DOI: 10.15849/IJASCA.221128.02

Int. J. Advance Soft Compu. Appl, Vol. 14, No. 3, November 2022
Print ISSN: 2710-1274, Online ISSN: 2074-8523

Performance Comparison of Xen AND Hyper-V in Cloud Computing While Using Cryptosystems

Waleed K. Abdulraheem

Department of Information and Network Security
World Islamic Sciences and Education University
e-mail: waleed.amin@wise.edu.jo

Abstract

Cloud computing is internet-distributed computing model transferring processes from personal computers or servers to cloud servers. Nowadays, security and performance of cloud computing is considered challenging for both users and cloud service providers. Securing data on cloud computing servers will ensures privacy, confidentiality, integrity, and availability. Using cryptographic techniques is one of the major methods to ensure the data security while storing and transmission. Hypervisor in a cloud is a software that provides abstraction and called virtual machine monitor. Hyper-V and Xen are two different types of hypervisors. In this paper, eight different types of cryptographic algorithms are deployed by using the two hypervisors with instances, to measure the hypervisors performance while encryption and decryption. CPU utilization and response time are measured while encryption and decryption are having different data types and sizes. Results show that Xen is better than Hyper-V in most results on average at 15% and 6.1% for time duration and CPU utilization respectively.

Keywords: *Cloud Computing, Virtualization, Hypervisors, Xen, Hyper-V, Cryptographic Algorithm*

1 Introduction

According to the National Institute of Standard and Technology (NIST), cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models [1].

The five essential characteristics of cloud computing are: on-demand self-services, broad network access, rapid elasticity, resource pooling, and measured service [2], while there are three types of cloud services, namely; Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [3]. Moreover, in terms of deployment there are four models, which are public, private, community and hybrid model [4], as shown in Fig 1 below.

Received 16 July 2022; Accepted 30 October 2022

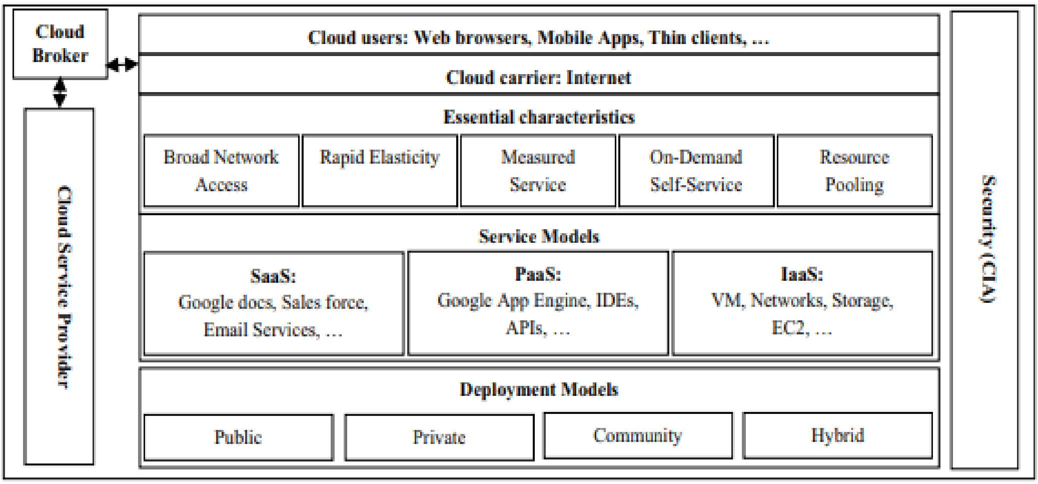

Fig 1: Definition of cloud computing architecture inspired by NIST

Virtualization is the key technology of cloud computing. It enables multiple logical resources to users on a single server through virtual machined and virtual networks. Virtualization technology provides the opportunity to improve hardware usage by increasing the number of functions that one server (machine) can handle for both organizations and users. Virtualization makes the control and management simpler, reduces the operational cost, and provides speedy disaster recovery [5].

Hypervisor is the most critical component of the virtualization since it provides the abstraction to the virtual machine. It controls the hardware resources and runs at the highest privilege level [6].

System virtualization can be classified as Type-I or Type-II hypervisor, where Type-I hypervisors run directly on the hardware (called bare metal), and Type-II hypervisors run on top of the host operating system [7].

As an example of Type-I are Citrix XenServer, NS Windows Hyper-V, Linux KVM, and VMWare ESXi. While Oracle VM Virual Box and VMware Workstation are examples of Type-II hypervisor. Practically, Type-I hypervisors are better choice than Type-II in terms of performance [8].

