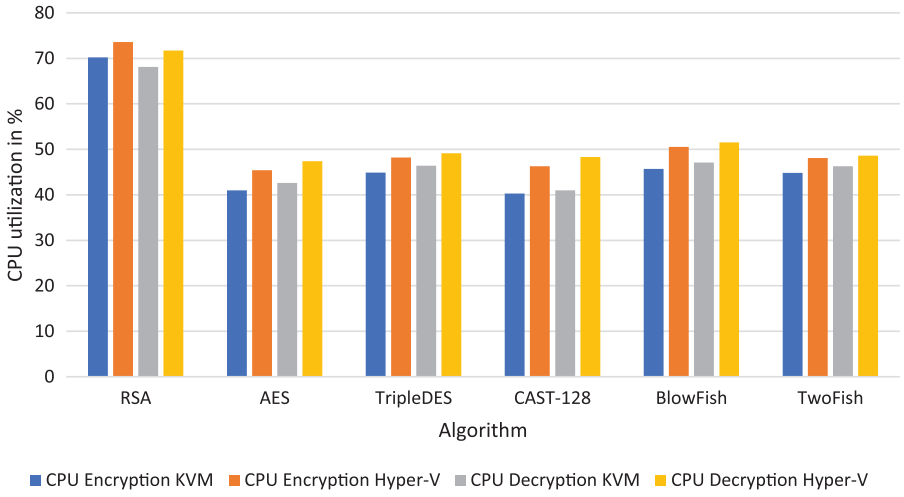


**Figure 4:** Overall CPU utilization of cryptography algorithms in % during encryption and decryption

**Table 14:** Comparison with other studies

| Ref. | Tested hypervisor | Tested algorithms | Results |
|---|---|---|---|
| [24] | Xen and Hyper-V | RSA, AES, RC4, CAST-128, TripleDES, DES, TwoFish, and BlowFish. | Hyper-V is better than Xen for most results. |

(Continued)

**Table 14 (continued)**

| Ref. | Tested hypervisor | Tested algorithms | Results |
|---|---|---|---|
| This study | Hyper-V and KVM | RSA, AES, CAST-128, TripleDES, TwoFish, and BlowFish. | KVM is better than Hyper-V for all results. |

## 5 Conclusion

Cryptographic methods are essential for preserving data security and privacy in the cloud environment. This study evaluated the efficiency of two widely used hypervisors, Hyper-V and KVM, in implementing six cryptographic algorithms: RSA, AES, TripleDES, CAST-128, BLOWFISH, and TwoFish. The study measured response time and CPU utilization during encryption and decryption processes. The results show that KVM surpasses Hyper-V in terms of time duration for all the experiments and CPU utilization for all algorithms, especially with more cores. It is important to remember that various variables might affect how well virtualization solutions work, including the hardware and software configurations utilized in the study. The results also support the prevailing view that using the KVM hypervisor is better than using Hyper-V for VMs since KVM works with the Linux kernel, making it more lightweight than the Windows kernel. Thus, it is essential to conduct further research to confirm these findings and explore other factors that may impact the performance of virtualization technologies. The following future works can also be undertaken:

- Examine the performance of using other hypervisors, such as VMware or VMWare ESX.
- Examine the performance of other cryptographic algorithms, such as Salsa20 and Curve25519, in cloud environments.
- Study and compare the performance of different versions of Hyper-V and KVM.
- Study the possibility of improving the effectiveness of encryption and decryption on the hypervisor using artificial intelligence.

The study had some limitations, such as:

- Specific software and hardware configurations were used during the study. Different settings may produce different results.
- The effects of network congestion, bandwidth, and latency on the encryption and decryption operations were not taken into account in this investigation. These factors could have an impact on cloud environments' quality of service and user experience, particularly for apps that need data transmission and communication in real-time or almost real-time.

