Cloud Computing Architecture and Implementation Network Security Technologies for Defense and Virtual Computing

Mr. Omarsharif A. Terdalkar, Mr. Santosh S. Kore, Mr. Rahul S. Kumbhar, Mr. Nilesh V. Patil

[1,2,3]Asst. Prof., [3]In charge HoD
[1,2]D. Y. Patil College of Engineering and Technology, Kolhapur,
[3]D.Y. Patil Technical Campus, Faculty of Engineering and Faculty of Management, Talsande, Kolhapur,
[4]KE Society’s Rajarambapu Institute of Technology, Rajaramnager, Sangli.

Article Info
Page Number: 12290-12301
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 15 September 2022
Revised: 24 October 2022
Accepted: 18 November 2022
Publication: 21 December 2022

Abstract

A research and implementation approach of cloud computing is needed to improve the defense effect in network security. Technology for virtual computing and network security is suggested. architecture fully utilizes the structural benefits of the user's various authentication demands can be supported in a virtualized environment, which can more reliably realize the trusted measurement of the user's virtual machine. This paper introduces the idea of cloud computing, cloud computing classification, and cloud computing features. network protection. The topology of the cloud computing network is constructed when fully taking into account the coupling relationship between the physical network and the logical network, and the cloud computing network is then analyzed using the appropriate network theory based on the network topology. The study of avalanche failure within the computing network. The findings of the research indicate that the relative performance under various trusted measurement periods can reach more than 97%, allowing for flexible user trusted authentication demands as well as efficient trusted security for user virtual machines. The robustness of the entire cloud computing network topology can be significantly increased, ensuring that the network can withstand the attack. This can be done by adding additional protection measures to some special nodes in the cloud computing network topology to make sure they are not damaged when attacked. The avalanche effect won't cause a significant area to become paralyzed, and the network's structure and functionality remain unchanged. This technique can significantly enhance the network security's security protection effect.

1. Introduction

Cloud computing technology has been increasingly prevalent and employed in a variety of disciplines and industries as a result of the ongoing development of Internet computer technology. In today's society, technology is a must. It is impossible to imagine daily living without cloud computing technologies. Although cloud computing technology has had a significant positive impact on society, it has also presented various concerns and problems to Internet security. These dangers significantly impede the advancement of cloud computing technologies. Thus, increasing network security is crucial for cloud computing [1]. The security of virtual networks has altered a little with the advent of SDN.

A challenging issue is how to isolate the network in a standard virtual network. The isolation issue will result in numerous security issues, as depicted in Figure 1. In SDN, control and data are divided. The network's isolation is managed by the controller, and the switch solely carries out the controller's orders. This centralized control mode gives the network a good, adaptable, and dynamic isolation scheme. As a result, network isolation has a relatively less impact on SDN. Although though the isolation issue in SDN is quite simple to resolve, it should not be ignored.

Every node in the network could end up becoming the attacker's target. There are significant security dangers if an attacker takes over control of a network node and gains access to the controller's authority [2]. The security of the SDN controller needs extra consideration due to the peculiarities of centralized SDN control. The entire network's operation logic, as well as data transmission with the top application and lower switch, are under the control of the controller. If the controller responds to the attacker's message after the attacker forges data packets to attack the controller, the attacker can gain the controller's sensitive information and evade security monitoring to attack the network. DDoS attacks are rising as the Internet gets more developed. It is challenging to estimate the loss if the controller is subjected to a DDoS attack because it won't be able to handle normal network traffic and the entire network will become immobilized. This research has significant implications for the advancement of cloud computing technology [3] and analyses and examines network security protection under cloud computing technology.machines. Using all of the structural benefits of a virtualization environment, we can more accurately monitor the trustworthy performance of users' virtual machines, accommodate users' various authentication needs, and enhance network security.

