IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Implementation Of Advance Cyber Security Iaas Environment Through SSL Surveillance Framework With E Governance & Smart City

Enhancing Load Balancing

Mr. Jigul Nimavat [1], Dr.Vijaykumar B. Gadhavi[2]

[1]PhD Scholar – Computer Engineering Department Swaminarayan University, India
[2]Associate Professor & Dean – Faculty of Engineering (I/C), Computer Engineering Department Swaminarayan University, India

***Abstract*—** The utilization and management of compute resources have been significantly transformed by cloud computing, specifically in Infrastructure as a Service (IaaS) environments. Nevertheless, in light of the exponential growth of cloud services, security and load balancing concerns have assumed critical importance. By leveraging Secure Sockets Layer (SSL) technology, this paper presents a method for complementing load balancing and security in IaaS environments. The implementation of load balancing is essential for cloud environments to achieve optimal resource utilization and performance. Conventional load-balancing strategies frequently fail to adequately manage fluctuating duties and safeguard data confidentiality. Through the incorporation of SSL into the load-balancing mechanism, this investigation endeavours to establish a secure channel of communication between virtual machines and clients, thus reducing the likelihood of security breaches including data tampering and espionage. Furthermore, the implementation of SSL encryption for the data exchanged between clients and virtual machines serves to bolster security measures, guaranteeing both confidentiality and integrity. By implementing this strategy, the IaaS environment's overall security posture is not only strengthened but regulatory compliance requirements regarding data protection are also met. In addition, experimental evaluations of the suggested SSL-based load-balancing technique are performed in a simulated cloud environment. The findings illustrate enhanced performance concerning resource utilization, response time, and throughput when compared to traditional load-balancing techniques. Furthermore, the security analysis validates the efficacy of SSL in safeguarding confidential information against unauthorized intrusion and manipulation. By incorporating SSL into the load-balancing mechanism, IaaS environments can effectively tackle security and load-balancing challenges simultaneously. This investigation contributes substantially to the advancement of knowledge and implementation regarding cloud computing architectures that are both secure and efficient. The security and dependability of cloud-based services consequently improve.

***Index Terms*—** Cloud Computing, Infrastructure as a Service (IaaS), Load Balancing, Secure Sockets Layer (SSL), Security, Data Privacy, Encryption, Virtual Machines, Performance Optimization, Regulatory Compliance.

I. INTRODUCTION

Cloud computing has become an integral part of modern-day computing due to its numerous benefits, such as scalability, availability, and cost-effectiveness. However, load balancing and security remain significant challenges in a cloud computing environment. To ensure data security and improve performance in an Infrastructure as a Service (IaaS) environment, it is crucial to establish strong protocols. The reason for this is that SSL improves the security of cloud computing and load balancing [1]. A crucial element of load balancing is the allocation of incoming traffic among many servers. The main goal is to prevent servers from being overloaded, therefore maximizing resource use and ensuring high availability. To guarantee the security of communication routes between servers and users, an organization may employ load balancing and SSL, which provides encryption for data carried over the network [2].

Encryption improves the overall security of the cloud architecture by reducing susceptibility to surveillance, man-in-the-middle attacks, and data invasions [3]. Moreover, SSL encryption guarantees the privacy and protection of delicate information, such as personally identifiable information (PII), financial transactions, and private corporate data, while it is being sent [4]. SSL encryption guarantees the segregation and protection of individual users' data against unauthorized access or modification in IaaS systems, where several tenants use the same physical infrastructure [5]. Furthermore, SSL-enabled load balancing enhances the efficiency and scalability of cloud services by spreading incoming requests across several servers. This process takes into account factors such as server load, geographical location, and general health. This approach enhances user experience by efficiently distributing resources, resulting in accelerated application performance, reduced response times,

cloud computing security [7]. Organizations can improve the performance and scalability of their cloud infrastructure, protect sensitive information, and effectively manage security risks by implementing measures like data encryption, server authenticity verification, and data confidentiality assurance.

1.1. Background on Cloud Computing and IaaS

Cloud computing has revolutionized the way computing resources are provisioned, managed, and accessed. It offers scalable and on-demand access to a pool of computing resources, including servers, storage, networking, and applications, over the Internet. Infrastructure as a Service (IaaS) is a fundamental model of cloud computing, providing virtualized computing resources over the internet on a pay-as-you-go basis. These advancements are accompanied by improvements in security, resource management, and quality of service [8]. Infrastructure as a Service (IaaS) minimizes the costs related to the deployment and maintenance of applications that depend on computing, networking, and data storage by offering shared cloud capabilities [9]. Discussions are already taking place on the use of stochastic neural networks (SNNs) to evaluate the quality and functionality of IaaS systems [10]. The integration of artificial intelligence technology into applications is enabling the creation of intelligent and the functioning of cloud AI [11]. Public cloud providers provide Platforms as a Service (IaaS) that might be a suitable option for organizations in need of powerful computing capabilities [12]. This is because it provides flexibility in terms of hardware selection and running expenditures.