Security of cloud computing is the most critical aspect, since data exists in different locations around the world, with new threats are arising daily [9]. Data at rest in the cloud servers is vulnerable to misuse. As per recent survey conducted by Sky High, only 9.4% of cloud service providers CSP are encrypting data at rest. Hence, users do not realize who is revealing their data [10].

According to [11], there are three vector of attacks in cloud computing, namely; hypervisor, network, and hardware, which can be mapped to attacks in terms of internal, external, and CSP respectively.

Virtual machines can be accessed by attackers if they exploit hypervisor weak points, and then compromising confidentiality and integrity. Thus, hypervisor security is one of cloud service pillars [6].

The main potential contribution of this paper is to compare and analyze the performance of two common different hypervisors, XEN and Hyper-V while using eight different types of cryptographic algorithms. The performance are time duration and CPU consumption while using different data size, keys, and core numbers in encryption and decryption.

The remaining sections of the paper as distributed as follows: The related work is introduced in Section 2, while the suggested approach and the experimental design is in Section 3. Results are in Section 4, and finally conclusion and future works are presented in Section 5.

2 Related Work

In cloud computing, users store their data on the cloud which are means at remote location. It creates problems concerning security and trust, which are essential requirements for acceptability of cloud computing [12].

Cryptography is widely used in cloud computing to achieve more security and trusting. In [13], they suggest four-steps data security model in cloud computing. They combine three cryptographic algorithms, which are RSA, AES, and identity-based encryption alongside with steganography by using least significant bit LSB techniques. While in [12], they proposed a model combining between different symmetric and asymmetric algorithms, alongside with CAPTCHA and two factor authentication as in Fig 2 below.

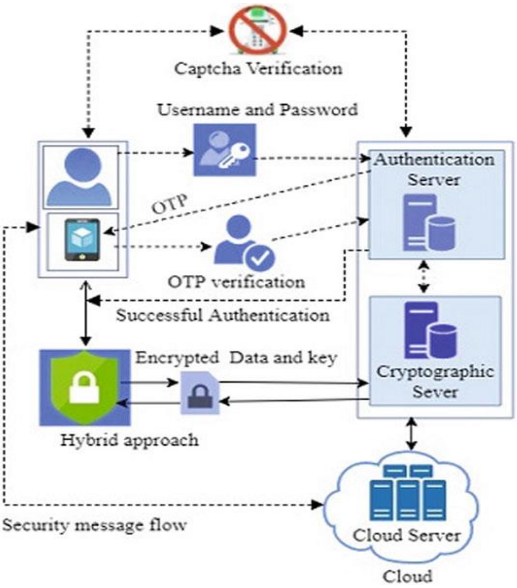

Fig 2: Framework in cloud environment

In [14], they used multifold techniques based on DNA as a symmetric cryptographic algorithm, where the user (client) encrypts data before it is uploaded to cloud servers. While in [15], they present a lightweight homomorphic cryptographic algorithms which contain two layers of encryption. The proposed approach offers features of symmetric and asymmetric cryptographic algorithms.

In [16], they proposed an apriori algorithm to improve the privacy of data while being encrypted. It is integrated with El-Gamal algorithm as an asymmetric which causes more data protection, query privacy, and hide data frequency. In [17], they introduced a security system for mobile cloud computing using hashing and symmetric parameter function as a biometric based authentication scheme to resist the impersonation. In [18], they proposed a hybrid cryptosystem to enable security in cloud computing. Their system includes 3DES as a symmetric for encryption, RSA as an asymmetric for authentication, and SHA-3 as a hash function for integrity. While in [19], they proposed hybrid multi stages data encryption architecture to secure data while transmitting in cloud computing and other communication based on internet technology. The system is hybrid of cryptography and steganography using one-time pad (OTP) and least significant bit (LSB) respectively.

In [20], they proposed a hybrid scheme for big data in cloud computing. The scheme which has three steps aims to restrict illegitimate users from accessing the cloud, while encryption, data access control, and illegal access are detected by using advanced encryption standards (AES), attribute-based access control (ABAC), and hybrid intrusion detection (HID) respectively.