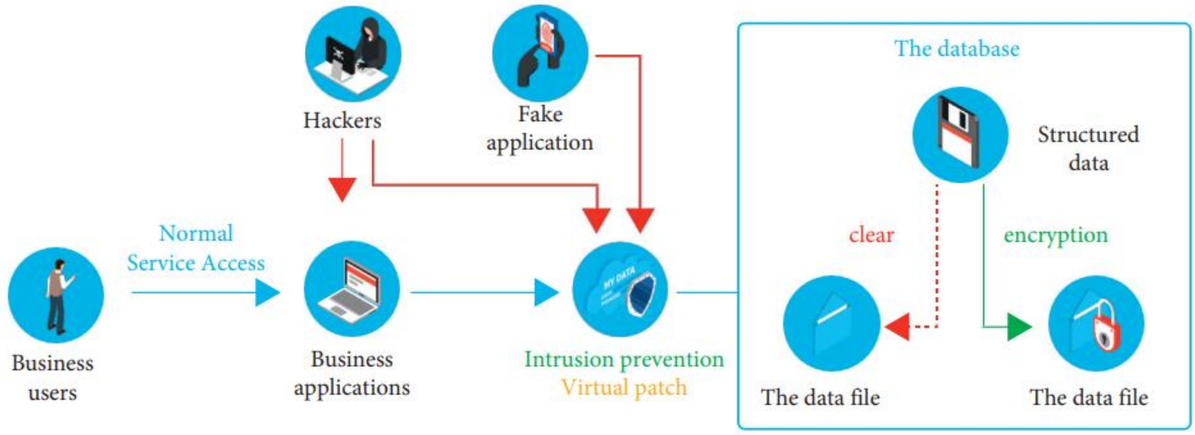


Figure 1: Secure virtual computing and protection.

2. Literature Review

The security of cloud computing has drawn increasing attention as its use has become more and more widespread. It has been examined by numerous groups and subjects both domestically and overseas. Many standardization groups have started to create cloud computing security-related standards in other nations. These organizations include the International Telecommunication Union ITU-TSG17 Study Group, the Cloud Security Alliance CSA, and the Organization for the Advancement of Structured Information Standards (OASIS). Also, a symposium on cloud computing security and associated study has been organized by the worldwide computer society ACM.

the renowned worldwide information security conference Cloud computing security has been prioritized as a research area by RSA [4]. There has been a lot of research on cloud computing security challenges and technology in academic circles, and some advancement has been made. How to encrypt data and safely retrieve encrypted data are the primary issues that need to be resolved in terms of data security.

The former primarily uses cipher text search technology, whilst the latter concentrates on encryption technology. Khalil has contributed to the realm of encryption technology, along with others. By combining integer arithmetic with ideal lattice techniques, they were able to create a fully dynamic encryption solution that ensures data security [5].

This study offers a dynamic trusted authentication architecture (DIMA) in response to the users' trusted and security requirements for virtual machines in order to address the deficiencies of virtual machine trusted authentication technology in the current cloud computing environment. Using all of the structural benefits of a virtualization environment, we can more accurately monitor the trustworthy performance of users' virtual machines, accommodate users' various authentication needs, and enhance network security.

3. Research Methods

3.1. Dynamic Trusted Authentication Architecture for Cloud Virtual Machines (DIMA). This study offers a cloud virtual machine dynamic trusted authentication architecture called DIMA (Dynamic Integrity Measurement and Attestation) in order to allow cloud service providers to offer consumers a set of trusted authentication schemes that may simultaneously meet the above objectives. To monitor the user's virtual machine and dynamically gather integrity evidence in accordance with the user's trusted authentication request, the (e architecture utilizes virtual machine introspection technology based on virtualization technology [6]. The use of virtual machine introspection technology has allowed DIMA to realize the isolation between the target system and the authentication system and to gather reliable evidence outside of the user's virtual machine. This means that malicious attackers inside the virtual machine are unable to interfere with or go around the authentication scheme. Additionally, the DIMA trusted authentication system's trusted measurement rules can be flexible generated in response to the user's authentication request for the security of virtual machines and can measure the security of virtual machine systems in many ways. To overcome the issue that the architecture design of extraterritorial measurement may bring performance load on the management domain and cloud computing platform, DIMA also develops a set of effective trusted verification mechanisms.