**Acknowledgement:** Not applicable.

**Funding Statement:** The authors received no specific funding for this study.

**Author Contributions:** Study conception and design: Nader Abdel Karim, Waleed K. Abdulraheem, Osama A. Khashan; data collection: Hasan Kanaker, Mahmoud Farfoura, Mohammad Alshinwan; analysis and interpretation of results: Waleed K. Abdulraheem, Nader Abdel Karim, Osama A. Khashan, Moutaz Alazab; draft manuscript preparation: Nader Abdel Karim, Waleed K.

Abdulraheem, Osama A. Khashan, Moutaz Alazab. All authors reviewed the results and approved the final version of the manuscript.

**Availability of Data and Materials:** Not applicable.

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

## References


[1] H. Shukur, S. Zeebaree, R. Zebari, D. Zeebaree, O. Ahmed and A. Salih, "Cloud computing virtualization of resources allocation for distributed systems," *J. Appl. Sci. Technol. Trends*, vol. 1, no. 3, pp. 98–105, 2020. doi: 10.29121/granthaalayah.v8.i8.2020.926.

[2] T. G. Peter Mell, "The NIST definition of cloud computing," *Reco. Natl. Inst. Stand. Technol.*, pp. 1–3, 2011. Accessed: Aug. 10, 2023. [Online]. Available: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

[3] N. Tissir, S. E. Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal," *J. Reliab. Intell. Environ.*, vol. 7, no. 2, pp. 69–84, Jun. 2021. doi: 10.1007/s40860-020-00115-0.

[4] M. Herman *et al.*, "NIST cloud computing forensic science challenges," US Depart. Commer., Natl. Inst. Stand. Technol., 2020. doi: 10.6028/NIST.IR.8006.

[5] M. Quraishi, E. Tavakoli, and F. Ren, "A survey of system architectures and techniques for FPGA virtualization," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 9, pp. 2216–2230, 2021. doi: 10.1109/TPDS.2021.3063670.

[6] A. Khayer, M. S. Talukder, Y. Bao, and M. N. Hossain, "Cloud computing adoption and its impact on SMEs' performance for cloud supported operations: A dual-stage analytical approach," *Technol. Soc.*, vol. 60, pp. 101225, 2020. doi: 10.1016/j.techsoc.2019.101225.

[7] L. Columbus, *83% of Enterprise Workloads Will Be in the Cloud by 2020*. Forbes, 2018. Accessed: Aug. 10, 2023. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloadswill-be-in-the-cloud-by-2020

[8] N. Sreenivasulu, "Cloud computing statistics & trends for 2023," 2023. Accessed: Oct. 15, 2023. [Online]. Available: https://www.vpnhelpers.com/cloud-computing-statistics/

[9] N. M. Al-Ramahi, M. Odeh, Z. Alrabie, and N. Qozmar, "The TOEQCC framework for sustainable adoption of cloud computing at higher education institutions in the Kingdom of Jordan," *Sustain.*, vol. 14, no. 19, pp. 12744, 2022. doi: 10.3390/su141912744.

[10] S. Kent, "Federal cloud computing strategy (June 24, 2019)," 2019. Accessed: Jul. 12, 2023. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf

[11] S. Louvros, M. Paraskevas, and T. Chrysikos, "QoS-aware resource management in 5G and 6G cloud-based architectures with priorities," *Inform.*, vol. 14, no. 3, pp. 175, Mar. 2023. doi: 10.3390/info14030175.

[12] K. Filippou, G. Aifantis, G. A. Papakostas, and G. E. Tsekouras, "Structure learning and hyperparameter optimization using an automated machine learning (AutoML) pipeline," *Inform.*, vol. 14, no. 4, pp. 232, Apr. 2023. doi: 10.3390/info14040232.

[13] P. Bir, S. V. Karatangi, and A. Rai, "Design and implementation of an elastic processor with hyperthreading technology and virtualization for elastic server models," *J. Supercomput.*, vol. 76, no. 9, pp. 7394–7415, 2020. doi: 10.1007/s11227-020-03174-5.