In [21], they present a system for securing the multimedia data in the cloud computing. They started with data classification by using optimized convolutional neural network (CNN-EEO) based on data sensitivity, then they used infinite elliptic curve cryptography with Merkle hash digest algorithm (IECC-MHDA) to generate and encrypt a key pair, and finally they used Kernel Homomorphic chaos encryption algorithm (KHCEA) to encrypt the classified data. While in [22], they proposed a framework to secure and preserve healthcare data by using data hiding and restoration operations. They used a Gaussian mutation-based firebug optimization (GM-FBO) method for the generation of an optimal key as in Fig 3.

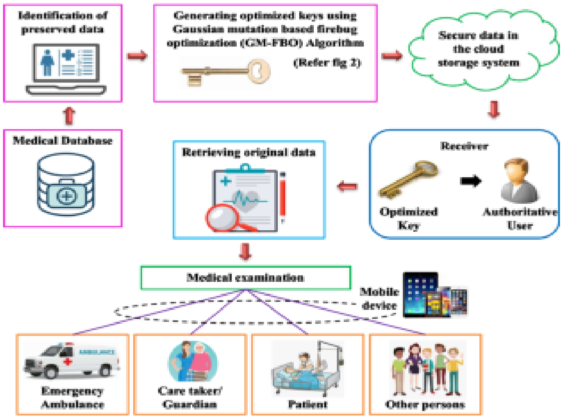

Fig 3: GM-FBO framework

In [23], they proposed a multi-tiered cryptography-based with a middleware interface for CSP by using authentication algorithms to encrypt the attached file and document. The proposed frame uses Blowfish and RSA/SRNN algorithms for both key and data and key encryption/decryption.

In [24], they proposed a model that includes variant of McEliece as quantum computing cryptosystem and the of N-th degree truncated polynomial ring units (NTRU) cryptosystem which are used to secure access control data and cloud user data respectively.

In [25], they proposed an approach to secure public cloud from unauthorized users. They used RSA cryptosystem in addition to Qusai modified levy flight distribution (QMLFD-RSA) approach. The system enhances the integrity of uploaded data in public cloud by using secured key generation. In [26], they proposed cryptosystem to secure the sensitive data located on multi-cloud environment which is created by integrated different public and private cloud. They used elliptic curve integrated encryption scheme (ECIES) which enable the user to encrypt the data before uploading it to the cloud, i.e., preventing CSP from accessing their data.

In [27], they proposed a cryptosystem to secure uploaded files on the cloud server. They used CHACHA20_POLY1305, AES-CCM, and AES-GCM asymmetric cryptographic algorithms. They split the file into N parts, and then encrypt each part by using different cryptographic algorithm. While in [28] they proposed a hybrid crypto system to secure data on the cloud. They used Blowfish for data encryption, RSA for secret key encryption, and Replace R as a steganography in RGB algorithm for more security.

In [29], they proposed a hybrid system to secure the cloud storage in a decentralized way. The system is combined between user’s iris to verify authenticity, a hybrid of cryptographic algorithms included AES, DES and CST to verify the confidentiality, and matrix code and blockchain to verify integrity. In [30], they proposed a system to secure pictures that stored on the cloud server. Their approach is based on cryptographic using deoxyribose nucleic acid (DNA) and chaotic logistic mapping encoding.

3 Problem Statement and the Proposed Approach

While different cryptosystem approach is introduced to secure the cloud computing, performance is considered a major component in it. Different cloud computing hypervisors are used while implementing cloud infrastructure to provide the virtuality, Xen and Hyper-V hypervisors are widely used therein. This study aims to evaluate the performance of the two hypervisors while encryption and decryption process for different data. Time duration in minute: second and CPU utilization in % are used. To achieve this goal, Fig 4 shows the proposed approach for this study.

