Enhancing Cloud Security with Zero Trust in Infrastructure as a Service IaaS

[1]**Venkata Surya Bhavana Harish Gollavilli,**
Asurion, TN, USA
venharish990@gmail.com

[2]**Thanjaivadivel M**
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Assistant professor
chennai, india
thanjaivadivel@gmail.com

Abstract

The rapid adoption of Infrastructure as a Service (IaaS) has introduced significant security challenges, particularly around trust, data protection, and access control. This paper presents frameworks such as Cloud-Trust and Trusted-Cloud to enhance the security posture of IaaS environments. Through trust evaluation criteria like provider reputation and service availability, the frameworks help improve decision-making when selecting IaaS providers. Key security measures, including cryptographic techniques and automated security policies, are discussed, emphasizing the importance of Zero Trust principles. Latency increased from 50 ms to 80 ms after Zero Trust implementation, and incident response times improved from 30-40 minutes to 15-25 minutes, demonstrating the effectiveness of Zero Trust in enhancing security and response speed.

Keywords: Infrastructure as a Service (IaaS), Zero Trust Security, Trust Evaluation, Incident Response Time, Identity and Access Management (IAM), Data Encryption.

1. INTRODUCTION

The rapid adoption of cloud computing, particularly in the Infrastructure as a Service (IaaS) model, has significantly transformed the way businesses and individuals utilize IT resources. However, concerns surrounding security and trust have become critical factors in the widespread adoption of IaaS. To address these concerns, various security frameworks and trust models have been developed, focusing on ensuring confidentiality, integrity, and availability in cloud environments. A security assessment model known as Cloud-Trust has been introduced to evaluate the security of IaaS clouds. This model identifies key trust factors such as access control, network security, and data protection, providing a comprehensive approach to trust assessment in cloud infrastructure. The work emphasizes the need for transparent and robust security measures to foster confidence in IaaS cloud services [1]. In addition to these security frameworks, a novel evaluation framework has been proposed to improve the trust level of IaaS. It recognizes the importance of trust in fostering secure interactions between users and cloud providers. This approach introduces several evaluation criteria, including provider reputation, service availability, and trustworthiness of the underlying cloud infrastructure. By focusing on these dimensions, the framework aims to improve decision-making when selecting IaaS providers. This work provides valuable insights into how trust factors can be quantified and utilized to enhance the security posture of cloud computing services [2].

Another study delves into the concept of trust within the IaaS framework by presenting a cloud security model known as Trusted-Cloud. This model focuses on securing virtualized resources and mitigating potential threats in cloud environments. The Trusted-Cloud framework leverages both cryptographic techniques and trust management systems to ensure that data and resources are protected from unauthorized access or malicious actors. The model is adaptable, providing a versatile solution for various IaaS environments while maintaining a high level of security and trust [3]. Further research explores the challenges of security in cloud computing, proposing a trust-based approach to enhance security within IaaS infrastructure. This model integrates security measures such as data encryption, authentication protocols, and continuous monitoring to create a more secure cloud environment. The study argues that trust plays a fundamental role in determining the overall security of a cloud infrastructure and that a proactive approach to trust management is necessary to combat the evolving landscape of cyber threats. The work highlights the importance of adopting comprehensive security measures

that not only address technical vulnerabilities but also consider trust as an essential element for successful cloud computing adoption [4].

In the context of IaaS cloud security, an in-depth analysis of the challenges and solutions that organizations face when deploying IaaS services has been presented. The work covers a broad range of security challenges, including data privacy, multi-tenancy issues, and the complexities of ensuring compliance with regulations. A set of solutions has been proposed to address these challenges, focusing on the need for robust authentication, secure data storage, and advanced encryption techniques. The necessity of establishing strong trust relationships between cloud providers and consumers is highlighted as key to mitigating security risks and ensuring the success of cloud deployments [5]. Building on the need for trust in cloud computing, an intelligent attribute-based access control (ABAC) model has been designed to enhance security in IaaS environments. By incorporating attributes such as user roles, location, and time into access control policies, this model provides a more dynamic and context-aware approach to cloud security. The research underscores the importance of adaptive security mechanisms that can respond to the changing nature of cloud services and user requirements. The use of ABAC is seen as a critical step in building trust by providing fine-grained control over who can access specific cloud resources [6].

