Hindawi
Security and Communication Networks
Volume 2023, Article ID 9826393, 1 page
https://doi.org/10.1155/2023/9826393

Retraction

Retracted: Design and Implementation of Cloud Computing Network Security Virtual Computing and Defense Technology

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Cheng, "Design and Implementation of Cloud Computing Network Security Virtual Computing and Defense Technology," *Security and Communication Networks*, vol. 2022, Article ID 7876199, 7 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 7876199, 7 pages
https://doi.org/10.1155/2022/7876199

Research Article

Design and Implementation of Cloud Computing Network Security Virtual Computing and Defense Technology

Yongbing Cheng

Electronic Information Department, Xinxiang Vocational and Technical College, Xinxiang, Henan 453000, China

Correspondence should be addressed to Yongbing Cheng; 1710711222@hbut.edu.cn

Received 29 June 2022; Revised 8 August 2022; Accepted 16 August 2022; Published 30 August 2022

Academic Editor: C. Venkatesan

In order to improve the defense effect in network security, a research and implementation method of cloud computing network security virtual computing and defense technology is proposed. This architecture makes full use of the structural advantages of the virtualized environment, which can realize the trusted measurement of the user's virtual machine in a more reliable way and can support the user's diverse authentication requests. This paper introduces the concept of cloud computing, the classification of cloud computing, and the characteristics of cloud computing network security. In the case of fully considering the coupling relationship between the physical network and the logical network, the topology of the cloud computing network is established, and based on the network topology, the relevant network theory is used to analyze the cloud computing network. The avalanche failure under the computing network is studied. The research results show that the relative performance under different trusted measurement periods can reach more than 97%, which can flexibly meet the needs of user trusted authentication and can effectively provide trusted protection for user virtual machines. Adding additional protection measures to some special nodes in the cloud computing network topology to ensure that they are not damaged when attacked can greatly improve the robustness of the entire cloud computing network topology, therby ensuring that the network can avoid the attack. A large area will not be paralyzed due to the avalanche effect, and at the same time, the function and topology of the network itself have not changed. This method can effectively improve the security protection effect in network security.

1. Introduction

With the continuous development of Internet computer technology, cloud computing technology is widely used in various fields and industries and has developed into an indispensable technical guarantee in modern society. Even in people's daily life, it is inseparable from cloud computing technology. Cloud computing technology has brought a great impact to the society, but the subsequent cloud computing technology has also brought some threats and challenges to Internet security. These threats hinder the development of cloud computing technology to a great extent. Therefore, it is very important to improve network security under cloud computing [1]. After the rise of SDN, the security of virtual network has changed a little. How to isolate the network in traditional virtual network is a complex problem. Many security problems will appear on the isolation problem, as shown in Figure 1. Control and data are separated in SDN. The isolation of the network is controlled in the controller, and the switch only executes the instructions of the controller. This centralized control mode makes the network have a good, flexible, and dynamic isolation scheme. Therefore, SDN is relatively less affected by network isolation. Even if the isolation problem in SDN is relatively easy to solve, it cannot be taken lightly. Every node in the network may become the target of the attacker. If the attacker obtains the authority of the controller by controlling a node in the network, it will bring great security risks [2]. Because of the characteristics of SDN centralized control, the safety of SDN controller needs more attention. The controller is responsible for the operation logic of the whole network and the data transmission with the upper application and the lower switch. If the attacker attacks the controller by forging data packets and the controller replies

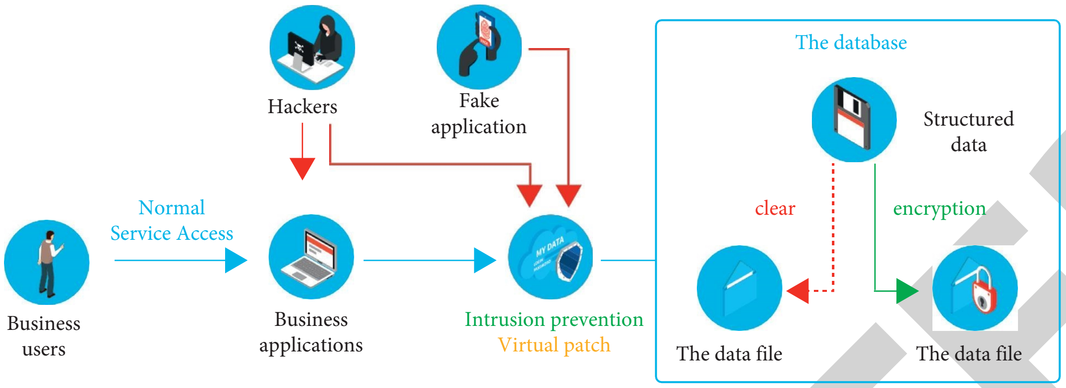

Figure 1: Secure virtual computing and protection.

to the attack message, the attacker can obtain the sensitive information of the controller, so as to bypass the security monitoring to attack the network. With the development of the Internet, DDoS attacks are increasing. If the controller is attacked by DDoS, it will not be able to handle the normal network traffic, and the whole network will be paralyzed, which makes the loss difficult to estimate. This paper analyzes and studies the network security protection under cloud computing technology, and this research is of great significance to the development of cloud computing technology [3].

2. Literature Review

With the continuous popularization of cloud computing services, the security of cloud computing has attracted more and more attention. Many organizations and topics have studied it at home and abroad. In foreign countries, many standardization organizations have begun to formulate cloud computing security-related standards.These organizations include the Cloud Security Alliance CSA ,Structured Information Standards Promotion organization OASIS, and the International Telecommunication Union ITU-TSG17 Study Group. In addition, the international computer society ACM has set up a symposium on cloud computing security and its research. The famous international conference on information security RSA has also taken cloud computing security as an important research topic [4]. In academic circles, the research on cloud computing security issues and technologies has been widely carried out, and some progress has been made. In terms of data security, the solution to the security problem mainly lies in how to encrypt the data and how to safely extract the encrypted data. The former focuses on encryption technology, while the latter mainly uses ciphertext search technology. In the field of encryption technology, Khaliq and others have made contributions. They have successfully constructed a fully dynamic encryption technology by using the methods of ideal lattice and integer arithmetic, which ensures data security [5]. Aiming at the shortcomings of virtual machine trusted authentication technology in the existing cloud computing environment, this paper proposes a dynamic trusted authentication architecture DIMA according to the users' trusted and security requirements for virtual machines. Making full use of the structural advantages of virtualization environment, we can realize the trusted measurement of users' virtual machines in a more reliable way, support users' diversified authentication requests, and improve the security protection effect in network security.

3. Research Methods

3.1. Cloud Virtual Machine Dynamic Trusted Authentication Architecture (DIMA).

In order to enable cloud service providers to provide users with a set of trusted authentication scheme that can meet the above requirements at the same time, this paper proposes a cloud virtual machine dynamic trusted authentication architecture—DIMA (Dynamic Integrity Measurement and Attestation). The architecture adopts the virtual machine introspection technology based on virtualization technology to monitor the user's virtual machine and dynamically collect integrity evidence according to the user's trusted authentication request [6]. Due to the adoption of virtual machine introspection technology, DIMA can collect trusted evidence outside the user's virtual machine and realize the isolation between the authentication system and the target system. Therefore, malicious attackers in the virtual machine cannot interfere with or bypass the authentication system. In addition, DIMA's trusted authentication system can flexibly generate corresponding trusted measurement rules according to the user's authentication request for virtual machine security and can measure the security of virtual machine system in different aspects. Finally, DIMA also designs a set of efficient trusted verification mechanism to solve the problem that the architecture design of extraterritorial measurement may cause performance load to the management domain and cloud computing platform. This mechanism skillfully uses hash-based signature technology to effectively reduce the additional load of cloud platform in trusted measurement, improve the efficiency of verification, and reduce the possibility of verification system being attacked by potential malicious users [7].

3.2. Mitigation Mechanism of Credible Measurement.

On the basis of providing users with trusted authentication services, a set of mitigation mechanism is designed for DIMA architecture, which can implement corresponding mitigation measures for different situations in which the integrity of users' virtual machines is damaged, so as to help users stop attacks in time and protect users' data and application security to the greatest extent [8]. According to the different security requirements of users for virtual machines or this specific service, DIMA currently sets two types of mitigation mechanisms: virtual machine level mitigation mechanism and system mitigation mechanism. These two mitigation mechanisms deal with the potential malicious destruction from two different kinds of granularity, so as to ensure the security and the stable operation of the user system.

The virtual machine level mitigation mechanism is a coarse-grained response measure that takes the user's target virtual machine as the object. Such measures are mainly aimed at the situation where the harm is serious and users have high security requirements for the virtual machine environment. Using this mitigation mechanism will have a certain impact on the normal operation of the virtual machine system, resulting in its performance degradation. Therefore, the conditions for using such measures are relatively strict. At present, this kind of mitigation mechanism mainly includes three measures: termination of operation, temporary suspension, and migration [9].

The mitigation mechanism in the system is a fine-grained response measure aiming at the specific objects in the virtual machine system. Such measures are mainly applied when users have high requirements for the continuity of virtual machine operation, so it is not easy to terminate the normal operation of the whole virtual machine. According to the security requirements put forward by users, only the objects in the system such as files, processes, and network connections with hazards are processed [10]. At present, this kind of mitigation mechanism is mainly aimed at process level processing. Through damaged files, malicious network connections, and system objects with damaged integrity, find the process accessing these objects and then close the process.

3.3. Remote Authentication Protocol. In view of the limitations of the existing remote authentication protocol in DIMA architecture, this section specifically aims at the structural characteristics and security requirements of DIMA architecture and designs the remote authentication protocol of DIMA architecture based on hash signature technology, so that the protocol can meet the requirements of security and efficiency at the same time [11]. In the remote authentication protocol designed in this section, there are three participants:

(1) Virtual machine user (*T*): the virtual machine user is the challenger or verifier in the authentication protocol to initiate a trusted authentication request to the remote virtual machine system. Different from the classical remote authentication protocol, in the application scenario designed by DIMA, there is no explicit distinction between the challenger and the verifier, and the virtual machine user plays this role.

(2) Prover (*P*): it responds to the tenant's authentication request and proves the result of trusted measurement to the user through trusted measurement and authentication.

(3) Certificate authority (PCA): the private certificate authority (PCA) is a trusted third party that authorizes and guarantees the verification key technology.

Considering the characteristics of multi-tenancy and multi-requirements on the cloud platform and the limitations of OTS scheme signature, the verification protocol proposed in this section is implemented based on XMSS multiple signature scheme, and WOTS+ is used as the implementation method of single signature. In this protocol, in order to be more compatible with the existing trusted platform, hash-based signature technology is only applied to the signature authentication of trusted evidence, and other identity authentication processes are implemented based on the existing public key cryptosystem [12]. In order to facilitate the description of the protocol, the description of symbols used in the protocol is listed in Table 1.

Before the implementation of the agreement designed in this section, we made some basic assumptions for each participant to ensure the correct implementation of the agreement. First, each participant has a unique key pair used to prove identity. The key pair is based on the traditional public key cryptosystem and the public key is broadcast by the authority [13]. Secondly, in the DIMA architecture, the virtual machine user *T* and the certifier *P* of the cloud service platform fully trust the certificate authority (PCA). Finally, the private key used for trusted verification is protected by the platform security storage mechanism, so it will not be stolen by the attacker. The protocol execution process for trusted authentication of DIMA architecture is generally divided into two parts [14]. The first part is the process of authenticating a new user when he first initiates an authentication request and generating a key for trusted authentication through PCA. The second part is the process of responding to the user's trusted confirmation and feeding back the trusted report. The main purpose of the first step is to generate the key pair confirmed by the user for the user with the assistance of the certificate authority PCA and distribute the public key part to the user [15]. For XMSS signature algorithm, its public key is a string with a length of N bits, which is aggregated by multiple WOTS + public keys according to formula (1). The first leaf of the XML tree + node is called the signature of the first leaf of the XML tree + node. When the height of XMSS public key tree is set to *h*, the generated key contains 2^{H} WOTS + key pairs, which can complete 2^{H} signatures and authentication.

$$\mathrm{NODE}_{i,j} = h_K \left\| \left(\mathrm{NODE}_{2i,j-1} \oplus b_{l,j} \right) \right\| \left\| \left(\mathrm{NODE}_{2i+1,j-1} \oplus b_{r,j} \right) \right\|. \tag{1}$$

In each trusted authentication report, the format of the confirmation signature received by the virtual machine user is Sig = (id, σ, Auth), where id $(0 < i < 2^{H} - 1)$ is the number index of the WOTS + key pair used for this signature, σ is a

Table 1: Description of symbols in remote authentication protocol based on hash signature technology.

Symbol	Meaning
$(M)_K$	Symmetric key K to encrypt M
$[M]_{\text{SK}}$	Private key K to perform asymmetric cryptographic operation on M
$\{M\}_{\text{PK}}$	Asymmetric cryptographic operation on m using public key K
$\|\|$	Connection operation
K	Session key
PK	Asymmetric cryptographic public key
SK	Asymmetric password private key
APK	Public key for user trusted authentication (for hash-based signature)
ASK	Private key for trusted authentication (for hash signature-based authentication)
X_{id}	Identification of parameter x in trusted verification
α, β, γ	The protocol is used to protect the signature of message integrity
N_i	Random number used in protocol session

signature based on the WOTS + algorithm, and E is the authentication path in the XMSS tree. Its function is to assist the signature authenticator to verify the validity of the signature through the XMSS public key. Taking WOTS + key pair as an example, if the private key in the corresponding L-Tree is used for signature, the authentication path used to authenticate the signature is the path represented by the circle.

In various aggregation methods based on Merkel tree, authentication path is needed. At present, there are many alternative schemes for computing authentication path. In the DIMA architecture proposed in this paper, we adopt the method proposed in [16] because this method can well balance and optimize the computing overhead and storage overhead and is very suitable for the scenario of trusted verification of multi-tenant virtual machines in DIMA architecture. When the virtual machine user receives the trusted evidence sent by the certifier and the above evidence signature, he needs to confirm the content of the trusted evidence according to his existing public key. Because the signature algorithm XMSS of MTS is used in the trusted verification designed by us, its verification process is different from the verification method based on the signature of public key cryptosystem. Virtual machine users first need to calculate the verification public key PK of a signature according to the verification data and signature they get and then construct an XMSS public key APK according to PK and authentication path Auth. If the APK exactly matches the public key APK distributed by the verifier before, the user confirms that the signature of the verifier is valid; otherwise, the verification fails.

In the authentication protocol of DIMA architecture, in order to prevent replay attack, the certifier will maintain a local database that records the random numbers attached to all received authentication requests. After receiving a new request message, the certifier will first check whether the random number carried by the request exists in the database [17]. If it does not exist, the certifier will add the random number to the local database and accept the verification request; if it exists, he will reject the authentication request, clear the existing connection information of the user, and wait for the next request to reestablish a new secure connection [18].

4. Result Analysis

Although using DIMA architecture to implement trusted verification on the security of user virtual machines can effectively ensure the security of user virtual machines, DIMA framework will bring performance overhead in the process of trusted measurement, which will have a certain impact on the system performance of virtual machines. In order to test the practicability of DIMA, this section evaluates the performance impact of runtime DIMA architecture on the virtual machine system. During the operation of the virtual machine, the user can initiate a trusted authentication request at any time and can also require the certifier to regularly feed back the reliability measurement results. Therefore, different request cycles will lead to different frequencies of credibility measurement [19]. In order to test the performance impact of the virtual machine under different trusted measurement frequencies, we run different benchmark test sets in the virtual machine and initiate periodic trusted authentication requests through users at different frequencies. In this section, the PALMS Cloud test program from the PALMS Cloud platform benchmark set was used. Each benchmark program has been tested many times under different credible measurement cycles. Figure 2 shows the performance impact of DIMA architecture on different benchmark programs under different trusted measurement cycles. The label base represents the performance of the benchmark program when there is no credible measurement, and the test results under other conditions are used as the benchmark to obtain the relative performance [20]. From the test results in Figure 2, it can be seen that the implementation of trusted measurement by DIMA at run time will affect the performance of benchmark programs, and the impact on the performance of different benchmark programs is different. Among them, the performance impact of CPU and memory is relatively small, and the relative performance can reach more than 97% under different trusted measurement cycles. This is mainly because the running time of the micro-benchmark is relatively short, and the DIMA-trusted measurement cycle involved is less, so the performance impact can be almost ignored [21]. In comparison, the three macro-benchmark programs, database, web, and app, are greatly affected by the performance,

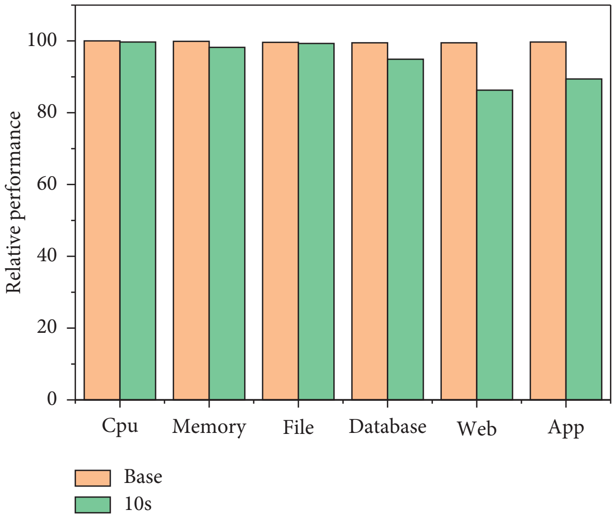

Figure 2: Impact of DIMA runtime reliability on the performance of benchmark test set.

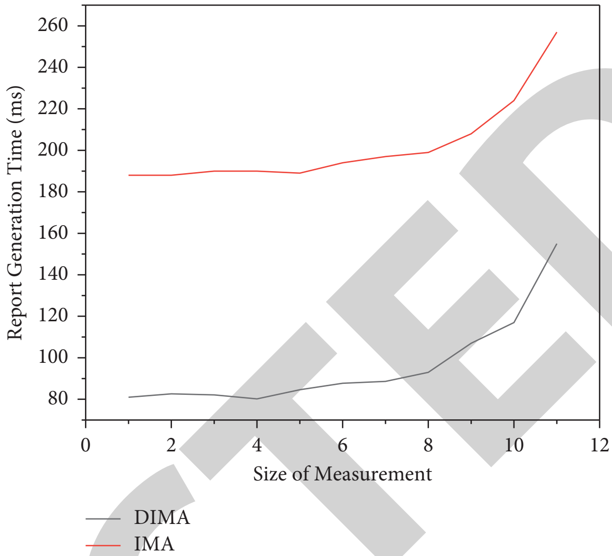

Figure 3: Trusted report generation time of DIMA for measurement content of different sizes.

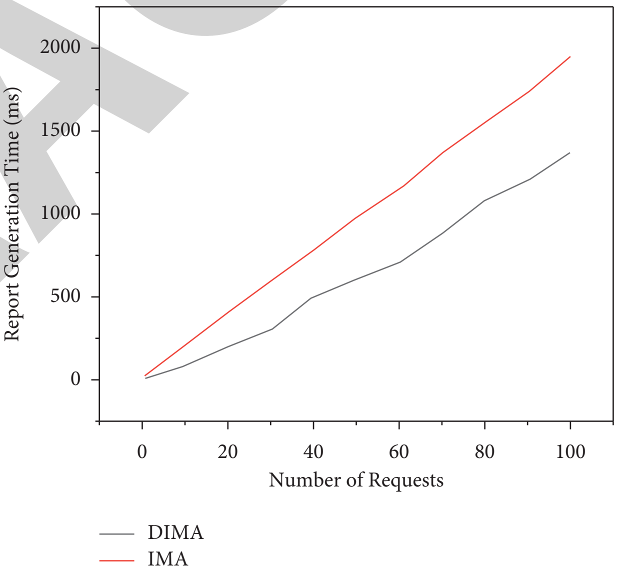

Figure 4: Variation of trusted report generation time with the number of authentication requests in two authentication schemes.

especially when the reliability is relatively frequent (the result shown in the label base in Figure 2).

In the DIMA architecture proposed in this paper, the trusted verification service module needs to respond to a large number of trusted verification requests from different users. Whether the trusted verification report can be generated with high efficiency and fed back to the requester in time is directly related to the reliability of trusted verification. In order to test the verification scheme based on hash signature technology designed in this paper, this paper tests the time overhead and space overhead and compares the efficiency with the traditional verification scheme [22]. Firstly, we test the time overhead of the verification service of DIMA architecture when generating trusted reports for measurement results of different sizes. In the experiment, different sizes of measurement results are constructed, and then different confirmation schemes are used to generate trusted reports. Figure 3 shows the test results with the measurement scale between 1k and 1024k. It can be seen from the results shown in the figure that for the measurement results of the same scale, the time cost of generating trusted reports by the confirmation service of DIMA architecture is only about 50% of that of the traditional IMA confirmation scheme, and when the scale of the measurement results is less than 128K, the time cost of generating trusted reports will not change much [23]. The test results show that the verification scheme designed by DIMA architecture has better performance when dealing with the measurement results of the same scale.

Secondly, aiming at the performance of the verification service in the scenario of responding to multi-user trusted authentication requests, this section compares and tests the time cost of generating trusted reports when the verification service responds to different numbers of user requests [24]. It can be seen from the test results shown in Figure 4 that with the increase of the number of trusted authentication requests, the time cost of generating trusted reports by the confirmation service of DIMA architecture and IMA is increasing. However, it is not difficult to find that for the same number of requests, the report generation time overhead of DIMA architecture is much lower than that of IMA. More importantly, with the gradual increase of the number of requests, the time overhead of IMA increases almost linearly, but the growth trend of time overhead of DIMA architecture is relatively slow. This fully shows that when dealing with large-scale authentication requests, the verification scheme designed by DIMA brings less time overhead, so it can be better suitable for multi-tenant application scenarios in cloud environment [25].

Finally, considering that the trusted report generated in response to a large number of trusted verification requests may occupy the storage space of the system, this section also

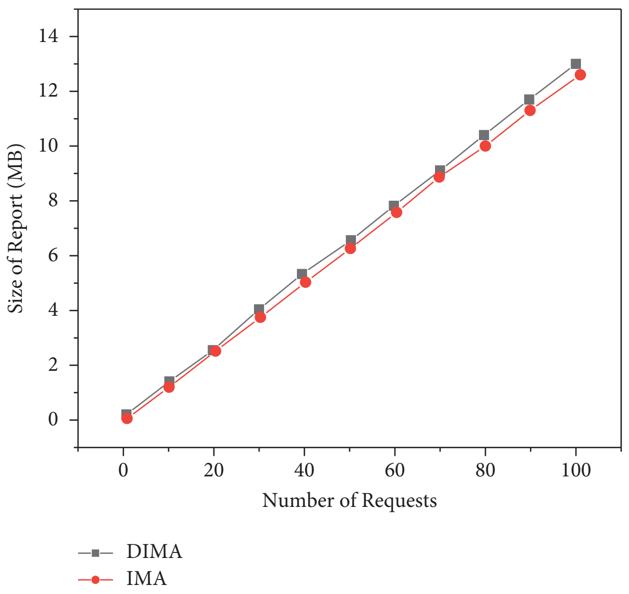

Figure 5: The space cost of the verification service in the two verification schemes varies with the number of verification requests.

tests the space overhead of the confirmation service. Figure 5 shows the variation curve of the space overhead required by the two authentication schemes with the increase of the number of trusted authentication requests. It can be seen from the figure that the space overhead of the two verification schemes basically increases linearly with the number of requests, and the space overhead of DIMA architecture verification service is slightly larger, mainly because the length of the report produced by using hash signature technology will be slightly larger. However, generally speaking, the space cost of the two verification schemes is not very large, which is within the acceptable range of cloud computing system, and the two are almost the same [26]. The experimental results show that the verification scheme with higher security does not bring higher space overhead to DIMA architecture, so it has strong practicability.

From the above experimental results, it can be seen that DIMA architecture can realize various trusted authentication when it brings less additional overhead to user virtual machine and cloud computing platform and can flexibly meet the needs of user trusted authentication, so it can effectively provide trusted protection for user virtual machine.

5. Conclusion

Aiming at the shortcomings of virtual machine trusted authentication technology in the existing cloud computing environment, this paper proposes a dynamic trusted authentication architecture DIMA according to the users' trusted and security requirements for virtual machines. The architecture makes full use of the structural advantages of the virtualization environment, can realize the trusted measurement of users' virtual machines in a more reliable way, and can support users' diversified authentication requests. As the basis of cloud computing technology, the security of virtualized environment will be a research hotspot at present and for a long time in the future. With the changing needs and application scenarios of users, there are still many security problems worth studying and solving. Due to the limitation of time and other factors, the research content of this paper still has many imperfections. In the future, we will further study the trusted guarantee of virtualized environment from the following two directions. In addition to the above integration and improvement of the existing work, in the next research work, we also plan to further explore other aspects of the credibility problem.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] N. Ashammakhi, B. D. Unluturk, O. Kaarela, and I. F. Akyildiz, "The cells and the implant interact with the biological system via the internet and cloud computing as the new mediator," *Journal of Craniofacial Surgery*, vol. 32, no. 5, pp. 1655–1657, 2021.

[2] P. W. Leclercq, A. Kääb, and B. Altena, "Brief communication: detection of glacier surge activity using cloud computing of sentinel-1 radar data," *The Cryosphere*, vol. 15, no. 10, pp. 4901–4907, 2021.

[3] G. S. Chawla, M. Zhang, S. Majumdar et al., "Vmguard: state-based proactive verification of virtual network isolation with application to nfv," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 99, pp. 1–x, 2020.

[4] F. J. Abdullayeva, "Cloud computing virtual machine workload prediction method based on variational autoencoder," *International Journal of Systems and Software Security and Protection*, vol. 12, no. 2, pp. 33–45, 2021.

[5] A. Khaliq, A. Umair, R. Khan, S. Iqbal, and A. Abbass, "Leadership and decision making among smes: management accounting information and the moderating role of cloud computing," *Business Ethics and Leadership*, vol. 5, no. 2, pp. 78–95, 2021.

[6] X. Yang, L. Shu, J. Chen et al., "A survey on smart agriculture: development modes, technologies, and security and privacy challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 273–302, 2021.

[7] P. Zhang, Y. Li, H. Zhang et al., "Stec-iot: a security tactic by virtualizing edge computing on iot," *British Journal of Neurosurgery*, vol. 8, no. 99, pp. 1–7, 2020.

[8] B. K. S. Et al, "Factors affecting fault tolerance during load balancing in cloud computing," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 11, pp. 1523–1533, 2021.

[9] J. Gu, W. Wang, R. Yin, C. V. Truong, B. P. Ganthia, and B. P. Ganthia, "Complex circuit simulation and nonlinear characteristics analysis of GaN power switching device," *Nonlinear Engineering*, vol. 10, no. 1, pp. 555–562, 2021.