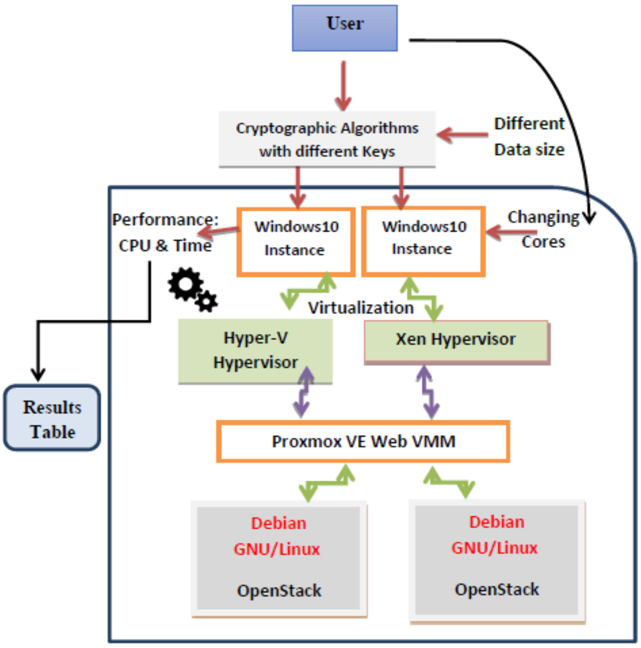

Fig 4: Study proposed approach

Two different cloud servers have been implemented to perform the experiment and extract the results as shown in Fig 4, one is using Hyper-V while the other uis sing Xen as two different hypervisors. From each, an instance virtual machine VM is implemented using Windows 10.

Eight different cryptographic algorithms are implemented on the instance. They are varied between symmetric and asymmetric, block and stream, etc. Which, BlowFish, TwoFish, DES, TripleDES, CAST-128, RC4, AES, and RSA. In the experiment, different key sizes, data sizes, and CPU core numbers are used to compare the results of time response and CPU utilization performance.

4 Result Analysis

For each algorithm, ten experiments are performed while changing key size, data size, and core numbers to measure time duration and CPU utilization.

BlowFish

BlowFish is a symmetric cryptographic algorithm that is frequently used to achieve security in cloud computing [31]. It is based on Feistel structure as a block cipher with 64-bit block size, and 32-448 bit of key size [32]. Table 1 shows the results of CPU utilization and time duration experiments while using BlowFish algorithm with two different hypervisors that have been implemented on two distinct servers while changing data, and core sizes. Moreover, it shall be noted that key size is 64-bit for all the experiments.

Table 1: Experimental Results of BlowFish

Hyp	Exp #	Core #	Size in Giga	Enc Time m.s	Dec Time m.s	Enc CPU %	Dec CPU %
Hyper-V	1	4	2	6.0	5.5	35	34
Xen				5.5	5.3	31	31
Hyper-V	2	4	3	7.4	7.3	36	36
Xen				7.1	6.5	32	32
Hyper-V	3	2	3	7.5	7.4	66	67
Xen				7.3	7.3	60	61
Hyper-V	4	2	2	6.1	5.5	64	64
Xen				5.5	5.3	59	61
Hyper-V	5	2	5	14.3	14.1	67	67
Xen				13.3	13.1	61	61
Hyper-V	6	2	1.3	5.2	3.4	66	67
-Xen				4.2	3.3	59	60
Hyper-V	7	2	0.8	2.2	2.1	66	67
Xen				2.1	2	60	60
Hyper-V	8	4	5	14.5	14.5	34	36
Xen				12.4	12.3	32	33
Hyper-V	9	4	1.3	4.1	4	36	37
Xen				3.4	3.2	33	33
Hyper-V	10	4	0.8	2.2	2.2	35	37
Xen				2	2	31	32

Whereas: Hyp is a hypervisor type; experiment # is experiment number; enc/dec time is encryption/decryption duration in minutes and seconds; and enc/dec CPU % is the utilization percentage of CPU while encryption and decryption.

In order to understand Table 1, for example in experiment number 1, the core is 4, the size of the file is 2 gigabytes, and then followed by time duration and CPU utilization for both Hyper-V and Xen hypervisors.

For this cryptographic algorithm and for the rest of results, an abbreviation table will show the average results for the time duration and CPU utilization while encryption and decryption as in Table 2.

Table 2: Average Results of BlowFish

BlowFish	**Time Duration m.s**		**CPU Utilization %**	
	Encrypt	Decrypt	Encrypt	Decrypt
Hyper-V	6.5	6.2	50.5	51.2
Xen	6.3	6.0	45.8	46.4
Variation	0.2	0.2	4.7	4.8

According to Table 2, the average experiment results of the BlowFish cryptographic algorithm show that Xen hypervisor is better that Hyper-V hypervisor in terms of time duration and CPU utilization while encryption and decryption.

TwoFish

TwoFish is a symmetric cryptographic algorithm, it follows the BlowFish algorithm with 128-bit block size and key size up to 256 using 16 rounds [29]. TwoFish is used for both hardware and software context as well as to secure cloud computing [33].

Table 3: Average Results of TwoFish

TwoFish	**Time Duration m.s**		**CPU Utilization %**	
	Encrypt	Decrypt	Encrypt	Decrypt
Hyper-V	6.1	6.0	51.5	50.9
Xen	5.5	5.4	45.8	46.2
Variation	0.2	0.2	5.7	4.7

As shown in Table 3, the average experiment results of the TwoFish cryptographic algorithm show that Xen hypervisor is better that Hyper-V hypervisor in terms of time duration and CPU utilization while encryption and decryption.