1.2. Importance of Load Balancing and Security in Cloud Environments

Security and load balancing in cloud systems are crucial due to the numerous advantages and difficulties associated with cloud computing. Cloud computing provides accessibility, scalability, and cost-effectiveness [13]. Nevertheless, optimizing resource utilization and effectively managing the substantial volume of network traffic present formidable obstacles [14]. Load balancing techniques, including capacity-based load balancing (CBLB), enhance system performance by distributing the workload among the available resources at any given time [15]. Furthermore, load balancing contributes to the improvement of system stability, energy efficiency, and the utilization of computing resources [16]. Secure procedures, including SSL encryption, must be implemented to safeguard data privacy and deter unauthorized access [17]. Implementing load balancing and security measures alongside innovative algorithms such as the modified Genetic Algorithm can effectively decrease execution and response times in cloud environments. Incorporating load balancing and security mechanisms into cloud computing systems is essential for maximizing resource utilization, data protection, and performance. Figure 1 depicts the security domain in the cloud as shown below.

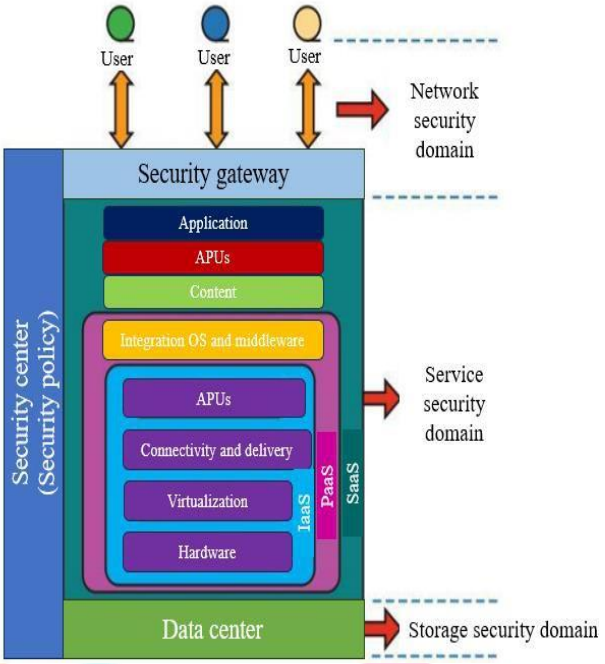

Figure 1. Security in Cloud [18]

1.3. Role of SSL in Enhancing Security in IaaS

Secure Sockets Layer (SSL) is an intricate component of the Infrastructure as a Service (IaaS) environment's security infrastructure [19] by facilitating encryption and authentication processes. Priority must be given to ensuring the security and integrity of data transmissions in the context of Infrastructure as a Service (IaaS), which operates on the Internet to deliver resources and services [20]. SSL—presently referred to as Transport Layer Security (TLS)—enables the encryption of data during transmission to erect a secure connection between a client and a server. Unauthorized parties are unable to intercept and obtain access to sensitive data [21]; thus, this encryption safeguards against espionage. The identities of the client, server, and all other participants in the communication process are additionally validated via digital certificate-based verification enabled by SSL [212. This authentication safeguards against man-in-the-middle attacks, which involve the unauthorized interception and modification of communication between two parties by a malicious actor. By encrypting and authenticating data, SSL enhances the security stance of IaaS environments. This ensures that the confidentiality and security of users' information are maintained throughout internet transmission [23]. In addition, frequent upgrades are made to SSL/TLS protocols to address emerging security concerns. This mitigates the impact of evolving threats and vulnerabilities by enabling cloud-based IaaS providers to employ the most recent encryption standards [24]. SSL/TLS enhances confidence and trust in the cloud computing ecosystem by serving as a critical security protocol in Infrastructure as a Service (IaaS).