[14] H. Akbar, M. Zubair, and M. S. Malik, "The security issues and challenges in cloud computing," *Int. J. Electron. Crime Investig.*, vol. 7, no. 1, pp. 13–32, 2023. doi: 10.54692/ijeci.2023.0701125.

[15] D. Silva, J. Rafael, and A. Fonte, "Virtualization maturity in creating system VM: An updated performance evaluation," *J. Electr. Comput. Eng. Res.*, vol. 3, no. 2, pp. 7–17, 2023. doi: 10.53375/ijecer.2023.341.

[16] A. Ullah, N. M. Nawi, and S. Ouhame, "Recent advancement in VM task allocation system for cloud computing: Review from 2015 to 2021," *Artif. Intell. Rev.*, vol. 55, no. 3, pp. 2529–2573, 2022. doi: 10.1007/s10462-021-10071-7.

[17] J. Li, S. Xue, W. Zhang, R. Ma, Z. Qi and H. Guan, "When I/O interrupt becomes system bottleneck: Efficiency and scalability enhancement for SR-IOV network virtualization," *IEEE Trans. Cloud Comput.*, vol. 7, no. 4, pp. 1183–1196, 2017. doi: 10.1109/TCC.2017.2712686.

[18] S. Ali, "Virtualization with KVM," in *Practical Linux Infrastructure*, 1st ed. Cham, Switzerland: Springer Nature, 2015, pp. 53–80.

[19] R. Morabito, J. Kjällman, and M. Komu, "Hypervisors vs. lightweight virtualization: A performance comparison," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Tempe, Arizona, USA, 2015, pp. 386–393.

[20] Huawei Technologies Co., Ltd., "Virtualization technology," in *Cloud Computing Technology*, 1st ed. Cham, Switzerland: Springer Nature, 2022, pp. 97–144.

[21] J. Hwang, S. Zeng, F. Y. Wu, and T. Wood, "A component-based performance comparison of four hypervisors," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manag. (IM 2013)*, Ghent, Belgium, 2013, pp. 269–276.

[22] B. Djordjevic, V. Timcenko, N. Kraljevic, and N. Macek, "File system performance comparison in full hardware virtualization with ESXi, KVM, Hyper-V and Xen hypervisors," *Adv. Electr. Comput. Eng.*, vol. 21, no. 1, pp. 11–20, 2021. doi: 10.4316/AECE.2021.01002.

[23] C. Jiang *et al.*, "Energy efficiency comparison of hypervisors," *Sustain. Comput.: Inform. Syst.*, vol. 22, pp. 311–321, 2019. doi: 10.1016/j.suscom.2017.09.005.

[24] W. K. Abdulraheem, "Performance comparison of Xen AND hyper-V in cloud computing while using cryptosystems," *Int. J. Adv. Soft Comput. Appl.*, vol. 14, no. 3, pp. 17–30, 2022. doi: 10.15849/IJASCA.221128.02.

[25] V. K. Manik and D. Arora, "Performance comparison of commercial VMM: ESXI, XEN, HYPER-V & KVM," in *Proc. Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Bharati Vidyapeeth, New Delhi, India, 2016, pp. 1771–1775.

[26] P. K. Das, "Comparative study on XEN, KVM, VSphere, and Hyper-V," *Emerging Research Surrounding Power Consumption and Performance Issues in Utility Computing*, pp. 233–261, 2016. doi: 10.4018/978-1-4666-8853-7.ch011.

[27] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, and M. M. Hassan, "DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2472–2481, 2023. doi: 10.1109/TITS.2021.3122368.

[28] P. Kumar, R. Tripathi, and G. P. Gupta, "P2IDF: A privacy-preserving based intrusion detection framework for software defined Internet of Things-fog (SDIoT-Fog)," in *Proc. Int. Conf. Distrib. Comput. Netw. (ICDCN)*, Quezon City, Philippines, 2021, pp. 37–42.