DES

Data encryption standard DES is a symmetric cryptographic algorithm uses Fiestel structure with 64-bit for both block and key size [14]. Different models are proposed to secure cloud computing using DES algorithm as in [34].

Table 4: Average Results of DES

DES	**Time Duration m.s**		**CPU Utilization %**	
	Encrypt	Decrypt	Encrypt	Decrypt
Hyper-V	7.2	6.5	50.9	49.1
Xen	7	6.3	49.3	49.1
Variation	0.2	0.2	1.6	0

Table 4 shows that Xen hypervisor is also better that Hyper-V hypervisor in term of time duration for time duration and CPU utilization while encryption. However, the result is the same at CPU while decryption process.

TripleDES

Triple DES or TDES or 3DES is a replacement of the traditional DES but with 112-bit or 192-bit key size and more encryption/decryption stages. It is a symmetric algorithm using block cipher method [35]. 3DES also are widely used to secure the cloud computing as well as in different models and hybrid algorithms as used in [18] and [36].

Table 5: Average Results of TDES

TDES	**Time Duration m.s**		**CPU Utilization %**	
	Encrypt	Decrypt	Encrypt	Decrypt
Hyper-V	13.2	13.1	53.4	54.1
Xen	12.5	12.4	50.4	50.1
Variation	0.3	0.3	3.0	3.0

According to Table 5, there is stable difference between the two hypervisors with advantages to Xen, with 0.7 and 3.0 for time duration and CPU utilization respectively while encryption and decryption.

CAST-128

CAST-128 cryptographic algorithm is a symmetric block cipher based on Feistel structure with 16 round with 64-bit block size and up to 128 key size. It is used in many technical applications such in [37] and in cloud as better option than DES algorithm as in [38] and [39].

Table 6: Average Results of CAST-128

CAST-128	**Time Duration m.s**		**CPU Utilization %**	
	Encrypt	Decrypt	Encrypt	Decrypt
Hyper-V	2.3	2.4	50.2	49.8
Xen	2.1	2.0	46.8	44.8
Variation	0.2	0.4	3.4	5

Table 6 shows advantage for Xen hypervisor for both time duration and CPU utilization with more variation while decryption process than encryption.

RC4

Rivest cipher 4 or ARCFOUR (alleged RC4) is a symmetric cryptographic algorithm. It is most well-known stream cipher algorithm, with key size up to 2048 bit and was used in many applications such in securing socket layer/transport layer security (SSL/TLS) standards and other applications [40] and [41].

Table 7: Average Results of RC4

RC4	**Time Duration m.s**		**CPU Utilization %**	
	Encrypt	Decrypt	Encrypt	Decrypt
Hyper-V	4.0	4.0	48.5	48.6
Xen	3.1	3.1	45.7	43.9
Variation	0.5	0.5	2.8	4.7

In Table 7, Xen has better performance than Hyper-V hypervisor in terms of time duration and CPU utilization while encryption and decryption.

AES

Advanced Encryption Standard (AES) is a symmetric key algorithm has a great performance and acceleration among symmetric cryptosystem. Depending on key sizes, AES goes through 10, 12, and 14 round in case of key size 128, 192, and 256 bit size respectively [42]. To get more security in cloud computing, AES cryptosystem is implemented with other algorithms such as in [27] and [43].

Table 8: Average Results of AES

AES	**Time Duration m.s**		**CPU Utilization %**	
	Encrypt	Decrypt	Encrypt	Decrypt
Hyper-V	4.5	5.1	41.7	42.3
Xen	3.5	3.5	44.2	47.8
Variation	1.0	1.2	-2.5	-4.5

It is noticed that CPU utilization in Hyper-V hypervisor is better than Xen hypervisor, while in time duration Xen is proven to be better as shown in Table 8.

RSA

In 1977, Rivest, Shamir, and Adleman described RSA cryptosystem as secured asymmetric algorithm, which used public and private keys. In RSA, two very large prime numbers are easily multiplied. However, it is very difficult and requires considerable time duration to factorize them [44]. As asymmetric cryptosystem, RSA is the most algorithm used with other cryptosystem, such as in [25] and [45]

Table 9: Average Results of RSA

RSA	**Time Duration m.s**		**CPU Utilization %**	
	Encrypt	Decrypt	Encrypt	Decrypt
Hyper-V	26.3	25.3	75.7	73.8
Xen	22.5	21.4	69.5	68
Variation	3.4	3.5	6.2	5.8

In Table 8, Xen hypervisor has better performance than Hyper-V with big variation while encryption and decryption in terms of time duration and CPU utilization.