This mechanism deftly makes use of hash-based signature technology to efficiently lower the additional strain placed on the cloud platform for trusted measurement, boost the effectiveness of verification, and lessen the risk of hostile users attacking the verification system [7]. 3.2. Mechanism of Credible Measurement for Mitigation. In order to help users stop attacks in time and protect their data and application security to the greatest extent, a set of mitigation mechanisms is created for DIMA architecture on the basis of offering users trusted authentication services. These mechanisms can implement corresponding mitigation measures for different situations in which the integrity of users' virtual machines is damaged [8].

A coarse-grained response measure called a virtual machine level mitigation mechanism uses the user's target virtual machine as the object. These precautions are primarily intended for situations in which there has been significant harm and users have high security demands for the virtual machine environment. The usual operation of the virtual machine system will be affected in some way by using this mitigation method, which will lower its performance.

Therefore, there are quite rigorous requirements for utilizing such techniques. Currently, this type of mitigation method largely consists of three steps: ceasing operations, temporarily suspending operations, and migrating [9].

The system's mitigation mechanism is a targeted, fine-grained response measure that is directed at particular virtual machine system objects. These precautions are typically used when users have stringent requirements for the continuance of virtual machine operation and it is difficult to stop the usual operation of the entire virtual machine.

Only system objects with risks are processed, such as files, processes, and network connections [10], in accordance with the security specifications given by users. Currently, this form of mitigation mechanism focuses mostly on processing at the process level. (roughly) Identify the processes accessing corrupted files, malicious network connections, and compromised system objects; stop the processes.

Remote Authentication Protocol, section 3.3. This section specifically targets 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]. This is done in light of the limitations of the existing remote authentication protocol in DIMA architecture. There are three parties involved in the remote authentication protocol created in this section:

Section 3.3 of the Remote Authentication Protocol. The remote authentication protocol of the DIMA architecture is specifically designed in this section based on hash signature technology to meet the needs of security and efficiency simultaneously [11]. It is targeted at the structural characteristics and security requirements of the DIMA architecture. Given the shortcomings of the current remote authentication protocol in the DIMA architecture, this is done. The remote authentication protocol developed in this section involves three parties:

(1) Virtual machine user (T): In the authentication protocol, the virtual machine user acts as the challenger or verifier to send a trusted authentication request to the distant virtual machine system. In contrast to the traditional remote authentication protocol, the DIMA application scenario does not explicitly distinguish between the challenger and the verifier; instead, the virtual machine user fulfils this function.
(2) Prove (P): It replies to the tenant's request for authentication and, using trusted measurement and authentication, shows the user the outcome of the measurement.
(3) Private certificate authority (PCA): The PCA is a dependable third party that certifies and backs up the verification key technology.

The verification protocol suggested in this section is implemented on the basis of XMSS, taking into account the characteristics of multi-tenancy and multiple requirements on the cloud platform as well as the restrictions of OTS scheme signature. WOTS+ is utilized as the single signature implementation method for a multiple signature system. In this protocol, hash-based signature technology is only used for the signature authentication of trustworthy evidence in order to be more compatible with the existing trusted platform, while other identity authentication processes are implemented based on the current public key cryptosystem [12]. The definitions of the symbols used in the protocol are presented in Table 1 to make it easier to describe the protocol.

