International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Real-Time Zero-Trust Monitoring for Cloud Security and Integrity in Trusted Public Clouds

G Vijay[1], K Bhaskar[2]

[1]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: gurramvijay2002@gmail.com, ORC-ID: https://orcid.org/0009-0003-5236-4527

[2]Assistant Professor, Department of CSE(AI & ML),, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: bhaskark.mca@gmail.com , ORC-ID: https://orcid.org/0009-0000-3309-4240

Abstract: Due to its scalability, cost efficiency, and high quality storage and computational abilities, cloud computing is increasingly being adopted in critical spheres such as healthcare, finance, and social media. Outsourcing of data and processing to third-party cloud architectures expose data integrity and privacy risks including data alteration and unauthorized access by both external and internal users. To help prevent these threats, a Zero-Trust runtime architecture is adopted to provide continuous monitoring and validation of the status of the client machine. TPC system ensures integrity by integrating a monitoring module at the kernel level, a trust agent, a Software Trusted Platform Module (SWTPM), and a verification cluster. It validates the client-side changes by using cryptographic hash and real-time verification systems to detect the anomalies and unauthorized changes. The system supports dynamic verification rules by using an Include and Exclude strategy to increase the efficiency of the computation. An activity monitoring addon is added to log-based, which monitors the patterns of the activity so that it can prevent the entry of unauthorized users. The framework is deployed to local environment to simulate the actions of cloud and tested with simulated virtual machines which is efficient in monitoring of state of machine and real time notification of security breach.

"Index Terms: *Zero-Trust, Cloud Security, Machine State Monitoring, TPM, Hash Verification, Intrusion Detection, User Activity Logging, Data Integrity".*

1. INTRODUCTION

Cloud computing has become an important part of modern digital environment, which offers scalable and on-demand access to computing resources without a major investment in initial capital. Its optimization capabilities and reduction of infrastructure costs has led to extensive implementation in many industries, such as health, financial services, education, and government services [1][2]. Companies are increasingly relying on third-party cloud vendors such as AWS, Microsoft Azure and Google Cloud Platform, which operate large networks of geographically distributed data centers to deliver on-demand and high-performance services. Such companies manage data storage, processing, and application deployment enabling clients to focus on key business goals rather than maintenance of infrastructure.

Despite these advantages, remote cloud infrastructure transition poses serious concerns pertaining to data privacy, trust and data security. Because user data is often stored and processed by third parties, users lose their direct control over their assets, which becomes problematic in terms of unlawful access to it, manipulation and the prolonged existence of unnoticed security breaches [4]. Some of the cloud threat vectors include external malware injections as well as rogue insiders who have increased access controls. The malefactors may capitalize on vulnerabilities in the virtual environments, shared resources, or misconfigured access control privileges to violate sensitive data [5].

Traditional perimeter based security frameworks assume that every component in the network is trustworthy. This approach has become inadequate in the modern scenario where threats can be posed by both internal and external networks perimeter [6]. The perimeter defenses often do not detect developed attacks that bypass firewalls or are a result of compromised internal accounts. As a result, a number of security breaches go unnoticed over extended periods, which leads to losses of finances and legal consequences, as well as damaged reputation [7].

Considering these limitations, the Zero-Trust security paradigm has emerged as an active approach assuming

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

the lack of the trust in any user or system element, whether internal or external. It involves continuous authentication of user identity, device status and system integrity before a resource can be accessed [8]. Although the concept of Zero-Trust is widely applied in network and access control, many have overlooked monitoring clients and runtime verification, which leaves systems vulnerable to internal attacks or administrative breaches. As a result, it is high time to have better Zero-Trust architectures that offer protection on an endpoint level and incorporate real-time verification of client system states.

2. LITERATURE REVIEW

In their presentation at the 30th USENIX Security Symposium, R. Khandelwal, T. Linden, H. Harkous, and K. Fawaz [9] have presented PriSec, which is a controller that implements privacy settings. This strategy addresses the problem of limited control of privacy settings and permissions of users of cloud applications. PriSec has been designed so that it provides a user-friendly approach to privacy, where the user can define, apply, and manage their privacy policies on different platforms. The framework ensures that the preferences of the users are respected during the operation of the systems, and sensitive data is also not abused. The authors emphasize that the decentralization of control may lead to the improvement of privacy guarantees in large cloud systems.