[29] T. Liu, B. Di, P. An, and L. Song, "Privacy-preserving incentive mechanism design for federated cloud-edge learning," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2588–2600, 2021. doi: 10.1109/TNSE.2021.3100096.

[30] Z. Yan, Z. Peng, and V. V. Athanasios, "A security and trust framework for virtualized networks and software-defined networking," *Secur. Commun. Netw.*, vol. 5, no. 16, pp. 3059–3069, 2016. doi: 10.1002/sec.1243.

[31] N. A. Karim and A. H. Ali, "E-learning virtual meeting applications: A comparative study from a cybersecurity perspective," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 24, no. 2, pp. 1121–1129, 2021. doi: 10.11591/ijeecs.v24.i2.

[32] N. A. Karim, H. Kanaker, S. Almasadeh, and J. Zarqou, "A robust user authentication technique in online examination," *Int. J. Comput.*, vol. 20, no. 4, pp. 535–542, 2021. doi: 10.47839/ijc.20.4.2441.

[33] S. S. Gaur, H. S. Kalsi, and S. Gautam, "A comparative study and analysis of cryptographic algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH," *Int. J. Res. Electron. Comput. Eng.*, vol. 7, no. 1, pp. 996–999, 2019.

[34] A. Martín, A. Hernández, M. Alazab, J. Jung, and D. Camacho, "Evolving generative adversarial networks to improve image steganography," *Expert Syst. Appl.*, vol. 222, pp. 119841, Jul. 2023. doi: 10.1016/j.eswa.2023.119841.

[35] R. di Pietro and F. Lombardi, "Virtualization technologies and cloud security: Advantages, issues, and perspectives," in *Lecture Notes in Computer Science*, vol. 11170, pp. 166–185, 2018. doi: 10.1007/978-3-030-04834-1_9

[36] F. Thabit, S. Alhomdy, and S. Jagtap, "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing," *Glob. Transit. Proc.*, vol. 2, no. 1, pp. 100–110, 2021. doi: 10.1016/j.gltp.2021.01.014.

[37] R. R. Bhandari and N. Mishra, "Cloud computing a CRM service based on separate encryption and decryption using Blowfish algorithm," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 1, no. 4, pp. 217–223, 2013. doi: 10.17762/ijritcc.v1i4.2766.

[38] P. Chinnasamy and P. Deepalakshmi, "HCAC-EHR: Hybrid cryptographic access control for secure EHR retrieval in healthcare cloud," *J. Amb. Intel. Hum. Comp.*, vol. 13, no. 2, pp. 1001–1019, 2021. doi: 10.1007/s12652-021-02942-2.

[39] R. Dwivedi, R. K. Kumar, and R. Buyya, "Secure healthcare monitoring sensor cloud with attribute-based elliptical curve cryptography," *Int. J. Cloud Appl. Comput. (IJCAC)*, vol. 11, no. 3, pp. 1–18, 2021. doi: 10.4018/IJCAC.2021070101.

[40] S. Vinothkumar, J. Amutharaj, and S. Jeyabalan, "A comprehensive study of cryptography and key management based security in cloud computing," *J. Contemp. Issues Bus. Gov.*, vol. 27, no. 3, pp. 1909–1923, 2021. doi: 10.31838/jcr.07.14.412.

[41] D. Suresha and K. Karibasappa, "Enhancing data protection in cloud computing using key derivation based on cryptographic technique," in *Proc. Int. Conf. Comput. Methodol. Commun. (ICCMC)*, Erode, India, 2021, pp. 291–299.

[42] A. Orobosade, T. Aderonke, A. Boniface, and A. J. Gabriel, "Cloud application security using hybrid encryption," *Commun. Appl. Electron.*, vol. 7, no. 33, pp. 25–31, 2020. doi: 10.5120/cae2020652866.

[43] M. S. Abbas, S. S. Mahdi, and S. A. Hussien, "Security improvement of cloud data using hybrid cryptography and steganography," in *Proc. Int. Conf. Comput. Sci. Softw. Eng. (CSASE)*, Duhok, Iraq, 2020, pp. 123–127.