The rapid growth of cloud computing infrastructure has

introduced new challenges, particularly in ensuring robust load balancing and security within the Infrastructure as a Service (IaaS) environment. Addressing these challenges is critical to optimizing resource utilization and safeguarding sensitive data. Despite existing load-balancing techniques and security measures, vulnerabilities persist, necessitating innovative solutions. This research aims to enhance load balancing efficiency and bolster cloud computing security in the IaaS framework by leveraging Secure Sockets Layer (SSL) encryption. By integrating SSL into the load balancing mechanism, we aim to mitigate potential threats and vulnerabilities while optimizing resource allocation, thus contributing to the advancement of secure and efficient cloud computing infrastructures.

The novel contribution of this study is followed as:

- In this study, we propose a novel approach to enhance load balancing and bolster cloud computing security within the Infrastructure as a Service (IaaS) environment through the integration of the Secure Sockets Layer (SSL) protocol.
- Traditional load-balancing techniques often overlook the critical aspect of securing data transmissions, leaving systems vulnerable to potential breaches. By leveraging SSL, we not only optimize resource allocation across servers to mitigate overloads and improve efficiency but also ensure end-to-end encryption of data traffic, safeguarding against unauthorized access and data tampering.
- Our contribution lies in the seamless integration of SSL within the load-balancing framework, offering a robust solution that prioritizes both performance optimization and security reinforcement in cloud infrastructures.
- Through empirical evaluations and comprehensive analysis, we demonstrate the efficacy of our approach in enhancing the resilience and reliability of IaaS environments, thereby paving the way for a more secure and efficient cloud computing paradigm.

The remaining structure of this paper is followed as: section 2 discusses the reviewed literature work; section 3 presents the methodology and section 4 represents the findings of our study; section 5 intends to conclusion and future work of our study.

II. LITERATURE REVIEW

Al Reshan et.al (2023) [25] discussed cloud computing as the dynamic provisioning of resources for the suggested of delivering services to end consumers via the internet. Prerequisites for cloud computing deployment included load balancing, resource discovery, security, and scheduling, among others. One of the primary obstacles encountered in addressing these investigation concerns was load balancing. As a consequence, there has been a growing emphasis in recent years on investigating various static and dynamic algorithms that aim to achieve optimal outcomes. This suggested Swarm Intelligence (SI) as a potential load-balancing technology for cloud computing. Numerous alternatives (including genetic algorithm, ACO, PSO, BAT, GWO, and many others) were examined in the literature; however, none of them accounted for the convergence time of load balancing with global optimization. Particular emphasis was placed on the Grey Wolf Optimisation (GWO) and Particle Swarm Optimisation (PSO) algorithms. A GWO-PSO combined technique that leverages global optimization and rapid convergence. The integration of these two techniques generated improved system efficiency and resource distribution, thereby effectively resolving the load-balancing issue. In contrast to conventional methodologies, the outcomes of this investigation exhibited considerable promise due to their ability to attain globally optimized rapid convergence and an overall reduction in response time.

Zhou et.al (2023) [26] proposed that organizations that depended on cloud service providers (CSP) to ensure the efficient operation of services, as well as conformance with the service agreement, quality of service, and performance evaluation, encountered a substantial obstacle in the domain of cloud computing about load balancing. Through the distribution of processing capacity across tasks, load balancing aimed to substantially enhance system performance. Due to the vast solution space, load balancing in cloud computing was classified as an "NP-hard" challenge. As an outcome, additional time was required to ascertain the optimal course of action. For these issues, few methods might be capable of generating an optimal solution in a polynomial time. The investigations have demonstrated that techniques based on metaheuristics can effectively and expeditiously resolve comparable problems. Different metaheuristic load-balancing techniques for cloud computing are compared. Evaluation criteria included makespan time, degree of imbalance, response time, processing time at the data center, transit time, and resource utilization. Following performance metrics, the simulation outcomes demonstrated that several meta-heuristic load-balancing strategies were effective. Through particle swarm optimization, makespan, flow time, throughput time, reaction time, and degree of imbalance were all improved with greater success.

Shafiq et.al (2022) [27] determined the robust concept of cloud computing enabled customers and businesses to acquire services following their specific requirements. The model provided an extensive array of services, including but not limited to storage, deployment platforms, and straightforward access to web services. Businesses encountered challenges in ensuring application performance remained compliant with Quality of Service (QoS) metrics and the Service Level Agreement (SLA) mandated by cloud providers due to the prevalent challenge of load balancing in the cloud. Challenging was the task for cloud service providers to equitably distribute the workload across all servers. A successful LB strategy ought to have optimized the

utilization of virtual machine (VM) resources to maximize and guarantee a significant level of user satisfaction. The research paper incorporated a comprehensive examination of various load balancing strategies—both static and dynamic—implemented in a cloud environment that was naturally influenced, to improve the overall performance and response time of the data center.