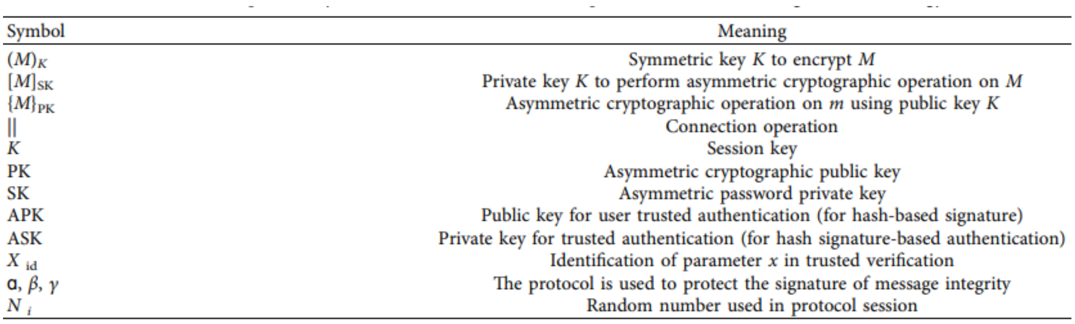
To ensure the proper implementation of the agreement created in this section, we made a few rudimentary assumptions for each participant prior to its implementation. To establish identify, each participant has a special key pair. The public key for the key pair, which is based on the well-known public key cryptosystem, is broadcast by the authority [13]. Second, the cloud service platform's certifier P and virtual machine user T both completely trust the certificate authority in the DIMA architecture (PCA). Finally, the platform security storage mechanism safeguards the private key used for trustworthy verification, ensuring that it cannot be taken by an intruder. The DIMA architecture's trusted authentication protocol execution procedure is often split into two components [14].

The process of authenticating a new user when he first makes an authentication request and creating a key for trustworthy authentication using PCA constitute the first phase of the authentication process. The procedure for the second portion is replying to the user's reliable confirmation and relaying the reliable report. The primary goal of the first phase is to create the key pair that has been verified by the user for the user with the help of the certificate authority PCA and to provide the user with the public key component [15]. The public key for the XMSS signature technique is a string of N bits in length that is combined using several WOTS + public keys in accordance with the formula (1). The signature of the first leaf of the XML tree + node is referred to as the first leaf of the XML tree + node. The created key contains 2H WOTS + key pairs, which can complete 2H signatures and authentication, when the height of the XMSS public key tree is set 2 h.

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

The format of the confirmation signature that is sent to the virtual machine user in each trusted authentication report is Sig (id,, Auth), where id(0 I 2H 1) is the index number of the WOTS + key pair used for this signature, is a signature built using the WOTS + algorithm, and E is the authentication path in the XMSS tree. Its purpose is to help the signature authenticator use the XMSS public key to confirm the authenticity of the signature. Using the WOTS + key pair as an example, the path symbolized by the circle is the authentication path used to authenticate the signature if the private key in the matching LTree is used for it.

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



Symbol	Meaning
$(M)_K$	Symmetric key K to encrypt M
$[M]_{\mathrm{SK}}$	Private key K to perform asymmetric cryptographic operation on M
$\{M\}_{\mathrm{PK}}$	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

A path for authentication is required in several aggregation techniques built on the Merkel tree. There are currently a variety of alternate ways for calculating the authentication path. We adopt the method from [16] for the DIMA architecture that is suggested in this research because it can effectively balance and optimize the compute overhead and storage overhead and is extremely suitable for the scenario of trustworthy verification of multi-tenant virtual machines. The virtual machine user must use his current public key to verify the trusted evidence's contents after receiving it from the certifier together with the evidence signature mentioned above.

The trustworthy verification we developed differs from the verification technique based on the signature of public key cryptosystem because it uses the MTS signature algorithm XMSS. Users of virtual machines must first determine the signature's verification public key (PK) using the verification data and signature they get, and then they must build the XMSS public key (APK) using the PK and the authentication path (Auth). The user acknowledges that the signature of the verifier is legitimate if the APK perfectly matches the public key APK that the verifier previously delivered; otherwise, the verification is unsuccessful.

The certifier will keep track of the random numbers connected to all received authentication requests in a local database as part of the DIMA architecture's authentication protocol in order to prevent replay attacks. The certifier will initially determine whether the random number contained in the request is present in the database after receiving a fresh request message [17]. If it does, the certifier will reject the authentication request, clear the user's existing connection information, and wait for the subsequent request to reestablish a secure connection. If it does not exist, the certifier will add the random number to the local database and accept the verification request.