Total Average Results

The aggregation average of all algorithms is shown in Table 10.

Table 10: Total Average of All Algorithms

Total Average	**Time Duration m.s**		**CPU Utilization %**	
	Encrypt	Decrypt	Encrypt	Decrypt
Hyper-V	8.5	8.4	52.8	52.5
Xen	7.4	7.3	49.7	49.5
Variation	1.1	1.1	3.1	3.0
Ratio	14.9%	15%	6.2%	6.0%

Formula 1 is used to calculate the average ration of all algorithms while encryption and decryption concerning time duration and CPU utilization performance.

$$Average\ Ration = \frac{Variation}{Average\ Xen}\ X\ 100\% \tag{1}$$

The total variation results show that Xen hypervisors is better than Hyper-V with average 14.9% while encryption and 15% while decryption in terms of time duration. Meanwhile, 6.2% while encryption and 6% while decryption in terms of CPU utilization.

5 Conclusion

Security is considered major concern in cloud computing. Using cryptographic algorithms with a hybrid cryptosystem and other security techniques such as authentication and authorization will increase cloud security. This study concluded that using different cryptographic in Xen hypervisors while encryption has more performance than Hyper-V hypervisors, which is compatible with the literature such in [46] and [2]. The overall results show that Xen is better than Hyper-V with average 15% in terms of time duration, and 6.1% in terms of CPU utilization. In AES algorithm, Hyper-V is better than Xen in terms of CPU utilization, but not in time duration. In terms of CPU utilization, the biggest variation was RSA cryptosystem with advantages to Xen, while in terms of CPU utilization, the biggest ratio variation was in AES algorithm with advantage to Xen as well. it is recommended to use Xen hypervisor than Hyper-V hypervisor for more performance while using the variety cryptographic algorithms.

This study can be improved by adding more hypervisors such as Exsi, VMware and KVM with more cryptographic algorithms and cryptosystem types such as hashing algorithms, quantum cryptography and different type of steganography in the future works.

References

[1] Peter Mell, T.G. (2011) The NIST Definition of Cloud Computing. 1–3.

[2] Abdulraheem, W.K.A. (2014) Comparative Analysis of the Performance for Cloud Computing Hypervisors with Encrypted Algorithms, 2014.

[3] Chyad, H.S., Mustafa, R.A., and George, D.N. (2022) Cloud resources modelling using smart cloud management. *Bulletin of Electrical Engineering and Informatics*. 11 (2), 1134–1142.

[4] El Kafhali, S., El Mir, I., and Hanini, M. (2022) Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing. *Archives of Computational Methods in Engineering*. 29 (1), 223–246.

[5] Abu-Alhaija, M., Turab, N.M., and Hamza, A.R. (2022) Extensive study of cloud computing technologies, threats and solutions prospective. *Computer Systems Science and Engineering*. 41 (1), 225–240.

[6] Katz, A.C.R.C.J. (2022) Cloud Computing Security: Foundations and Research Directions. .

[7] Thamsen, L., Beilharz, J., Polze, A., and Kao, O. (2022) The Methods of Cloud Computing 1 Introduction. .

[8] Djordjevic, B., Timcenko, V., Kraljevic, N., and Macek, N. (2021) File System Performance Comparison in Full Hardware Virtualization with ESXi, KVM, Hyper-V and Xen Hypervisors. *Advances in Electrical and Computer Engineering*. 21 (3),

109–110.

[9] Sharma, R., Gourisaria, M. K., & Patra, S.S. (2021) Cloud Computing—Security, Issues, and Solutions. in: Commun. Softw. Networks, pp. 687–700.

[10] Panda, D. R., Behera, S. K., & Jena, D. (2021) A Survey on Cloud Computing Security Issues, Attacks and Countermeasures. in: Adv. Mach. Learn. Comput. Intell., pp. 513–524.

[11] Ramachandra, G., Iftikhar, M., and Khan, F.A. (2017) A Comprehensive Survey on Security in Cloud Computing. *Procedia Computer Science*. 110 (2012), 465–472.

[12] Manoj Tyagi, Manish Manoria, and B.M. (2021) Implementation of Cryptographic Approaches in Proposed Secure Framework in Cloud Environment. *Intelligent Computing and Applications, Springer, Singapore.* 1172 419–426.