Humayun et.al (2022) [28] discussed that cloud computing (CC) was an on-demand, "pay-per-use" service that provided computing resources. SaaS, the preeminent and widely adopted service platform from CC, was utilized by billions of businesses due to its manifold advantages. Encouraging cloud adoption required the resolution of security concerns. R&P, or investigation and practice, investigates potential solutions for SaaS security issues. There is a dearth of systematic investigation that has compiled and analyzed security issues and solutions. An exhaustive multivocal literature review (MVLR) of SaaS security challenges/issues and best practices was conducted for this study to close this knowledge divide and provide an up-to-date (SOTA) picture. To determine if R&P had similar or different views, we examined SaaS security problems and recommendations gathered from academic and unofficial sources. Through the evaluation and analysis of the chosen papers, best practices for R&P to enhance security and security concerns in SaaS computing were identified. This MVLR was utilized by SaaS users to identify several security hazards that required investigation and improvement. Anonymity and access management, data breaches and leakage, governance and regulatory compliance/SLA compliance, and hostile insiders emerged as the prevailing security concerns in Florida and Georgia, as determined by the analysis. Additionally, R&P held the view that robust encryption, regulatory and SLA compliance, multifactor authentication, and adherence to current security policies and standards were the most critical responses.

Alghofaili et al., (2021) [29] presented the onset of the "cloud computing" craze, prominent corporations such as Microsoft, Amazon, and Google were at the forefront of developing and delivering cost-effective, sophisticated cloud computing systems to their clientele. Users' primary objection to cloud computing was security concerns, which incited them to vehemently oppose the implementation of systems. It was critical to maintain the security of cloud computing, particularly the infrastructure. The domain of cloud infrastructure security has been a topic of numerous research endeavors; however, certain deficiencies have persisted without detection, and novel obstacles have emerged. The possible security issues with cloud architecture at the data, host, network, and application levels were carefully investigated It examined the primary infrastructure concerns that had the potential to impact the business model of cloud computing. Furthermore, known ways to address the many security vulnerabilities that crop up at each phase have been discussed and debated. To support the process of problem-solving, a comprehensive summary of the unresolved matters was provided. It was determined, following a comprehensive analysis of the existing obstacles, that certain cloud characteristics—including elasticity, multitenancy, and adaptability—present new challenges at each infrastructure level. It was demonstrated in particular that multi-tenancy had the most significant effect on all infrastructure layers due to the numerous security issues it can cause, including data loss, privacy infringements, abuse, and inaccessibility.

Dastres et.al (2020) [30] examined the outlook being among them, was introduced to enable network users to exchange information electronically via the web of data. By implementing secure and dependable data-sharing software, the number of individuals accessing a website or even the stories of a building may decrease. To facilitate the development of intricate communication systems, users of the data-sharing websites required a network infrastructure that was dependable, secure, and quick. A multitude of encoding algorithms and techniques were investigated to bolster the security of data-sharing systems through the prevention of unauthorized access by hackers to the transmitted data. A feasibility investigation was carried out to investigate the possibility of textual communication between users of a local network to improve network security. The investigation into encryption and decryption algorithms aimed to enhance network security through the prevention of unauthorized access by hackers. Implementing traffic restrictions within the website environment may contribute to enhancements in the velocity, precision, and safeguarding of data-sharing systems across the web and network. Additionally, it may enable network participants to communicate dependably and securely.

Alkhafajee et.al (2020) [31] discussed the Internet of Things (IoT) as a progressive iteration of the conventional Internet. Through the Internet of Things (IoT), every object in our lives can be linked to a network or one another to communicate information and carry out specific tasks. Several security hazards were introduced when multiple devices were integrated, particularly when performed by inexperienced users. Additional security vulnerabilities were discovered in several prevalent IoT communication protocols. However, security itself resulted in increased expenses, which negatively impacted overall performance. MQTT was a client-server architecture that employed a lightweight publish-subscribe messaging transport model. It was one of the most extensively used protocols for the Internet of Things. Due to its design intent to operate through the TCP protocol, MQTT by default did not offer any security measures. The MQTT protocol may therefore be fortified through the implementation of Transport Layer Security (TLS). The effect of two scenarios on the security and efficacy of the MQTT protocol. When the security of the MQTT protocol is supported by the TLS protocol. In the second scenario, the transmission is conducted using the standard MQTT protocol,

which lacks any form of data security safeguards. Security and performance were compromised when utilizing the MQTT protocol, regardless of whether the TLS protocol was employed.