4. Result Analysis

Although using the DIMA architecture to implement trusted verification on the security of user virtual machines can effectively ensure that those virtual machines are secure, using the DIMA framework will add performance overhead to the trusted measurement process, which will have some effect on the system performance of those virtual machines. This section assesses the performance impact of the runtime DIMA architecture on the virtual machine system in order to gauge the viability of DIMA. The user can request a trustworthy authentication at any time while the virtual machine is running, and they can also demand that the certifier send back the reliability measurement findings on a regular basis.Hence, the frequency of credibility measurement will vary depending on the request cycle. [19]

In order to test the performance impact of the virtual machine under different trusted measurement frequencies, we run different benchmark test sets on the virtual machine and initiate periodic trusted authentication requests through users at different frequencies. The PALMS Cloud test programme from the PALMS Cloud platform benchmark set was utilized in this section. Each benchmark software has undergone extensive testing using numerous reliable measurement cycles. The performance impact of the DIMA architecture on various benchmark programmes under various trustworthy measurement cycles is depicted in Figure 2.

The test results under different conditions are used as the benchmark to determine the relative performance, and the label base represents the performance of the benchmark programme when there is no reliable measurement [20]. According to the test findings shown in Figure 2, the implementation of trustworthy measurement by DIMA at run time will have an impact on the performance of benchmark programmes, and the impact on the performance of various benchmark programmes varies. The relative performance may reach more than 97% under various trusted measurement cycles, and the impact of CPU and memory on performance is relatively little among them.

This is mostly due to the micro-short benchmark's running time and the little amount of DIMA-trusted measurement cycles required, which allow the performance impact to be virtually completely disregarded [21]. Comparatively speaking, the performance of the three macro-benchmark programmes, database, online, and app, is significantly impacted, particularly when the dependability is very frequent (result given in label base in Figure 2).

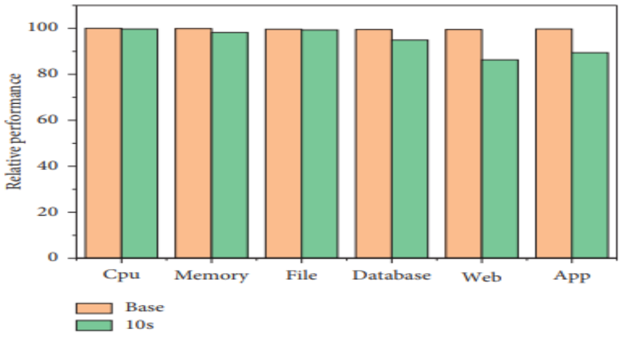


Figure 2: Impact of DIMA runtime reliability on the performance of benchmark test set.

The trusted verification service module in the DIMA architecture suggested in this study must respond to numerous trusted verification requests coming from various users. The dependability of trusted verification is directly tied to whether the trusted verification report can be produced with high efficiency and sent to the requester on schedule. This study tests the time overhead and space overhead of the verification strategy based on hash signature technology that was developed in order to compare the efficiency with the conventional verification scheme [22].

Initially, we evaluate the time consumption of the DIMA architecture's verification service for generating trusted reports for measurement results of various sizes. In the experiment, several measurement result sizes are built, and then various confirmation techniques are applied to produce reliable reports. The test results are displayed in Figure 3 with a measurement range of 1k to 1024k. The results shown in the figure demonstrate that, for measurement results of the same scale, the time cost of generating trusted reports by the confirmation service of DIMA architecture is only roughly 50% of that of the conventional IMA confirmation scheme. Additionally, when the scale of the measurement results is less than 128K, the time cost of generating trusted reports will not be necessary.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.

Second, this part compares and examines the performance of the verification service in the situation of responding to multi-user trusted authentication requests.Time spent producing reliable reports when the verification service handles a variety of customer queries [24].As can be observed from the test results displayed in Figure 4, the confirmation service of the DIMA architecture and IMA requires more time to generate trusted reports as the number of trusted authentication requests rises.