C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi [10] explored the security, privacy, and efficiency issues related to the sustainable cloud computing, particularly in the context of integrating the Big Data and IoT. Their study highlights the growing concern about handling large amounts of data in cloud systems, where sustainability and security are the key factors. They claim that traditional data security systems cannot support very dynamic IoT-based infrastructures. The authors support energy-efficient cryptography algorithms and architecture changes to enhance the overall system security and performance. Their works play a critical role in identifying the intersection of performance optimization and data confidentiality in the cloud environments.

The problem of the hardware versus software security of cloud systems was examined by L. Zhao and D. Lie [11], the question was as follows: Is hardware safer than software? They have been analyzed in IEEE Security and Privacy and define the strengths and weaknesses inherent in both approaches. They argue that even though hardware-based security mechanisms (including TPMs and SGX) offer stronger isolation and smaller attack surfaces, they are still susceptible to side-channel attacks and hardware-level threats. On the other hand, software based systems are more flexible and easier to patch but they lack strong physical protection. This paper is essential to the understanding of trade-offs during the design of Zero-Trust systems, which rely on hardware and software verification parts.

A comprehensive study of software-based remote attestation was conducted by S. F. J. J. Ankergard, E. Dushku, and N. Dragoni [12] and specifically in relation to IoT devices. They map the current limitations in the process of remote attestation in their article in Sensors and highlight the unsolved issues such as scalability, reliability, and resistance to tampering in large IoT deployments. The authors present a systematic review of innovative methods and emphasize the need to design lightweight and secure remote attestation models that could be implemented in Zero-Trust systems. Their concepts make significant contributions to the understanding of how to optimise the current state monitoring of a real-time system when it is used in a modern scaled dispersed setting, such as a cloud platform.

ZTA-IoT is a new Zero-Trust Architecture suggested by S. Ameer, L. Praharaj, R. Sandhu, S. Bhatt and M. Gupta [13] and is created to operate in IoT environments. Their article in ACM Transactions on Privacy and Security proposes a model of comprehensive use control that was designed to enhance access control mechanisms beyond the conventional methods. They have a persistent policy enforcement approach that does not only authenticate individuals and devices at the access point but also during their interaction lifecycle. This is a dynamic and adaptive access control which prevents the threats of the devices or individuals who have been compromised and become malicious after authentication. Their architecture is particularly important to deploy the ideas of Zero-Trust to the IoT and other edge devices connected to cloud systems.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Y. Liu et al. [14] developed a model of cross-domain data sharing in Zero-Trust cloud-edge-end systems through a blockchain framework based on sharding. They are reported to have conducted a study, which was published in IEEE Transactions on Dependable and Secure Computing that centers on the transmission of secure data in a decentralized environment whereby multiple trust domains coexist. They point out how traditional centralized data sharing systems are prone to single-point failures and data loss. Sharding in blockchain enables scalability and fault tolerance and also upholds Zero-Trust principles of authentication, confidentiality, and integrity. This study is critical in ensuring safe communication between cloud, edge and endpoint devices in distributed real-time applications.

B. Ali, M. A. Gregory, S. Li, and O. A. Dib [15] presented a two-dimensional fuzzy approach to the implementation of Zero-Trust-based security in MEC systems. They use fuzzy logic in their work published in Computer Networks to make trust-based authentication and job offloading decisions. This combined approach allows systems to dynamically react to the changing levels of trust between users and devices, thus reducing the vulnerability of rigid, binary access decisions. The authors show that adaptive processes increase the accuracy of choices in uncertain situations, which comply with the concept of Zero-Trust according to which the assessment of trust should be conducted on an ongoing basis.

Q. Shen and Y. Shen [16] presented a collaborative endpoint security paradigm, which improves Zero-Trust systems by combining identity checks and continuous behavior monitoring. Their work in Computers and Security defines the way the endpoint devices, which are often the most susceptible element of enterprise networks, can be hardened by exchanging collaborative intelligence. Their methodology collects contextual information from user behavior, device activity, and access history to perpetually revise access rights. This strengthening of endpoint security complies with the general principle of Zero-Trust which states that no element, including the presence of the perimeter, can be trusted. In their study, they emphasize the importance of client-side security validation that is overlooked in the classic Zero-Trust design.