III. METHODOLOGY & EXPERIMENTATION

A comprehensive account of the investigation undertaken to provide a secure architecture for cloud-hosted apps can be found in [24], [25]. Before the release of our IaaS, it used a gateway-level F5, Inc. BIG-IP box strategy. To enhance apps, we build a virtual instance of the product and utilize two of its primary features. The first of these two characteristics is the load balancing mechanism (LTM), which is also in charge of expanding the SSL service. Nevertheless, it is recommended that two actual BIG-IP devices be used for this experimental investigation. An SSL VPN, which is integrated into all web browsers, assists in establishing a private virtual network over the Internet by using authentication and encryption technologies [26, 27]. It intends to implement BIG-IP between remote clients and cloud-based application servers. The recommended cloud computing service is going to use an SSL VPN secure connection channel created by an F5 machine when a user attempts to access a hosted application. By clicking the F5 button, load balancing will be performed to identify the optimal server. The Local Traffic Manager Module (LTCM) and Access Policy Manager (APM) are included in the F5 device, which makes integration easier. High Availability (HA) is also proposed using two BIG-IP APM machines in active standby deployment mode. BIG-IP features of LTM and APM offer support for an authenticated client session in the event of a failure (Figure 2). Requests that occur promptly following a failover shall be forwarded automatically to the active unit, ensuring that session connections remain operational without any observable disruption.

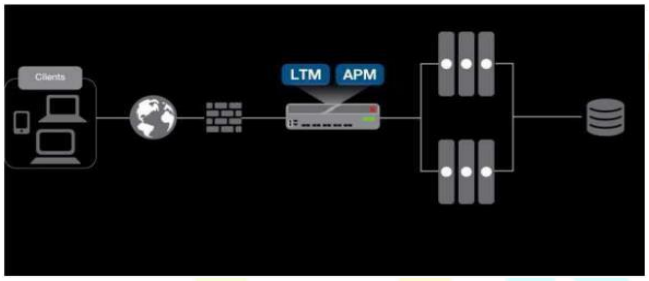

Figure 2. Diagram showing the proposed layout of APM and LTM working as a composite unit or module

IV. RESULTS & DISCUSSION

These investigations have involved two application servers. Additionally, it is protected by the virtual version of BIG-IP developed by F5, Inc. Installing the virtual edition or OVF file that F5, Inc. offers in a VMware environment is the first step (Figure 3). Network access, portal access, client and clientless features, SSL VPN, and other secure access functionalities are used together to build a secure access solution for our IaaS infrastructure. This allows us to test a cloud-hosted application. The following are the criteria that the experimental approach considers:

1. The suggested system would be capable of supporting at least 100 people at once.
2. Configuration changes are possible to grant various types of access depending on whether the access required is an application, network, or portal.
3. The URI is published on a portal to enable assorted SSO applications to access either Linux or Windows operating system software.
4. The suggested technique could handle four application servers for load balancing and 100 concurrent users.
5. The suggested approach makes use of HA in an active-active setup.

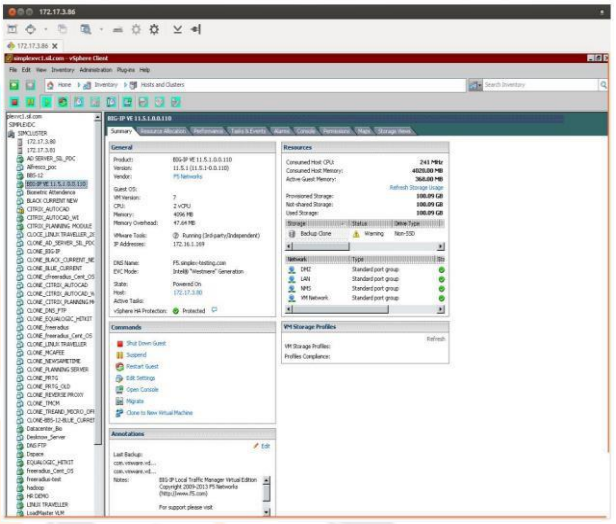

Figure 3. Installation of F5 .ovf file on virtual platform

To use APM and LTM capabilities for our lab investigations, we made use of an evaluation license. The following screenshots (Figures 4a–4d) show how we set up our solution for IaaS deployment mode.

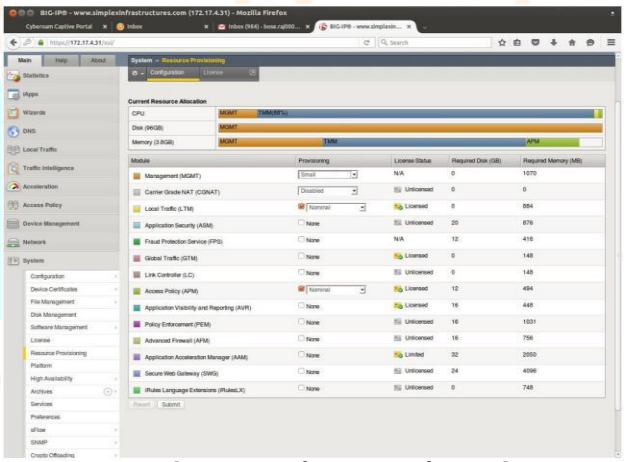

Figure 4 a: Step-by-step configuration of our solution in IaaS development mode

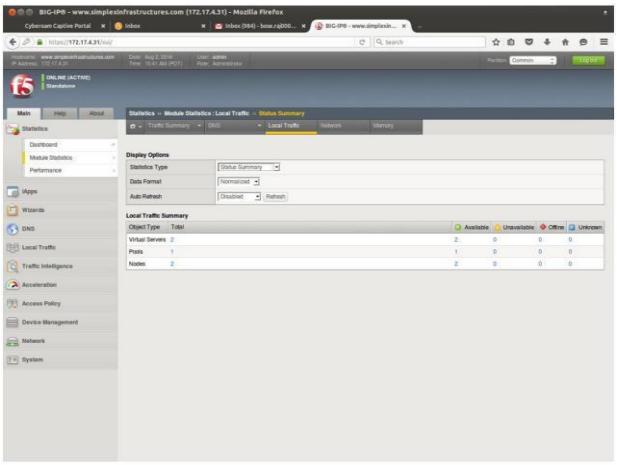

Figure 4 b: Step-by-step configuration of our solution in IaaS development mode

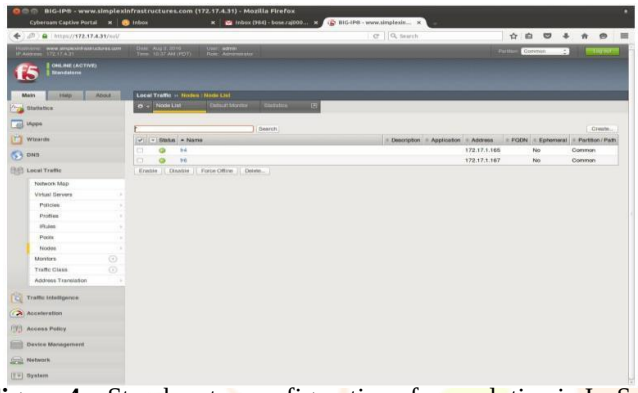

Figure 4c: Step-by-step configuration of our solution in IaaS development mode

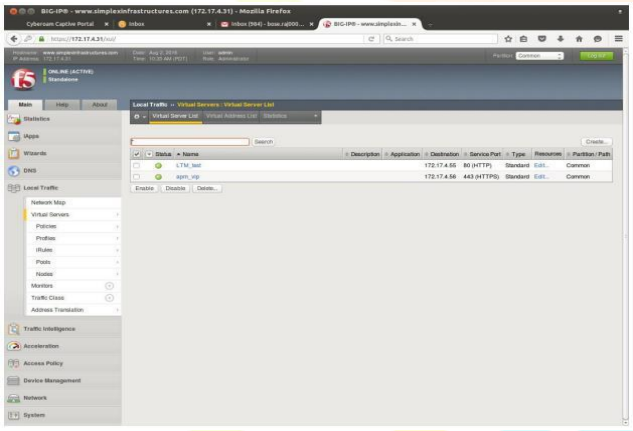

Figure 4 d: Step-by-step configuration of our solution in IaaS development mode

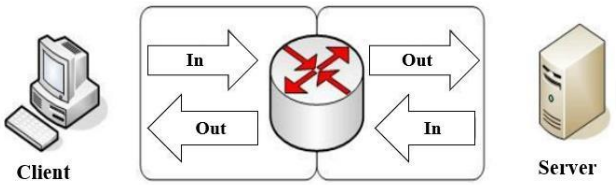

Figure 5. Inbound and outbound data procedure

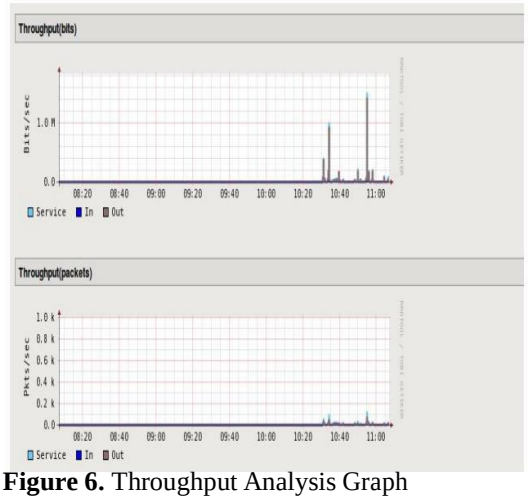

Figure 6. Throughput Analysis Graph

The default setup of our virtual server keeps it client-side accessible, independent of the gateway servers using it. By design, the virtual server may direct data traffic towards itself and service users. That is displayed in Figure 5. Having 100 users connect at once can be used to assess the performance of our product. The experiment's outcomes, as illustrated in Figure 6, demonstrate a notable performance improvement.

V. CONCLUSION

In summary, load balancing and cloud computing security are greatly enhanced when SSL (Secure Sockets Layer) is added to an Infrastructure as a Service (IaaS) environment. SSL uses encryption and authentication procedures to protect sensitive data during data transfer between clients and servers. These techniques also guard against unwanted access and interference. SSL helps load-balancing processes work better by distributing incoming traffic among several servers, which increases security and efficacy. SSL can create encrypted connections between servers and clients, which reduces the risk of data interception and tampering and allows for smooth communication. This facilitates enhanced resource allocation and improved overall efficacy of the Infrastructure as a Service (IaaS). In addition, SSL serves as a critical component in fortifying the security of cloud computing by protecting a multitude of cyber threats, including eavesdropping, man-in-the-middle assaults, and data breaches. By employing SSL certificates and protocols, a secure environment is created for the exchange of data, thereby fostering trust among users and stakeholders concerning the privacy and integrity of their information. An Infrastructure as a Service (IaaS) environment's use of SSL often indicates a proactive approach to lower security concerns and improve load-balancing capabilities. Adding SSL to cloud-based services is crucial to enhancing their resilience and dependability since cloud computing is growing in popularity among enterprises due to its flexibility and scalability. By routinely monitoring, making adjustments, and adhering to established norms, SSL, load balancing, and

cloud computing security may work together better to manage new technological difficulties and satisfy user expectations. Future endeavours may focus on integrating AI-driven algorithms for dynamic load distribution and anomaly detection, alongside continuous advancements in cryptographic techniques to uphold the resilience of cloud environments against emerging security challenges.

REFERENCES

[1] Ang'udi, Janet Julia. "Security challenges in cloud computing: A comprehensive analysis." World Journal of Advanced Engineering Technology and Sciences 10.2 (2023): 155-181.

[2] Marianthony Renjitham, Archana Jenis, et al. "The Intelligent Connection Management Model to Enhance the Security of Cloud Computers in High-Density Fog Networks." Engineering Proceedings 59.1 (2023): 105.

[3] Eyeleko, Anselme Herman, and Tao Feng. "A Critical Overview of Industrial Internet of Things Security and Privacy Issues Using a Layer-Based Hacking Scenario." IEEE Internet of Things Journal (2023).

[4] Patel, Rahul K., Piyush Gidwani, and Nikunj R. Patel. "Privacy Preservation and Cloud Computing." Privacy Preservation and Secured Data Storage in Cloud Computing. IGI Global, 2023. 88-107.

[5] Dass, Ashish Kumar, et al. "Virtualization in Cloud Computing: Transforming Infrastructure and Enhancing Efficiency." Research and Applications: Emerging Technologies 5.3 (2023): 26-40.

[6] Sobh, Tarek S., Ashraf Elgohary, and M. Zaki. "Performance improvements on the network security protocols." International Journal of Network Security 6.1 (2008): 103-115.

[7] Mallikarjuna, B., and D. A. K. Reddy. "The role of load balancing algorithms in next generation of cloud computing." Control Syst 11 (2019): 20.