The report generating time overhead of the DIMA architecture is significantly lower than that of the IMA, however, for the same number of requests. More significantly, the time overhead of IMA increases roughly linearly as the number of requests rises gradually, but the growth trend of the time overhead of DIMA architecture is very moderate. (It amply demonstrates that the verification technique created by DIMA has less time overhead when handling large-scale authentication requests, making it more appropriate for multi-tenant application scenarios in cloud environments. [25]

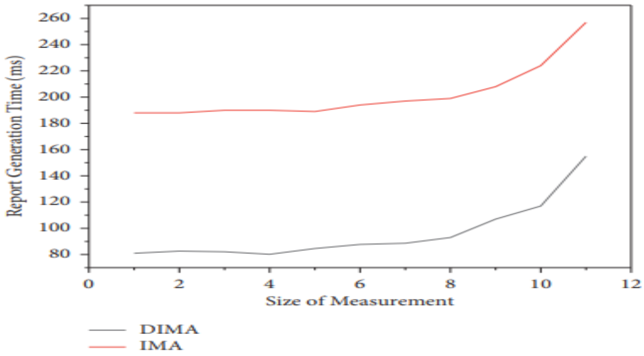


Figure 3: Trusted report generation time of DIMA for measurement content of different sizes

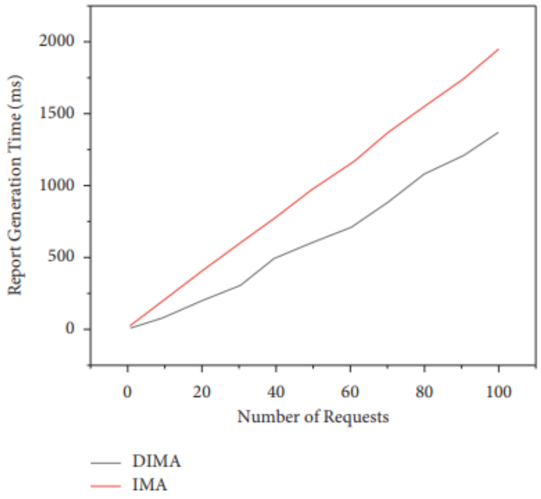


Figure 4: Variation of trusted report generation time with thenumber of authentication requests in two authentication schemes.

This component additionally evaluates the space overhead of the confirmation service because the trustworthy report produced in response to numerous trusted verification requests may take up a lot of system store space. With a rise in the quantity of trustworthy authentication requests, Figure 5 depicts the variation curve of the space overhead needed by the two authentication systems. The DIMA architecture verification service has a slightly higher space overhead than the other two verification schemes, primarily due to the lengthier report generated by hash signature technology. This is evident from the figure, which shows that the space overhead of the two verification schemes basically increases linearly with the number of requests.

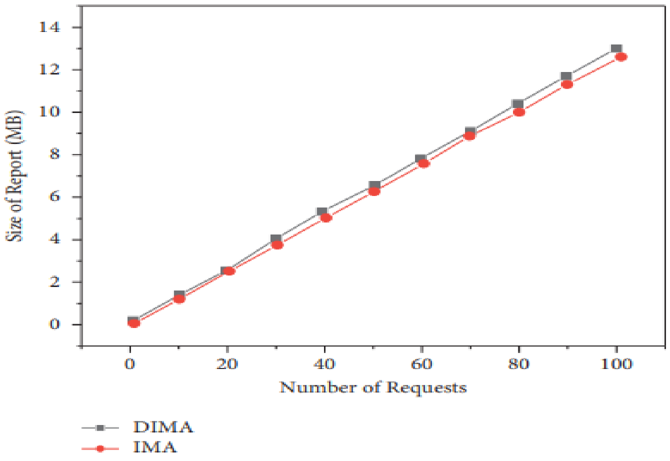


Figure 5: The space cost of the verification service in the two verification schemes varies with the number of verification requests

Yet, in general, the space costs of the two verification procedures are not particularly high and fall within the permitted range for cloud computing systems [26]. Moreover, the two are nearly identical. The experimental findings demonstrate the strong practicability of the greater security verification scheme, which does not result in a larger space overhead for the DIMA architecture.