3. MATERIALS AND METHODS

The given system suggests a Zero-Trust runtime framework [18] that can serve to ensure that the state of the client machines in the cloud is verified continuously. It aims at detecting the illegal changes and potential security breaches by checking file-level updates by verifying cryptographic hash values. It consists of four basic parts: a Kernel Module, which tracks file activity and generates hashes, a Trust Agent which manages hash queues and communicates with verification services [17], a Trusted Platform Module (TPM) or a software implementation of secure cryptographic operations, and a Verification Cluster, which performs verification of machine integrity by use of include/exclude verification policies. The process of capturing user activity has been developed to track suspicious logins and detect brute force attacks. An administrator can study this log to prohibit rogue users and avert additional harm. The system is set to run on a local cloud server architecture which will be simulating a real cloud infrastructure so that effective emulation, monitoring and application of Zero-Trust principles is done.

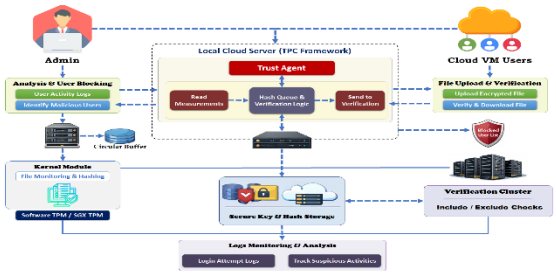


Fig.1 Proposed Architecture

The System Architecture (fig.1) depicts secure cloud set up where the Administrator monitors the user activities, and Cloud VM User uploads, verifies, and downloads files. A verification graph represents the process. Everything is documented in the blockchain which ensures transparency, data integrity and secure management of files in the cloud.

a) Modules:

1) Admin Module

Admin Login: This module allows the administrator to obtain the system with pre-defined credentials without risks of being detected. Once the user is successfully authenticated, they gain access to the record of user activities, monitoring tools in the system and the ability to control the behavior of cloud users.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

It is the channel through which the administrative oversight and decision-making in the entire structure is made [19, 20].

View & Block VM User Activities: This module enables the administrator to get the detailed logs of user actions, including the information about the attempts at logins and the manipulations with files. It can help to determine suspicious activity like the frequent unsuccessful logins or the lack of authorization tendencies. The administrator can then limit access of some of the users to the system to prevent further malicious practices.

Logout (Admin): The log out module ensures the safe termination of the administration session. It helps to prevent unauthorized access by ending the active session and sending the user to the homepage or the interface of the login. This maintains integrity of the sessions and prevents the abuse or exposure of important administrative functions.

2) User Module

User Login: The module allows registered users to be able to access their virtual cloud environment via entry of valid login credentials. It authenticates the user and allows access to the features like file upload, verification and download. The failure to log in is logged in to be assessed by the administration, therefore, increasing the security of the system and accountability of the user.

Upload File: This module will enable users to post files on the cloud server. Before uploading, the file is encrypted and hashed, and the user selects a verification type: the user can either include it or exclude it. This ensures the integrity of files uploaded and makes it easier to perform a later verification in order to detect the illegal changes and manipulations.

Verify & Download File: The module ensures the integrity of the uploaded file by comparing the current value of the hash to the previous hash values. When the hashes match, then the file will not be changed; otherwise, a user will be informed that the file has been altered. After authentication, the user is able to decrypt and access his original file on the cloud with a lot of protection.

Verification Graph: Verification graph module presents the trusted and untrusted machine activity graphically based on the verification time. The graph shows that trusted systems tend to be verified faster whereas hacked or altered computers take more time and therefore help users to detect the integrity of cloud systems and identify anomalies in a timely manner.

Logout: This module safely closes the user session, and the access is shut off to the system to prevent malicious activity. It ensures that the user cannot perform sensitive operations, including file operations or user monitoring, after logging out of the system and thus maintain the overall system confidentiality and session integrity.

b) Methods/Technologies:

1. File Hashing (Integrity Check): Hashing of files is also used to ensure the integrity of data by computing a different hash value with each file during the upload process. The file is rehashed during verification and the resultant hash is compared to the original. When the hashes are equal, then the file is not changed. This helps in detection of any malicious changes or intrusions in the cloud environment.

2. File Encryption (Confidentiality): File encryption is used to protect sensitive data by converting data to inreadable ciphertext using a cryptographic key before uploading to the cloud. Only the authorized persons who have the decryption key are allowed access to the original data. This will ensure that in case an attacker gains access to the cloud server, he/she will not be able to read and use the content of the files.