[13] Adee, R. and Mouratidis, H. (2022) A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. *Sensors*. 22 (3), 1–23.

[14] Sohal, M. and Sharma, S. (2022) BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. *Journal of King Saud University - Computer and Information Sciences*. 34 (1), 1417–1425.

[15] Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G.H., and Jagtap, S. (2022) A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. *International Journal of Intelligent Networks*. 3 (April), 16–30.

[16] Mustafa, R.A., Chyad, H.S., and Mutar, J.R. (2022) Enhancement in privacy preservation in cloud computing using apriori algorithm. *Indonesian Journal of Electrical Engineering and Computer Science*. 26 (3), 1747.

[17] Lu, Y. and Zhao, D. (2022) Providing impersonation resistance for biometric-based authentication scheme in mobile cloud computing service. *Computer Communications*. 182 (January), 22–30.

[18] Kolawole Damilare Abel, Sanjay Misra, Oluranti Jonathan, Akshat Agrawal, R.M.& R.D. (2022) Data Security in Cloud Computing Using a Hybrid Algorithm Approach. in: Comput. Intell. Mach. Learn. Springer, Singapore., pp. 467–474.

[19] Osman, O.M., Kanona, M.E.A., Hassan, M.K., Elkhair, A.A.E., and Mohamed, K.S. (2022) Hybrid multistage framework for data manipulation by combining cryptography and steganography. *Bulletin of Electrical Engineering and Informatics*. 11 (1), 327–335.

[20] Razaque, A., Shaldanbayeva, N., Alotaibi, B., Alotaibi, M., Murat, A., & Alotaibi, A. (2022) Big Data Handling Approach for Unauthorized Cloud Computing Access. *Electronics*. 11 (1), 131.

[21] Swetha, G. and Janaki, K. (2022) Cloud based secure multimedia medical data using optimized convolutional neural network and cryptography mechanism. *Multimedia Tools and Applications*. 1–37.

[22] Anand, K., Vijayaraj, A., and Vijay Anand, M. (2022) Privacy preserving framework using Gaussian mutation based firebug optimization in cloud computing. *Journal of Supercomputing*. 78 (7), 9414–9437.

[23] Kumari, N. and Malhotra, P.V. (2022) Secure Cloud Data Storage Using Hybrid Cryptography. *International Journal for Research in Applied Science and Engineering Technology*. 10 (4), 60–63.

[24] Ukwuoma, H.C., Arome, G., Thompson, A., and Alese, B.K. (2022) Post-quantum cryptography-driven security framework for cloud computing. *Open Computer*

Science. 12 (1), 142–153.

[25] Kaliyamoorthy, P. and Ramalingam, A.C. (2022) QMLFD Based RSA Cryptosystem for Enhancing Data Security in Public Cloud Storage System. *Wireless Personal Communications*. 122 (1), 755–782.

[26] Latha, V.L.P., Reddy, N.S., and Babu, A.S. (2022) Modified Intelligent Elliptic Curve Cryptography Algorithm To Mitigate Security Concerns of Big Data Storage in Multi-Cloud Environment. *Journal of Tianjin University Science and Technology*. 22 (03), 385–400.

[27] Garad, A., Agrawal, R., Suryawanshi, A., and Rodagi, J. (2022) SECURING FILE STORAGE IN CLOUD USING HYBRID. *International Journal of Advances in Engineering Research*. 23 (5), 44–50.

[28] Kolawole Damilare Abel, Sanjay Misra, Akshat Agrawal, R.M.& R.D. (2022) Data Security Using Cryptography and Steganography Technique on the Cloud. in: Comput. Intell. Mach. Learn., pp. 475–481.

[29] Neela, K.L. and Ramesh, R.K. (2022) A Hybrid Cryptography Technique with Blockchain for Data Integrity and Confidentiality in Cloud Computing. in: Cloud Comput. Enabled Big-Data Anal. Wirel. Ad-Hoc Networks, pp. 15-29 CRC Press.

[30] Elminaam, D.S.A., Mousa, M.A.W., and El Fattah, M.A. (2022) Secure Data Storage in the Cloud by Using DNA and Chaos Cryptography. in: MIUCC 2022 - 2nd Int. Mobile, Intelligent, Ubiquitous Comput. Conf., IEEE, pp. 175–182.