Furthering the discussion on trust criteria, common trust criteria for evaluating and selecting IaaS providers have been proposed. Trust plays a significant role in the decision-making process for cloud service adoption and should be integrated into the evaluation of IaaS providers. The work outlines key factors such as service reliability, security measures, and provider transparency. By focusing on these trust criteria, organizations can make more informed decisions about which IaaS providers to engage with, ultimately leading to better security and a stronger trust relationship between consumers and providers [7]. A novel design to increase trust within the IaaS cloud model has also been introduced by incorporating a comprehensive approach to trust management. The importance of ensuring data confidentiality and integrity in IaaS environments is emphasized, along with a layered security model that incorporates both preventative and detective measures. This work aims to establish a trustworthy cloud infrastructure by focusing on transparency and accountability in cloud service delivery. By enhancing the trustworthiness of cloud providers, it is argued that users will be more willing to adopt IaaS services with confidence, knowing that their data and resources are adequately protected [8].

PROBLEM STATEMENT

The challenges and opportunities in resource scheduling for Infrastructure as a Service (IaaS) cloud computing have been discussed, emphasizing the complexities of balancing resource utilization and ensuring SLA compliance in dynamic cloud environments. It is proposed that intelligent scheduling mechanisms, such as machine learning and predictive analytics, can optimize cloud performance [17]. The lack of standardized trust evaluation models in IaaS has been highlighted, stressing the importance of a comprehensive framework to assess the trustworthiness of cloud providers, which could increase user confidence and security in cloud services [18]. A focus has been placed on identifying cloud security threats that hinder the adoption of cloud computing, arguing for the design of robust security frameworks to address evolving security challenges, ensuring that users feel more secure in transitioning to the cloud [19]. The role of Service Level Agreements (SLAs) in building trust between IaaS providers and customers has been explored, emphasizing that clear and enforceable SLAs are essential for ensuring transparency, accountability, and mutual trust in cloud computing [20].

Objectives:

- Enhance Cloud Security: Propose a comprehensive security model incorporating Zero Trust principles to strengthen the security posture of IaaS environments.
- Trust Evaluation: Introduce frameworks such as Cloud-Trust and Trusted-Cloud to assess and improve the trustworthiness of IaaS providers, focusing on criteria like provider reputation, service availability, and security measures.
- Minimize Security Risks: Implement automated security policies to proactively identify and remediate vulnerabilities, ensuring compliance with best practices and reducing the risk of data breaches or unauthorized access.
- Improve Incident Response: Demonstrate how Zero Trust security improves the speed of incident response, reducing the time required for remediation and enhancing operational efficiency.
- Evaluate Latency Impact: Analyze the impact of Zero Trust implementation on system latency and performance, providing a clear understanding of the trade-offs between enhanced security and operational efficiency.

2. LITERATURE SURVEY

The concept of cloud security has become a focal point in the development and deployment of cloud computing services, particularly in Infrastructure as a Service (IaaS) environments. An in-depth analysis of the infrastructure required for cloud security has been provided, offering a solutions-based perspective. The importance of building a secure cloud infrastructure that includes robust access control, encryption, and continuous monitoring is emphasized. The need for a holistic approach that integrates various security solutions, such as firewalls, intrusion detection systems, and secure communication protocols, to protect cloud environments is highlighted. By building a comprehensive security infrastructure, it is argued that cloud providers can ensure the protection of user data and services while maintaining the overall reliability and trust of the cloud platform [9].

A distributed trust protocol for IaaS cloud computing has been explored, aiming to enhance security through a decentralized trust management system. This protocol is designed to distribute trust calculations across multiple entities, helping to reduce the risk of single points of failure. The approach involves assessing trust levels based on various factors such as service performance, data integrity, and security posture. By decentralizing trust management, the protocol provides a more scalable and resilient security solution for IaaS environments, thus improving the overall trustworthiness of cloud services. This work underscores the importance of creating systems that can dynamically adapt to security threats while maintaining trust between cloud users and providers [10].

The issue of security attacks in cloud computing has been addressed by developing a taxonomy of attacks and proposing intrusion detection and prevention as a service (IDPaaS). A range of potential threats to cloud environments, such as denial of service (DoS) attacks, data breaches, and unauthorized access, has been identified. A layered security architecture that includes detection, prevention, and response mechanisms is proposed. The focus is on automating the intrusion detection process by utilizing machine learning techniques to identify abnormal patterns of activity. This approach ensures that security measures are continuously adapted to evolving threats, providing the protection for cloud services. It is argued that IDPaaS is a crucial component for maintaining security and trust in IaaS platforms [11].

The idea of applying security policies and service level agreements (SLAs) to enhance security in IaaS cloud environments has been introduced. By defining clear security policies within SLAs, both cloud providers and consumers can ensure that security expectations are met and that adequate measures are in place to address potential vulnerabilities. The focus is on aligning security policies with contractual agreements, thus providing a legal framework for cloud security. It is emphasized that SLAs play a significant role in fostering trust, as they hold cloud providers accountable for ensuring the security of their services. By incorporating security into SLAs, this work helps to bridge the gap between service delivery and customer trust, promoting better security practices and enhancing overall cloud security [12].

A novel trust management system for cloud computing IaaS providers has been proposed, addressing the growing concerns about trust and security in cloud environments. This system incorporates several trust factors, such as reputation, service availability, and security certifications, to build a comprehensive trust model. The system uses a dynamic approach, where trust levels are continuously updated based on the provider's performance and feedback from users. This model aims to provide a transparent and reliable trust framework that can help users make informed decisions when selecting IaaS providers. By focusing on trust management, this work enhances the security of cloud computing services and helps to build stronger relationships between users and providers, thus fostering a more secure cloud ecosystem [13].

An examination of the state of public IaaS cloud security has been conducted, identifying various challenges and vulnerabilities that exist in these systems. A comprehensive review of current security practices has been provided, highlighting areas where improvements are needed. Key security concerns, such as multi-tenancy, data isolation, and compliance with industry regulations, are discussed. It is emphasized that public IaaS cloud providers must implement more stringent security controls and work collaboratively with users to ensure that data protection measures are effective. This work contributes to the broader understanding of IaaS cloud security by identifying gaps and proposing solutions to address these challenges [14].

The design and implementation of FROST, a digital forensic tool tailored for the OpenStack cloud computing platform, have been examined. FROST is designed to provide forensic analysis capabilities for cloud environments, enabling the investigation of security incidents and ensuring that digital evidence can be collected and preserved. The importance of forensic readiness in cloud security is highlighted, especially as cloud platforms become more widely used in sensitive applications. By implementing forensic tools like FROST, organizations can strengthen their ability to investigate security breaches and ensure accountability in cloud environments. This work provides valuable insights into how cloud platforms can integrate forensic tools to enhance security and maintain data integrity [15].

Cloud computing security has been enhanced by proposing the use of the Advanced Encryption Standard (AES) algorithm to secure data within cloud environments. It is argued that AES, as a symmetric-key encryption algorithm, offers strong security for sensitive data stored and transmitted in the cloud. The implementation of AES is explored as a means to safeguard cloud data against unauthorized access and tampering. By focusing on encryption, this work contributes to the broader effort to improve cloud security by providing a practical solution to one of the fundamental challenges of cloud computing data privacy. This approach ensures that data remains secure while being processed in the cloud, helping to increase user trust in cloud services [16].

3. PROPOSED METHDOLOGY

Figure 1: outlines a step-by-step workflow for implementing Zero Trust (ZT) in IaaS environments. It begins by defining the scope and objectives, including identifying critical assets and establishing ZT principles. Next, it assesses current security through vulnerability audits and IAM policy reviews. The deployment phase enforces ZT controls like IAM, micro-segmentation, and monitoring, followed by tracking performance metrics to measure effectiveness. Automation strengthens security via IaC scans and Zero Trust Network Access (ZTNA), while data and workloads are secured through encryption. The workflow ensures a structured approach to adopting Zero Trust, though it could benefit from reordering steps (e.g., securing data earlier) and adding feedback loops for continuous improvement.

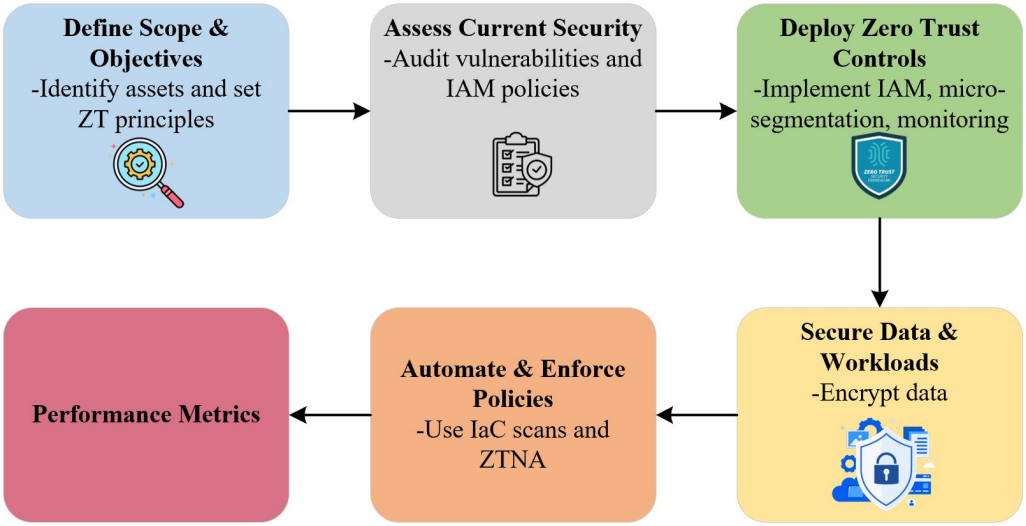

Figure 1: Zero Trust Implementation Workflow in IaaS Environments

3.1 DEFINE SCOPE

The Define Scope & Objectives phase establishes the foundation for implementing Zero Trust in an IaaS environment by clearly outlining what needs to be protected and how. This involves identifying critical assets such as virtual machines, storage systems, APIs, and network components, as well as mapping their interdependencies. Simultaneously, core Zero Trust principles like least-privilege access, continuous verification, and assume-breach mindset are formalized to guide subsequent security measures. The scope also aligns with business goals and compliance requirements (e.g., GDPR, HIPAA) to ensure regulatory adherence. By defining boundaries and priorities upfront, this phase ensures targeted, efficient deployment of Zero Trust controls while avoiding unnecessary complexity or coverage gaps.

3.2 ASSESS CURRENT SECURITY

The Assess Current Security phase involves a thorough evaluation of the existing security posture within the IaaS environment to identify vulnerabilities, misconfigurations, and gaps that could undermine Zero Trust adoption. This includes auditing identity and access management (IAM) policies to detect excessive permissions, inactive accounts, or weak authentication methods (e.g., missing MFA). Network and workload configurations are scrutinized for exposed ports, unsegmented traffic, or outdated encryption protocols. Additionally, logs and incident records are analysed to uncover past breaches or suspicious activities. Tools like cloud security posture management (CSPM) and vulnerability scanners automate parts of this process. The output is a risk profile that prioritizes issues such as overprivileged users or unpatched systems to address during Zero Trust

implementation. This assessment ensures the subsequent controls are tailored to the environment's specific weaknesses.

3.3 AUDIT IAAS FOR VULNERABILITIES

Auditing IaaS for vulnerabilities and misconfigurations involves systematically scanning the cloud infrastructure including virtual machines, containers, storage buckets, and network settings to identify security gaps such as unpatched software, exposed APIs, overly permissive firewall rules, or weak encryption practices. Using tools like CSPM (Cloud Security Posture Management) and vulnerability scanners, this process detects deviations from security best practices (e.g., CIS benchmarks) and compliance standards (e.g., NIST, ISO 27001). The audit also reviews Infrastructure as Code (IaC) templates (e.g., Terraform, CloudFormation) for insecure defaults, while runtime environments are checked for drift from intended configurations. Findings are prioritized based on risk severity, enabling targeted remediation such as patching CVEs, tightening IAM policies, or segmenting networks to harden the environment before Zero Trust controls are deployed. This proactive step minimizes attack surfaces and ensures a secure foundation for Zero Trust implementation.

$$\text{RiskScore}(V_i) = \frac{\text{Severity}(V_i) \times \text{Exploitability}(V_i)}{\text{CompensatingControls}(V_i)} \quad (1)$$

3.3.1 Zero Trust Network Access

Zero Trust Network Access (ZTNA) replaces traditional perimeter-based security with granular, identity-centric access controls for your IaaS environment. It enforces the principle of "never trust, always verify" by dynamically granting least-privilege access to workloads, users, or devices only after continuous authentication and context checks (e.g., device posture, user role, and behavioral analytics). Unlike VPNs, ZTNA operates on a need-to-know basis, micro-segmenting access to specific resources (e.g., VMs, APIs) without exposing the entire network. Integrated with IAM and SIEM tools, it logs all access attempts for the anomaly detection. For your workflow, ZTNA ensures secure remote access to cloud infrastructure while minimizing attack surfaces, aligning with the automated policy enforcement and micro-segmentation steps in your Zero Trust framework

3.3.2Micro-segmentation

Micro-segmentation is a security technique that divides a network into smaller, isolated segments, each with its own security controls and policies. Unlike traditional perimeter-based security models, which focus on securing the outer boundaries of a network, micro-segmentation limits the lateral movement of attackers within the network by enforcing strict access controls at a granular level. This involves segmenting the network based on workloads, applications, or users, and applying policies that control which resources can communicate with one another. By isolating sensitive data and services within these smaller segments, micro-segmentation enhances security, reduces attack surfaces, and ensures that even if an attacker gains access to one part of the network, they cannot easily move to other parts, thus providing more robust protection in cloud and data centre environments.

$$S_{\text{Access}} = f(\text{ Segment , Policy , Authentication }) \quad (2)$$

3.4 SECURE DATA

The Secure Data phase focuses on safeguarding sensitive information within the IaaS environment through robust encryption and access controls. This involves encrypting data both at rest (e.g., in storage buckets, databases) using AES-256 or similar standards, and in transit (e.g., API calls, inter-service communication) via TLS 1.2/1.3. Key management systems (e.g., AWS KMS, Azure Key Vault) ensure secure encryption key storage and rotation. Additionally, data classification policies tag assets by sensitivity (e.g., PII, PHI) to enforce granular access controls aligned with Zero Trust principles. Techniques like tokenization or masking may further protect high-risk data. By integrating these measures with IAM and micro-segmentation, the phase ensures that even if perimeter defense fail, data remains inaccessible to unauthorized entities closing critical gaps in the Zero Trust architecture.

3.4.1 Encrypt data

The "Encrypt Data" phase implements cryptographic protection for sensitive information in laaS environments, ensuring confidentiality through algorithms like AES-256. The core transformation is represented by:

$$C = E_k(P) \quad (3)$$

where C is ciphertext, P is plaintext, and E_k denotes AES-256 encryption with key k. This process secures both data at rest (in storage services) and in transit (via TLS 1.3), while integrated key management systems enforce strict access controls and automatic key rotation. The equation embodies the fundamental security operation that renders data unreadable to unauthorized entities, even if perimeter defense are compromised, operationalizing Zero Trust's core tenet of persistent verification. Additional controls like data classification and tokenization complement this encryption foundation for comprehensive protection.

3.5 AUTOMATE & ENFORCE POLICIES

The Automate & Enforce Policies phase leverages Infrastructure as Code (IaC) and policy-as-code tools to systematically implement and maintain Zero Trust security controls across the IaaS environment. This involves scanning IaC templates (Terraform, CloudFormation) for compliance violations using tools like Checkov or Open Policy Agent, and automatically remediating misconfigurations such as overly permissive IAM roles or unencrypted storage buckets. Zero Trust Network Access (ZTNA) solutions replace traditional VPNs with context-aware, identity-based access policies that are dynamically enforced. Policy engines continuously validate configurations against predefined rules (e.g., CIS benchmarks), while CI/CD pipelines integrate security checks to prevent drift. The automation ensures consistent enforcement of least-privilege principles at scale, with the alerts and self-healing mechanisms that maintain security posture without manual intervention, effectively operationalizing Zero Trust in dynamic cloud environments.

3.5.1 IaC security scans

The laC Security Scans process automatically analyses Infrastructure as Code (laC) templates (e.g., Terraform, AWS CloudFormation) to detect misconfigurations and enforce security best practices before deployment. Using tools like Chekov, Terrascan, or Open Policy Agent, these scans validate configurations against predefined policies (e.g., CIS benchmarks, Zero Trust principles) to flag risks such as exposed storage buckets, excessive IAM permissions, or missing encryption. The process can be formalized with the equation:

$$\text{Scan Result} = \sum_{i=1}^{n} [\text{Violation}_i \times \text{Severity}_i] \quad (4)$$

where Violation_i represents a detected policy violation (1 if present, 0 otherwise), and Severity_i is its risk weight. This quantifies the total risk score, enabling prioritization of fixes. Integrated into Cl/CD pipelines, laC scans prevent insecure deployments by blocking non-compliant resources, ensuring alignment with Zero Trust's proactive security model.

4. RESULT AND DISCUSSION

Figure 2: illustrates the Latency Comparison Before and After Zero Trust Implementation. It shows latency in milliseconds during 10 operational instances in an IaaS environment. Before implementing Zero Trust (represented by the blue line), latency starts at 50 ms and fluctuates between 50 and 64 ms, with a gradual increase over time. After Zero Trust (represented by the red line), latency starts higher at 65 ms and increases more significantly, reaching up to 80 ms by the 10th operation. The higher latency after Zero Trust implementation is likely due to the additional security layers, including continuous identity verification, access control policies, and encryption, which introduce some overhead compared to the pre-Zero Trust environment with fewer security measures.

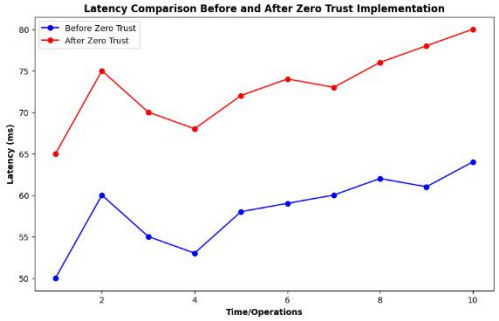

Figure 2: Latency Comparison of Zero Trust Implementation

The diagram shows a comparison of Incident Response Time Before and After Zero Trust Implementation**.** It plots the incident response time in minutes over 10 operational instances. Before Zero Trust (green line), the response times vary between 30 and 40 minutes, with fluctuations indicating slower responses, likely due to manual intervention and slower processes. After Zero Trust (orange line), incident response times are reduced, ranging from 15 to 25 minutes, showing a clear improvement likely due to the automation, proactive security measures, and continuous monitoring inherent in the Zero Trust approach. This demonstrates the effectiveness of Zero Trust in enhancing the speed of incident response.

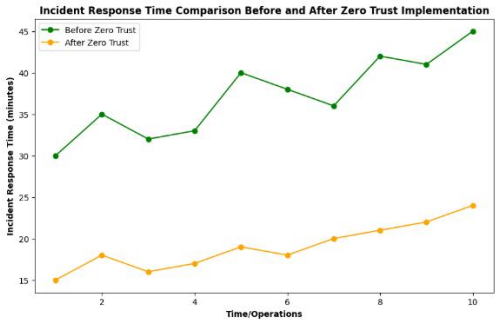

Figure 3: Incident Response Time Before and After Zero Trust Implementation

5. CONCLUSION

This paper presents effective security models for Infrastructure as a Service (IaaS) environments, with a particular focus on enhancing trust and security through frameworks like Cloud-Trust and Trusted-Cloud. These models introduce comprehensive trust evaluation criteria, such as provider reputation and service availability, which are vital for improving decision-making when selecting cloud providers. The adoption of Zero Trust principles, including least-privilege access and continuous verification, significantly strengthens the overall security posture of IaaS environments. However, the implementation of Zero Trust does introduce a slight increase in latency, with values rising from 50 ms to 80 ms. Despite this increase, Zero Trust notably enhances incident response times, reducing them from 30-40 minutes to 15-25 minutes, which highlights the efficiency of automated security policies, the monitoring, and proactive threat management. Additionally, integrating security measures like encryption, identity and access management (IAM) controls, and micro-segmentation not only mitigates vulnerabilities but also builds stronger trust between users and cloud providers. This study underscores the need for continuous security evaluation and automated remediation to ensure that cloud environments remain resilient to evolving cyber threats. The findings suggest that Zero Trust, although adding some overhead, results in better overall security management, faster incident handling, and a more reliable cloud infrastructure, fostering greater confidence in IaaS services.

REFERENCE

[1] Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2015). Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. IEEE Transactions on Cloud Computing, 5(3), 523-536.

[2] Alabool, H. M., & Mahmood, A. K. B. (2016). A novel evaluation framework for improving trust level of Infrastructure as a Service. Cluster Computing, 19, 389-410.

[3] Sethi, C., & Pradhan, S. K. (2016). Trusted-Cloud: A Cloud Security Model for Infrastructure as a Service (IaaS). International Journal of Advanced Research in Computer Science and Software Engineering, 6(3).

[4] Banirostam, H., Hedayati, A., Zadeh, A. K., & Shamsinezhad, E. (2013, April). A trust based approach for increasing security in cloud computing infrastructure. In 2013 UKSim 15th International Conference on Computer Modelling and Simulation (pp. 717-721). IEEE.

[5] Dawoud, W., Takouna, I., & Meinel, C. (2010, March). Infrastructure as a service security: Challenges and solutions. In 2010 the 7th International Conference on Informatics and Systems (INFOS) (pp. 1-8). IEEE.

[6] Al-Amri, S. M. (2017). IaaS-cloud security enhancement: an intelligent attribute-based access control model and implementation (Doctoral dissertation, Loughborough University).
[7] Alabool, H. M., & Mahmood, A. K. (2014, June). Common trust criteria for IaaS cloud evaluation and selection. In 2014 International Conference on Computer and Information Sciences (ICCOINS) (pp. 1-6). IEEE.
[8] Seth, J. K., & Chandra, S. (2013). A novel design to increase trust in cloud IaaS model. International Journal of Computer Science Issues (IJCSI), 10(4), 329.
[9] Yeluri, R., & Castro-Leon, E. (2014). Building the Infrastructure for Cloud Security: A Solutions View (p. 244). Springer Nature.
[10] Kashif, U. A., Memon, Z. A., Balouch, A. R., & Chandio, J. A. (2015, January). Distributed trust protocol for IaaS cloud computing. In 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST) (pp. 275-279). IEEE.
[11] Iqbal, S., Kiah, M. L. M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., & Choo, K. K. R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. Journal of Network and Computer Applications, 74, 98-120.
[12] Karadsheh, L. (2012). Applying security policies and service level agreement to IaaS service model to enhance security and transition. computers & security, 31(3), 315-326.
[13] Manuel, P. D., Abd-El Barr, M. I., & Thamarai Selvi, S. (2011). A novel trust management system for cloud computing IaaS providers. JCMCC-Journal of Combinatorial Mathematicsand Combinatorial Computing, 79(3).
[14] Huang, W., Ganjali, A., Kim, B. H., Oh, S., & Lie, D. (2015). The state of public infrastructure-as-a-service cloud security. ACM Computing Surveys (CSUR), 47(4), 1-31.
[15] Dykstra, J., & Sherman, A. T. (2013). Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. Digital Investigation, 10, S87-S95.
[16] Sachdev, A., & Bhansali, M. (2013). Enhancing cloud computing security using AES algorithm. International Journal of Computer Applications, 67(9).
[17] Madni, S. H. H., Abd Latiff, M. S., Coulibaly, Y., & Abdulhamid, S. I. M. (2016). Resource scheduling for infrastructure as a service (IaaS) in cloud computing: Challenges and opportunities. Journal of Network and Computer Applications, 68, 173-200.
[18] Alabool, H. M., & Mahmood, A. K. (2015, May). A novel evaluation model for improving trust level of infrastructure as a service. In 2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC) (pp. 162-167). IEEE.
[19] Sathiya, Aravindhan K., and D. Sathiya. "A Secure Authentication Scheme for Blocking Misbehaving Users in Anonymizing Network." International Journal of Computer Science and Technology 4, no. 1 (2013): 302-304.
[20] Stankov, I., Datsenka, R., & Kurbel, K. (2012). Service level agreement as an instrument to enhance trust in cloud computing–an analysis of infrastructure-as-a-service providers.