[8] Toni, Janevski., Borislav, Popovski. (2023). ANTICIPATED DEVELOPMENTS IN CLOUD SERVICES WITH A FOCUS ON THE INFRASTRUCTURE-AS-A-SERVICE (IaaS) MODEL. Journal of Electrical Engineering and Information Technologies, 8(1):29-38. doi: 10.51466/jeeit 2381205029j

[9] B., Vivekanandam., Midhunchakkaravarthy. (2022). mplementation of a Security System in IaaS Cloud Server through an Encrypted Blockchain. Journal of Soft Computing Paradigm, 3(4):336-348. doi: 10.36548/jscp.2021.4.008

[10] K., Karthikeyan., A., Bharathi. (2022). Performance evaluation of IaaS cloud using Stochastic Neural Network. Journal of Intelligent and Fuzzy Systems, 43(4):4613-4628. doi: 10.3233/jifs-220501

[11] (2023). AI Cloud Computing in Education. 37-42. doi: 10.55529/ijrise.34.37.42

[12] (2022). Evaluation of the Performance of Tightly Coupled Parallel Solvers and MPI Communications in IaaS From the Public Cloud. IEEE Transactions on Cloud Computing, 10(4):2613-2622. doi: 10.1109/tcc.2021.3052844

[13] (2023). A Novel Approach to Load Balancing and Security using SSL in Cloud Computing Environment. International Journal For Multidisciplinary Research, 5(3) doi: 10.36948/ijfmr.2023.v05i03.4171

[14] Shobha, K, R. (2022). Load Balancing in Cloud Computing Environment. 1-9. doi: 10.1109/ICWITE57052.2022.1017 6241

[15] Meenal, Sachdeva., R., (2022). Load balancing in cloud computing. Scholarly research journal for humanity science & English language, 10(53):13492-13504. doi: 10.21922/srjhsel.v10i53.11651

[16] Nisha, Verma., Bhavesh, N., Gohil. (2023). Load balancing in Cloud Computing Environment using Modified Genetic Algorithm. 1-8. doi: 10.1109/ISCON57294.2023.10111981

[17] (2023). Load balancing in Cloud Computing Environment using Modified Genetic Algorithm. doi: 10.1109/iscon57294. 2023.10111981

[18] Shafiq, Dalia Abdulkareem, N. Z. Jhanjhi, and Azween Abdullah. "Load balancing techniques in cloud computing environment: A review." Journal of King Saud University-Computer and Information Sciences 34, no. 7 (2022): 3910-3933

[19] Jensen, Meiko, et al. "On technical security issues in cloud computing." 2009 IEEE international conference on cloud computing. Ieee, 2009.

[20] Sengupta, Shubhashis, Vikrant Kaulgud, and Vibhu Saujanya Sharma. "Cloud computing security--trends and research directions." 2011 IEEE World Congress on Services. IEEE, 2011.

[21] Bhadauria, Rohit, and Sugata Sanyal. "Survey on security issues in cloud computing and associated mitigation techniques." arXiv preprint arXiv:1204.0764 (2012).

[22] Liu, Anyi, et al. "Iotverif: Automatic verification of SSL/TLS certificate for IoT applications." IEEE Access 9 (2019): 27038-27050.

[23] GARG, DR PRACHI, and DR SANDIP KUMAR GOYAL. "Secure service provider platform for cloud environment." (2020).

[24] Parast, Fatemeh Khoda, et al. "Cloud computing security: A survey of service-based models." Computers & Security 114 (2022): 102580.

[25] Al Reshan, Mana Saleh, et al. "A fast converging and globally optimized approach for load balancing in cloud computing." IEEE Access 11 (2023): 11390-11404.

[26] Zhou, Jincheng, et al. "Comparative analysis of metaheuristic load balancing algorithms for efficient load balancing in cloud computing." Journal of cloud computing 12.1 (2023): 85.

[27] Shafiq, Dalia Abdulkareem, N. Z. Jhanjhi, and Azween Abdullah. "Load balancing techniques in cloud computing environment: A review." Journal of King Saud University-Computer and Information Sciences 34.7 (2022): 3910-3933.

[28] Humayun, Mamoona, et al. "Software-as-a-service security challenges and best practices: A multivocal literature review." Applied Sciences 12.8 (2022): 3953.

[29] Alghofaili, Yara, et al. "Secure cloud infrastructure: A survey on issues, current solutions, and open challenges." Applied Sciences 11.19 (2021): 9005.

[30] Dastres, Roza, and Mohsen Soori. "Secure socket layer (SSL) in the network and web security." International Journal of Computer and Information Engineering 14.10 (2020): 330-333.

[31] Alkhafajee, A. R., et al. "Security and performance analysis of MQTT Protocol with TLS in IoT Networks." 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA). IEEE, 2021.