[31] Ghanmi, H., Hajlaoui, N., Touati, H., Hadded, M., and Muhlethaler, P. (2022) A Secure Data Storage in Multi-cloud Architecture Using Blowfish Encryption Algorithm. in: Int. Conf. Adv. Inf. Netw. Appl., pp. 398–408.

[32] Abdul, R., Abdul, H., and Al-wattar, A.H.S. (2021) A New Blowfish Using A Neural Network Research Article. *Turkish Journal of Computer and Mathematics Education*. 12 (7), 1546–1554.

[33] Utkarsha Kulkarni, Rosemeen Mansuri, R.A. (2022) File Storage on Cloud Using Cryptography. *International Journal for Research in Applied Science & Engineering Technology*. 10 (5), 1949–1953.

[34] Pankaj Balu Regade, Ajinkya Ashok Patil, Shubham Sambhaji Koli, Rahul Balu Gokavi, P.M.S.B. (2022) SURVEY ON SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY. *International Research Journal of Modernization in Engineering Technology and Science*. 4 (6), 170–177.

[35] Jammula, M. (2022) Comparative Study on DES and Triple DES Algorithms and Proposal of a New Algorithm Named Ternary DES for Digital Payments. *Asian Journal of Applied Science and Technology*. 06 (01), 89–98.

[36] Subathra, S., A, M.B., Sangavi, J., and Shrimathi, S. (2022) A PROFICIENT PRIVACY PROTECTION METHOD FOR CLOUD COMPUTING. *International Research Journal of Modernization in Engineering Technology and Science*. 04 (05), 4264–4267.

[37] Naser, E. F., Khudir, E. T., Mazher, A.N. (2022) Comparison between RSA and CAST-128 with Adaptive Key for Video Frames Encryption with Highest Average Entropy. *Baghdad Science Journal*. (May), 1378–1386.

[38] AbdElminaam, D., badr, alsayed, and Abdullah Ibrahim, M. (2022) FHE-Chaos NHCP: Developing a Novel Secure Framework for Cloud Computing Environment. *Journal of Computing and Communication*. 1 (1), 12–26.

[39] KAMDAR, H. (2022) EXPLORING THE SECURITY OF DATA IN THE CLOUD USING ENCRYPTION, 2022.

[40] Rizk-Allah, R.M., Abdulkader, H., Elatif, S.S.A., Elkilani, W.S., Al Maghayreh, E., Dhahri, H., et al. (2022) A Novel Binary Hybrid PSO-EO Algorithm for Cryptanalysis of Internal State of RC4 Cipher. *Sensors*. 22 (10), 3844.

[41] Kannan, M., Kumar, K. S., R. (2019) AN ILLUSTRATIVE REVIEWS ON CRYPTOGRAPHIC ALGORITHMS USED IN NETWORKING APPLICATIONS FOR. *International Journal of Computer Engineering and Technology*. 10 (4), 61–71.

[42] Masese Chuma Benard, Muhaise Hussein, Turiabe Victor, J.S.C. (2022) A review on data security issues and mechanisms in cloud computing. *International Journal of Research and Scientific Innovation*. 9 (6), 12–16.

[43] Varma, V., Patil, M., Patil, S., Patil, M., and Kadam, A. (2022) Data Storage Security in Cloud Computing Using AES Algorithm and MD5 Algorithm. *International Journal for Research in Applied Science and Engineering Technology*. 10 (5), 5052–5055.

[44] Sajid, F., Hassan, M.A., Khan, A.A., Rizwan, M., Kryvinska, N., Vincent, K., et al. (2022) Secure and Efficient Data Storage Operations by Using Intelligent Classification Technique and RSA Algorithm in IoT-Based Cloud Computing. *Scientific Programming*. 2022 1–10.

[45] Osman, F.A., Hashem, M.Y.M., and Eltokhy, M.A.R. (2022) Secured cloud SCADA system implementation for industrial applications. *Multimedia Tools and Applications*. 81 (7), 9989–10005.

[46] Akash, B., Anupam Bhatia, and Gurjeetsingh Bhattal (2016) A comparative study of Various Hypervisors Performance. *International Journal of Scientific & Engineering Research*. 7 (12), 65–71.

About Researcher

Dr. WALEED ABDULRAHEEM has received his B.S degree in computer and network from AOU Jordan, in 2012, M.S degree in computer and information security from MEU Jordan, in 2014, and Ph.D. in Cybersecurity from UPM Malaysia in 2019. He is currently an Assistant Professor with WISE University. His research interests are cryptography, IoT security, and cloud security.