[44] F. S. and N. K. J. Sumit Chaudhary, "Comparative study between cryptographic and hybrid techniques for implementation of security in cloud computing," in *Performance Management of Integrated Systems and its Applications in Software Engineering*, Cham, Switzerland: Asset Analytics, Springer Nature, 2019, vol. 22, pp. 127–135. doi: 10.1007/978-981-13-8253-6_12.

[45] S. Zaineldeen and A. Ate, "Review of cryptography in cloud computing," *Int. J. Comput. Sci. Mobile Comput.*, vol. 9, no. 3, pp. 211–220, 2020. doi: 10.47760/ijcsmc.

[46] U. Ogiela, "Cognitive cryptography for data security in cloud computing," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 18, pp. e5557, 2020. doi: 10.1002/cpe.5557.

[47] A. K. Singh and D. Saxena, "A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment," *J. Appl. Secur. Res.*, vol. 11, no. 3, pp. 1–24, 2021. doi: 10.1080/19361610.2020.1870404.

[48] W. G. V. L. R. W. Gaspar, "Private AI: Machine learning on encrypted data—Ericsson," *Ericsson*, 2021. Accessed: Aug. 19, 2023. [Online]. Available: https://www.ericsson.com/en/blog/2021/9/machine-learning-on-encrypted-data

[49] M. U. E. Mrbullwinkle, "Azure OpenAI service encryption of data at rest—Azure AI services | Microsoft Learn," *Microsoft*, 2023. Accessed: Aug. 19, 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/ai-services/openai/encrypt-data-at-rest

[50] W. K. A. Abdulraheem, "Comparative analysis of the performance for cloud computing hypervisors with encrypted algorithms," M.S. thesis, Middle East Univ., Jordan, 2014.

[51] E. Barker and W. Barker, *Recommendation for Key Management, Part 2: Best Practices for Key Management Organization*. Gaithersburg, Maryland, USA: National Institute of Standards and Technology, 2018.

[52] W. K. AbdulRaheem, S. B. M. Yasin, N. I. B. Udzir, and M. R. B. K. Ariffin, "Improving the performance of [0, 1, 3]-NAF recoding algorithm for elliptic curve scalar multiplication," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 4, pp. 275–279, 2019. doi: 10.14569/IJACSA.2019.0100432.

[53] W. K. AbdulRaheem, S. B. M. Yasin, N. I. B. Udzir, and M. R. B. K. Ariffin, "New quintupling point arithmetic 5P formulas for Lôpez-Dahab coordinate over binary elliptic curve cryptography," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 7, pp. 397–401, 2019. doi: 10.14569/IJACSA.2019.0100754.

[54] Y. M. Kuo, F. Garcia-Herrero, O. Ruano, and J. A. Maestro, "RISC-V galois field ISA extension for non-binary error-correction codes and classical and post-quantum cryptography," *IEEE Trans. Comput.*, vol. 72, no. 3, pp. 682–692, 2023. doi: 10.1109/TC.2022.3174587.

[55] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *J. Cryptogr. Eng.*, vol. 8, pp. 141–184, 2018. doi: 10.1007/s13389-017-0160-y.

[56] M. E. Haque, S. Zobaed, M. U. Islam, and F. M. Areef, "Performance analysis of cryptographic algorithms for selecting better utilization on resource constraint devices," in *Proc. Int. Conf. Comput. Inf. Technol. (ICCIT)*, Dhaka, Bangladesh, 2018, pp. 1–6.

[57] U. Chibueze Nwamouh, B. O. Sadiq, K. U. John, and S. N. Ndubuisi, "A comparative analysis of symmetric cryptographic algorithm as a data security tool: A survey," *J. Sci. Technol. Res.*, vol. 5, no. 3, pp. 2023–2144, 2023. doi: 10.5281/zenodo.8313097.