3. Verification Types (Include/Exclude): In order to improve the performance, the user assigns a verification type to each file: Include or Exclude. Include files are thoroughly integrity tested but exclude files are not. It is a type of selective verification technique, which minimizes unnecessary computing, especially in non sensitive files which are frequently modified files and hence the performance is not affected as well as the overall system security is not compromised.

4. Kernel-Level Monitoring: A kernel module is an operating system level operation that monitors file operations on a real-time basis. It determines the time files are accessed, modified, or opened and generates hash values on the files. The measurements are stored in a secure buffer to be later verified to enable one to identify state changes in the system in a timely and accurate manner.

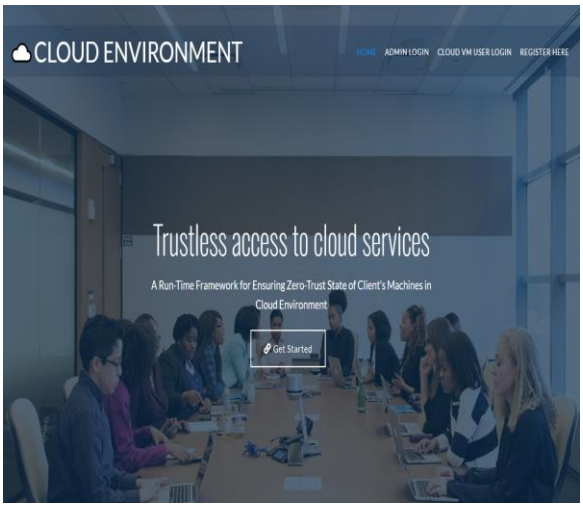
5. TPM Integration (Trusted Platform Module): Trusted Platform Module (TPM) is a secure

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

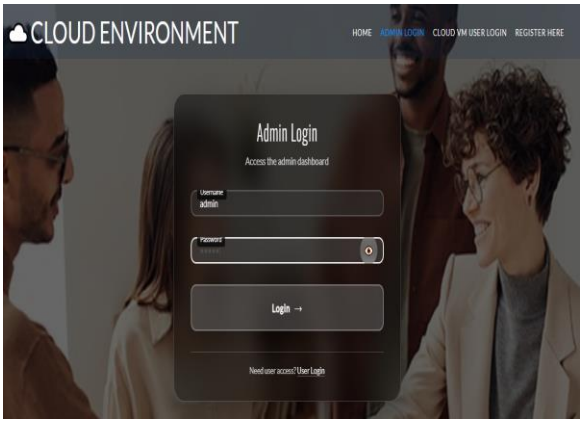
cryptographic processor, which may be a hardware or software-based, that is used to store and manipulate security keys and integrity measurements. It will ensure that only legitimate systems can perform necessary tasks. TPM or SGX-enabled TPM integration enhances reliability of the system and prevents illegal executing of codes or manipulation of data on the client devices.

6. Activity Logging and User Behavior Monitoring: A log is used to record every user activity such as logins, file uploads and failed attempts to access files. These logs are monitored by the administrator who can determine suspicious behavior like repeated failed logins or unusual use of the system. User blocking is one of the preventive measures that the administrator can use to maintain the security of the systems and prevent unauthorized access or attacks.

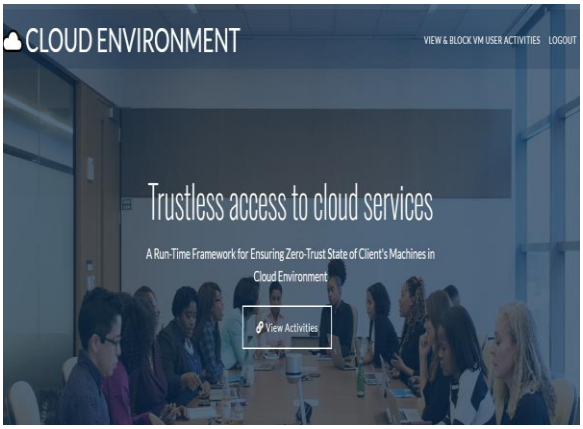
4. EXPERIMENTAL RESULTS



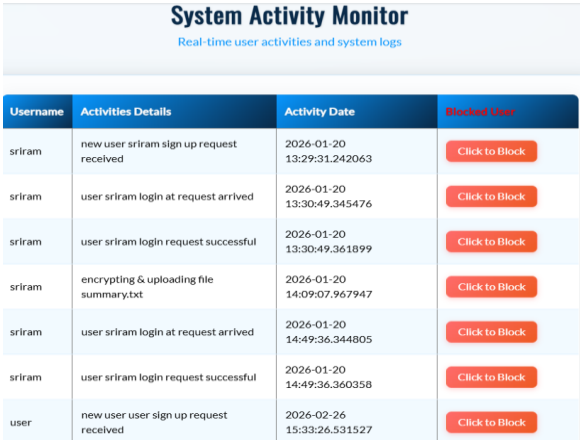
As a result, the project interface will be presented as shown in the above screen.



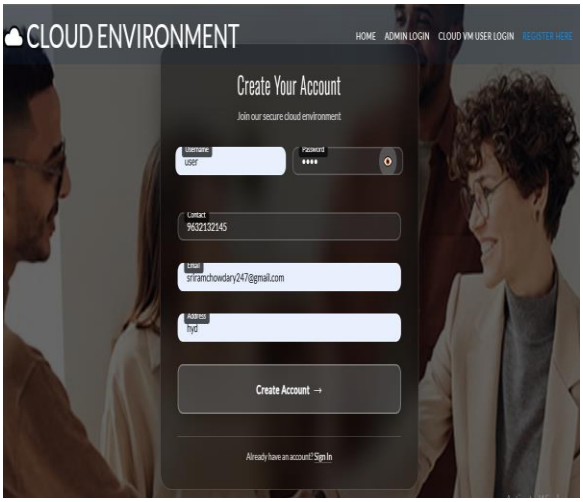
The administrator identifies himself with valid login and password credentials to gain account access.



After a successful login, the administrator homepage will be displayed.

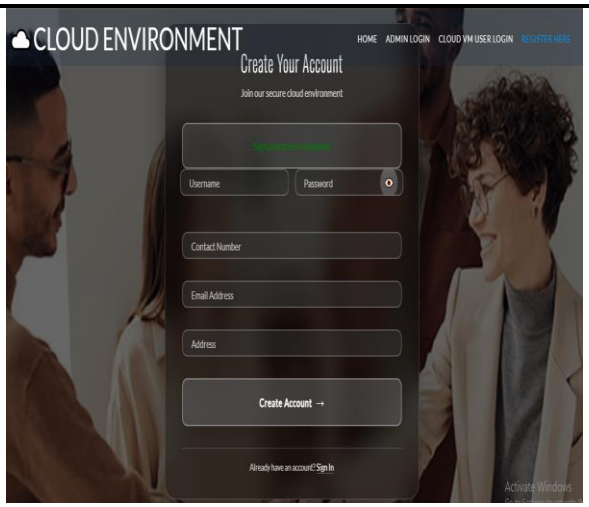


Enter all the required fields required to register the user and select the user type as shown below.

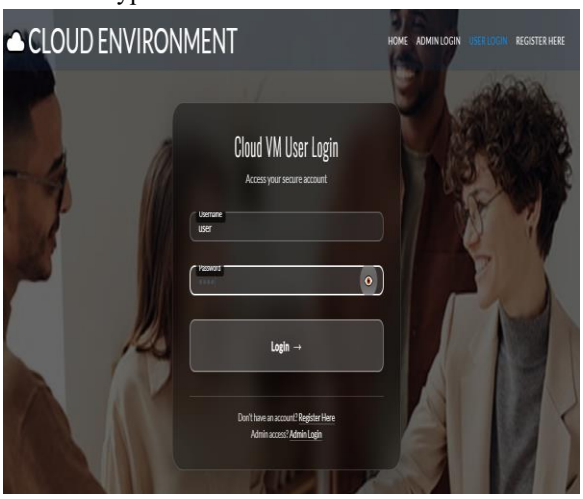


Provide relevant authentication details to get into the administration account.

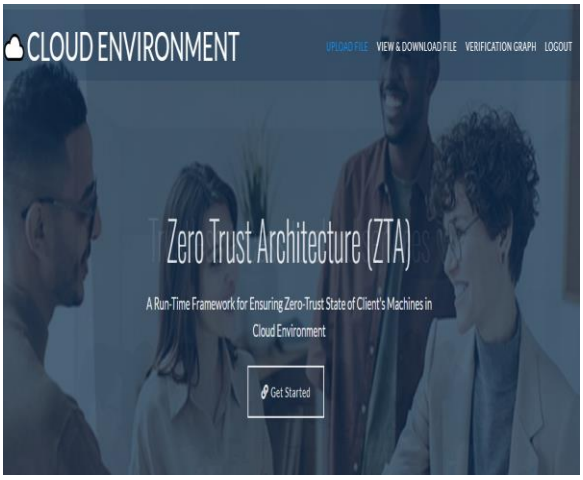
International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper



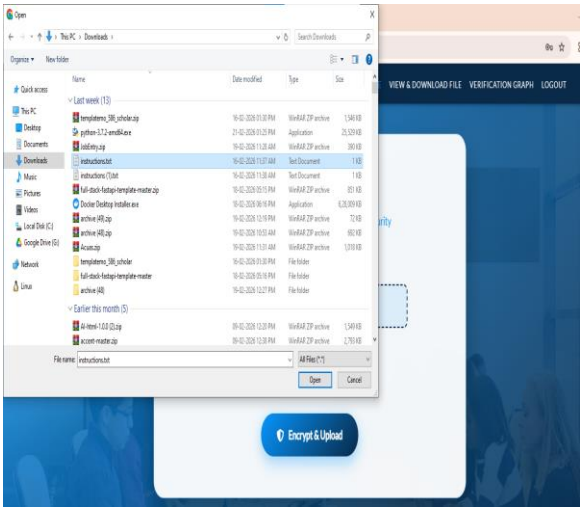
Fill in all the required fields of user registration and select the type of user as shown below.



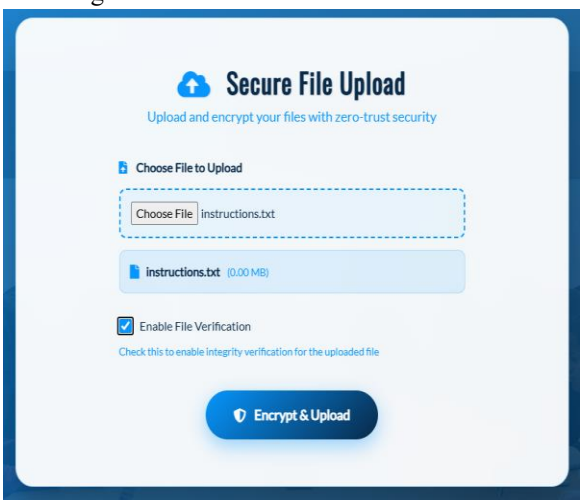
Enter in the appropriate authentication credentials to be able to access the administrative account.



Enter all the required fields to create an account and choose the type of user as shown below.

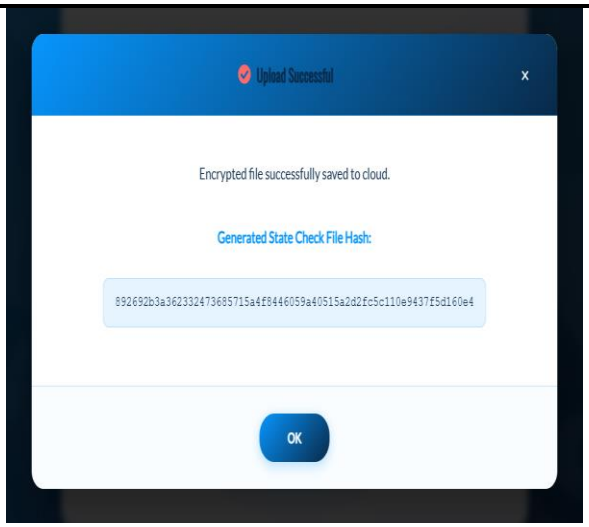


After registering, fill in and enter the valid credentials to the login screen.



Select a file at the local storage, upload it into the cloud, and encrypt it with the help of a zero-trust security system.