From the aforementioned experimental findings, it is clear that DIMA architecture can implement different trusted authentication when it adds little extra overhead to user virtual machines and cloud computing platforms and can adapt to user trusted authentication needs, effectively delivering trusted protection for user virtual machines.

5. Conclusion

This study suggests a dynamic trusted authentication architecture (DIMA) in response to users' trusted and security requirements for virtual machines in an effort to address the limitations of virtual machine trusted authentication technology in the current cloud computing environment. (e architecture fully exploits the structural benefits of the virtualization environment, enables more reliable trustworthy assessment of users' virtual machines, and supports a variety of authentication demands from users. The security of virtualized environments will continue to be a focus of research for a very long time because it forms the foundation of cloud computing technologies. There are still many security issues that merit research and solution due to the shifting needs and application situations of users.

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 planto further explore other aspects of the credibility problem.

References

1. N. Ashammakhi, B. D. Unluturk, O. Kaarela, and I. F. Akyildiz, “(e 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. K¨a¨ab, and B. Altena, “Brief communication: detection of glacier surge activity using cloud computing of sentinel-1 radar data,” 1e Cryosphere, vol. 15, no. 10, pp. 4901–4907, 2021.
3. G. S. Chawla, M. Zhang, S. Majumdar et al., “Vmguard: statebased 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 variationalautoencoder,” 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 AutomaticaSinica, 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.
7. 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.
8. 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.
9. H. F. Noureldin and M. Fadel, “Rationalizing resource utilization in cloud computing using coalition formationstrategy,” Journal of Computer Science, vol. 17, no. 6, pp. 539–555, 2021
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. X. Zhao, X. Liu, J. Liu, J. Chen, S. Fu, and F. Zhong, “(e 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.

20. 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.
21. H. S. Yahia, S. R. M. Zeebaree, M. A. M. Sadeeq et al., "Comprehensive survey for cloud computing based natureinspired algorithms optimization scheduling," Asian Journal of Research in Computer Science, vol. 8, no. 2, pp. 1–16, 2021.
22. 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.
23. 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.
24. P. Ajay, B. Nagaraj, R. A. Kumar, R. Huang, and P. Ananthi, "Unsupervised hyperspectral microscopic imagesegmentation using deep embedded clustering algorithm," Scanning, vol. 2022, Article ID 1200860, 9 pages, 2022.
25. S. Srivastava and R. Kumar, "Indirect method to measure software quality using CK-OO suite," 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), 2013, pp. 47-51, doi: 10.1109/ISSP.2013.6526872.
26. Ram Kumar, Gunja Varshney , Tourism Crisis Evaluation Using Fuzzy Artificial Neural network, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-NCAI2011, June 2011
27. Ram Kumar, Jasvinder Pal Singh, Gaurav Srivastava, "A Survey Paper on Altered Fingerprint Identification & Classification" International Journal of Electronics Communication and Computer Engineering Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278– 4209
28. Kumar, R., Singh, J.P., Srivastava, G. (2014). Altered Fingerprint Identification and Classification Using SP Detection and Fuzzy Classification. In: , et al. Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012. Advances in Intelligent Systems and Computing, vol 236. Springer, New Delhi. https://doi.org/10.1007/978-81-322-1602-5_139
29. 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.
30. Mr. Ajinkya S. Yadav, Dr. Vinayak I. Pujari, Dr. B.D. Jitkar "Make use of Cloud Computing in Educational Research" , GRADIVA REVIEW JOURNAL, VOLUME 8 ISSUE 3 2022, https://www.researchgate.net/publication/360009053_Make_use_of_Cloud_Computing_in_Educational_Research