[10] H. F. Noureldin and M. Fadel, "Rationalizing resource utilization in cloud computing using coalition formation

strategy," *Journal of Computer Science*, vol. 17, no. 6, pp. 539–555, 2021.

[11] P. B Jawade, K. D. Sai, and S. Ramachandram, "A compact analytical survey on task scheduling in cloud computing environment," *International Journal of Engineering Trends and Technology*, vol. 69, no. 2, pp. 178–187, 2021.

[12] A. Miracle and M. Opoku, "Patterned de-duplication on dependable data subcontracting with three error detecting techniques on cloud computing," *International Journal of Research*, vol. 8, no. 2, pp. 264–266, 2021.

[13] Z. Wu and J. Xiong, "A novel task-scheduling algorithm of cloud computing based on particle swarm optimization," *International Journal of Gaming and Computer-Mediated Simulations*, vol. 13, no. 2, pp. 1–15, 2021.

[14] G. Dhiman, V. Vinoth Kumar, A. Kaur, and A. Sharma, "Don: deep learning and optimization-based framework for detection of novel coronavirus disease using x-ray images," *Interdisciplinary Sciences: Computational Life Sciences*, vol. 13, no. 2, pp. 260–272, 2021.

[15] P. Zhang, H. Li, Y. Ni, F. Gong, M. Li, and F. Wang, "Security aware virtual network embedding algorithm using information entropy topsis," *Journal of Network and Systems Management*, vol. 28, no. 1, pp. 35–57, 2020.

[16] Z. Ullah, A. Umer, M. Zaree et al., "Negotiation based combinatorial double auction mechanism in cloud computing," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 2123–2140, 2021.

[17] J. Jayakumar, B. Nagaraj, S. Chacko, and P. Ajay, "Conceptual implementation of artificial intelligent based E-mobility controller in smart city environment," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5325116, 8 pages, 2021.

[18] C. Ling, W. Zhang, H. He, and Y. C. Tian, "Network perception task migration in cloud-edge fusion computing," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 43–16, 2020.

[19] T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "A survey and classification of the security anomaly detection mechanisms in software defined networks," *Cluster Computing*, vol. 24, no. 2, pp. 1235–1253, 2021.

[20] X. Zhao, X. Liu, J. Liu, J. Chen, S. Fu, and F. Zhong, "The effect of ionization energy and hydrogen weight fraction on the non-thermal plasma volatile organic compounds removal efficiency," *Journal of Physics D: Applied Physics*, vol. 52, no. 14, Article ID 145201, 2019.

[21] T. H. Jeng, W. Y. Luo, C. C. Huang, C. C. Chen, K. H. Chang, and Y. M. Chen, "Cloud computing for malicious encrypted traffic analysis and collaboration," *International Journal of Grid and High Performance Computing*, vol. 13, no. 3, pp. 12–29, 2021.

[22] H. S. Yahia, S. R. M. Zeebaree, M. A. M. Sadeeq et al., "Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling," *Asian Journal of Research in Computer Science*, vol. 8, no. 2, pp. 1–16, 2021.

[23] X. Wang, "Fuzzy decoupling energy efficiency optimization algorithm in cloud computing environment," *International Journal of Information Technologies and Systems Approach*, vol. 14, no. 2, pp. 52–69, 2021.

[24] A. Adebayo and D. B. Rawat, "Scalable service-driven database-enabled wireless network virtualization for robust rf sharing," *IEEE Transactions on Services Computing*, vol. 4, no. 99, p. 1, 2021.

[25] P. Ajay, B. Nagaraj, R. A. Kumar, R. Huang, and P. Ananthi, "Unsupervised hyperspectral microscopic image segmentation using deep embedded clustering algorithm," *Scanning*, vol. 2022, Article ID 1200860, 9 pages, 2022.

[26] G. Veselov, A. Tselykh, A. Sharma, and R. Huang, "Special issue on applications of artificial intelligence in evolution of smart cities and societies," *Informatica*, vol. 45, no. 5, p. 603, 2021, http://www.informatica.si/index.php/informatica/article/view/3600.