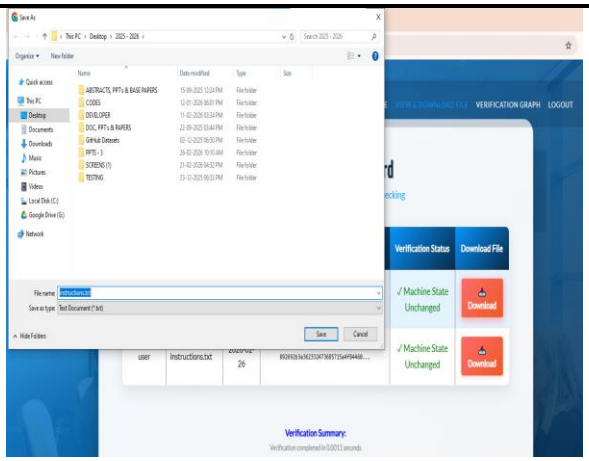
International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper



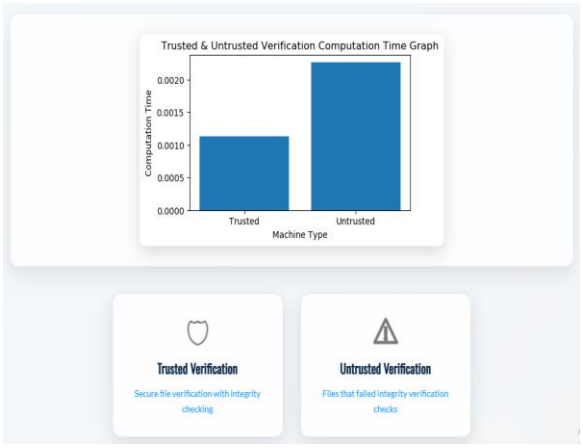
The file view and verification process such as integrity check and verification summary is given below.



The dashboard of the verification analysis of the uploaded file in the cloud is provided in the form of a graph.



Enter valid authentication details to enter the administrative account.



The system activity monitor logs the uploaded information in cloud storage and provides the user-blocking option.

5. CONCLUSION

The current study successfully uses a Zero-Trust security architecture that checks and validates the working condition of client machines in cloud environment. The system ensures continuous file integrity and early detection of undesirable changes by using a combination of kernel-level monitoring, cryptographic hash generation and trusted platform modules. The verification cluster properly identifies modified files by comparing the current hash values of the files to the previous values and to the verification criteria that the user sets, thus preventing the undetected modifications or data leakage.

An additional level of security is achieved through activity logging, where the activities of all users in the system are recorded. This will allow managers to

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

analyze the behavior of logging in, identify suspicious trends such as multiple failed attempt to log in, and limit access by users who may pose a threat, thereby enhancing the accountability of users and preventing threats within the organization.

It is fully simulated on a locally simulated cloud server, which replicates real-life scenarios. This approach shows that the Zero-Trust architecture is viable in real-time detection, safe file outsourcing, and user behavior surveillance, which can be a formidable defense against external and internal threats in the cloud.

REFERENCES

[1] Rosén, A. (2025). Achieving Zero Trust: A Strategic Roadmap for Phased Implementation of Zero Trust Architecture.

[2] Scientific, L. L. (2025). SECURE AND RESILIENT VIDEO BLOCK MANAGEMENT AND PRINCIPLES FOR ZERO TRUST CLOUD NETWORK. Journal of Theoretical and Applied Information Technology, 103(7).

[3] Jena, B., Mishra, D., Mishra, S., & Mishra, S. (2025). Zero Trust Architecture-Based Enhanced Security Framework for OTT in Hybrid Cloud Environment. In Ethical Impacts of Using AI for Sustainable Development (pp. 89-112). IGI Global Scientific Publishing.

[4] Avirneni, S. T. (2025). Intent-Aware Authorization for Zero Trust CI/CD. arXiv preprint arXiv:2504.14777.

[5] Asaithambi, S., Nallusamy, S., Yang, J., Prajapat, S., Kumar, G., & Rathore, P. S. (2025). A secure and trustworthy blockchain-assisted edge computing architecture for industrial internet of things. Scientific Reports, 15(1), 15410.

[6] D. N. Jha, G. Lenton, J. Asker, D. Blundell, and D. Wallom, "Trusted platform module based privacy in public cloud: Challenges and future perspective," IEEE IT Professional, pp. 1–5, 2022.

[7] M. Ma, Z. Yin, S. Zhang, S. Wang, C. Zheng, X. Jiang, H. Hu, C. Luo, Y. Li, N. Qiu et al., "Diagnosing root causes of intermittent slow queries in cloud databases," Proceedings of the VLDB Endowment, vol. 13, no. 8, pp. 1176–1189, 2020.

[8] H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," The journal of supercomputing, vol. 76, no. 12, pp. 9493–9532, 2020.

[9] R. Khandelwal, T. Linden, H. Harkous, and K. Fawaz, "Prisec: A privacy settings enforcement controller," in 30th {USENIX} