A Semantic Approach to Cloud Platform Security Protection Framework

Prof. Khatal Sunil S.[1] Hande Bhagyashree M.[2] Navale Adesh L.[3] Deshmukh Sumit B.[4] Doke Onkar B.[5]

[1,2,3,4,5]Department of Computer Engineering

[1,2,3,4,5]Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Maharashtra, India

Abstract— Cloud services became Associate in Nursing essential a vicinity of many organizations. Cloud suppliers have to adhere to security and privacy policies to form certain their users' data remains confidential and secure. though there are many efforts on developing cloud security standards, most cloud suppliers are implementing a combination of security and privacy controls. This has a semiconductor device to confusion among cloud customers on what security measures they need to expect from the cloud services, and whether these measures would go along with their security and compliance desires. we have conducted a comprehensive study to review the potential threats featured by cloud customers and have determined the compliance models and security controls that need to be in place to manage the chance. The cloud platform is that the company's new generation of information basic platform, Associate in Nursing it's associate important support for driving the company's IT and information resource construction. This paper proposes a security protection framework model at intervals the cloud environment, combined with the power cloud platform framework, vogue power protection framework system applicable to electric power firms elaborated the key technologies and system style of security protection at intervals the cloud surroundings. Finally, supported the power cloud platform style, the feasibility and reliability of cloud platform security protection was verified. Finally, summarize the paper and illustrate further work.

Keywords: Cloud Computing; Security Protection; Security Reinforcement; Situational Awareness, Security Compliance Models, Cloud Security Models

I. INTRODUCTION

At present, domestic and foreign research on cloud platform security square measure primarily targeted public clouds. The relevant security technologies are additional universal technologies. numerous cloud platform vendors are subject to technical barriers and are geared toward the image security of enterprise proprietary clouds. There are still no sensible solutions to security problems like runtime security, behavior auditing, and firewall between containers. Instances created through cloud platform custom images are identified as instances created through traditional official images. throughout the creation method, there may be vulnerabilities in several levels of the operative the system itself, like insecure vulnerabilities in remote command execution (that cause National Security Agency tools to be affected). Windows 0day vulnerability), application security vulnerability (weak parole, management background information revealing, SQL code injection vulnerability, Struts2 unsound vulnerability). Behaviour auditing is more concerning determination security audits at the cloud information level, and there's an absence of security audit solutions for the full life cycle of user behaviour. Cloud-native loader container firewalls are almost like next-generation firewalls or WAFs, however, they need vast variations in cloud and hosted safety features. good instrumentality firewall technology is presently being developed. By grouping the maximum amount of behavioural information as attainable, the instrumentality firewall will consistently perceive the intent of the applying, manage security policies to mechanically support this intent, and establish and forbid behaviours that don't conform to the present intent. This paper studies the safety protection framework model within the cloud environment. Combined with the cloud platform framework of the State Grid Corporation of China, a security protection framework system appropriate for electrical power firms is meant. Its structure is arranged as follows: The second half explains the key technologies and system design of security protection within the cloud atmosphere. The third half is based on the ability of cloud platform design, verifying the practicability and dependability of cloud platform security protection. Finally, summarize the paper and show further work.

II. CLOUD PLATFORM SECURITY DESIGN

1) Cloud platform security protection overall framework At present, power firms have primarily completed the construction and preparation of cloud platforms. With the subsequent migration of an oversized range of business applications to the cloud, the safety needs for cloud platforms are getting higher and better. Currently, the safety elements provided by the cloud the platform cannot adapt to the safety protection requirements of the facility company's cloud platform, and There are still massive security risks, that are in the main reflected within the cloud platform itself and also the application on the cloud. In terms of security improvement of the cloud the platform itself: business and management network isolation isn't effective, clear text transmission/no access authentication; host and management nodes are vulnerable to vulnerabilities, virus infections, and alternative risks; platform API interfaces and cloud mirroring console management and management aren't in situ risks, the chance of leakage of sensitive data on the cloud platform itself. In terms of cloud applications: network space division does not meet business operational needs, and communication knowledge is in danger of being stolen; system boundaries aren't clear, tenant resources aren't effectively isolated, business logic access management is missing; information is lost or broken, illicit access or tampering. Combining the characteristics of the cloud platform, accurately analyse the safety risk points moon-faced by the cloud platform and cloud applications; verify the overall security protection design of the cloud platform, style-specific protection measures hierarchically, establish a sound cloud platform security protection system, and comprehensively improve the

comprehensive defence capabilities of the cloud platform ; Prevent malicious network attacks against cloud platforms, ensure the security of business applications, micro applications, and micro-services on the cloud platform, and prevent the outflow of vital information and sensitive information on the cloud platform. perform cloud platform network security design under the national-level protection "one centre, triple protection" the general plan, and build a "5+4" broad security protection capability framework covering cloud platforms and cloud applications. The overall framework of cloud platform security protection proposes five security protection technical capabilities, and proposes five technical capability requirements for secure physical surroundings, secure communication network, secure space boundary, secure computing surroundings, and security management canter. It additionally proposes interface and boundary security, and cloud platform virtualization. needs for capabilities like centralized security, the cloud tenant resource isolation and management. the framework of cloud platform security protection proposes four security management capabilities, and proposes four security management capabilities requirements for building security management and control, online security management, and management, basic operation services, and added operation services. Put forward relevant capability needs for tenant security and two-level cooperative security operation key analysis.

2) Security Technology Defence Deployment Architecture contains In terms of cloud platform north-south protection design, combined with the present security protection technology route of the facility business, the prevailing boundary security protection equipment and strategies will be continued to satisfy the necessities of cloud platform access management, unknown threat detection, traffic cleansing, attack supply tracing, and intrusion detection, Malicious program observation, network isolation, and alternative protection needs. In terms of the east-west protection style of the cloud platform, cloud platform security elements (virtual firewall, host protection, cloud WAF, etc.) are additional to realize the protection necessities of cloud resource access management, resource isolation, intrusion interference, and computer program observation.
3) Platform side safety protection contains the cloud platform aspect security protection relies on the use of existing security reinforcement measures, and mainly enhances log auditing, information protection, and container security capabilities. Platform-side security protection principally includes border firewall, anti-DDoS equipment, IPS/antivirus, bastion machine, integrated log audit, cloud platform sensitive information protection, situational awareness (platform side), and instrumentation security. supported the effectiveness of the development of the two-level network security operation centre, establish and improve the cloud platform security operation and maintenance system, perform the cloud platform security operation and maintenance work daily, ensure that numerous security technical suggests that and measures area unit effectively enforced, and defend the cloud platform's own security and cloud business Security, to achieve cloud security capabilities of defence comprehensive, active defence, and resilient defence. and check out to develop value added operation services on the idea of safe operation and maintenance.

III. Result based verification

The cloud security protection part provides alarm and log interfaces for scenario awareness, and adapts to the cloud Security Service alarm and log interface. The cloud security protection part will also, send alarms and logs to true awareness the platform through the Syslog or Webservices interface.

1) Cloud security reinforcement verification. The cloud platform security baseline assessment and reinforcement stage need comb and analysis through cloud platform quality sorting, network security inspection, physical machine security review, platform application security review, etc., to judge the cloud platform security baseline scenario. The cloud tenant security baseline assessment and reinforcement stage require sorting and analysis through cloud application asset sorting, network security review, application security review, cloud host security review, cloud component security sorting, etc., to judge the cloud application security baseline scenario. the protection product configuration and reinforcement stage is especially through checking the protection product list, traffic operating status, security product operating standing, product rule base and different aspects to arranged investigate and measure the baseline scenario of cloud platform security merchandise. The arrange style stage is principally supported power business, asset sorting and analysis. Investigate and perceive the on-the-spot cloud business situation and cloud platform preparation state of affairs of the power cloud platform, confirm the work target, and formulate the project service implementation arrange based mostly on the customer's business, plus state of affairs, and target.
2) Business system disaster recovery rating and model recommendations. According to the quality sorting table of the business system dimension, rehearse the host security cluster binding of every business system, and fill in whether or not the security cluster has AN incoming whitelist and blacklist. The cloud platform security hardening check results square measure the cloud fort machine unified access authentication, authorization and audit capabilities for platform operation and maintenance of assets like hosts and databases. Provide info sensitive data decrement. info audit, record and audit operations like addition, deletion, modification, and checking of the info. Realize protection capabilities like fast discovery and positioning of sensitive information on the cloud platform. Host security services provide virtual machines with anti-virus, anti-intrusion, and host firewall capabilities. supported the cloud server cryptographic machine certified by the National Cryptographic Bureau, a virtual science resource pool is constructed to realize unified programming and control of IT and cryptographic resources, and provide users with virtual

science machine (VSM) services on demand. Realize cloud platform the security state of affairs awareness.

IV. CONCLUSION

The security of cloud platforms is turning into additional and more vital. The paper proposes a security protection framework model during cloud surroundings, combined with the power cloud platform framework, styles a security protection framework system appropriate for power companies, and elaborates key technologies for security protection within the cloud surroundings and system architecture. Finally, supported the ability of cloud platform architecture, the practicableness, and dependability of cloud platform security protection is verified. within the next step, in-depth analyses are conducted on the upper-layer business security of the cloud platform.

REFERENCES

[1] Mr.Sunil S.khatal1, Mr.B.S.Chunchore2, Mr.K.S.Kahate3 (2016). Survey on key aggregation system for secure sharing of cloud data. International Journal of Scientific Engineering and Applied Science (IJSEAS) –Volume-2, Issue-7, July 2016 ISSN: 2395-3470.

[2] Mr.Sunil S.khatal1, Mr. K.S.Kahate2 (2016). Data Security using KAC for Sharing Scalable Data. International Journal of Advance Research and Innovative Ideas in Education. IJARIIE-ISSN(O)-2395-4396

[3] Prof. Khatal S.S., Navale Adesh L., Hande Bhagyashree M., Deshmukh Sumit B., Doke Onkar B.. "COMPREHENSIVE REVIEW ON SECURE INFORMATION SHARING IN CLOUD COMPUTING", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Vol.9, Issue 11, pp.82-85, November 2021

[4] Tissir, Najat, Said El Kafhali, and Noureddine Aboutabit. (2021). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal.Journal of Reliable Intelligent Environments 7.2: 69-84.

[5] Taher, Kazheen Ismael, et al. (2021): Efficiency of semantic web implementation on cloud computing: A review. Qubahan Academic Journal 1.3 1-9.

[6] Ramalingam, Chithambaramani, and Prakash Mohan. (2021): Addressing Semantics Standards for Cloud Portability and Interoperability in Multi Cloud Environment." Symmetry 13.2 317.

[7] Kaur, Sandeep, and Gaganpreet Kaur. (2021) Threat and Vulnerability Analysis of Cloud Platform: A User Perspective.8th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2021.

[8] Sane, Ketki, Karuna Pande Joshi, and Sudip Mittal. (2021). semantically rich framework to automate cyber insurance services. IEEE Transactions on Services Computing.

[9] Al-Muhtadi, Jalal, et al. (2021) A lightweight cyber security framework with context-awareness for pervasive computing environments." Sustainable Cities and Society 66: 102610.

[10] Srinivasan, J., and C. Suresh Gnana Dhas. (2021): Cloud management architecture to improve the resource allocation in cloud IAAS platform." Journal of Ambient Intelligence and Humanized Computing 1-8

[11] Alam, Tanweer. (2021) Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI) 108-115.

[12] Singh, Harvinder, Sanjay Tyagi, and Pardeep Kumar. (2021) Comparative analysis of various simulation tools used in a cloud environment for task-resource mapping. Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences: PCCDS 2020. Springer Singapore.

[13] Baker, Thar, et al. (2015) Security-oriented cloud platform for soa-based scada. 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE.

[14] Kumar, Rohit. (2021) Dos attacks on cloud platform: Their solutions and implications. Research Anthology on Combating Denial-of-Service Attacks. IGI Global. 476-490.

[15] Iqbal, Salman, et al. (2021) on cloud security attacks: A taxonomy and intrusion detection and prevention as a service. Journal of Network and Computer Applications 74: 98-120.

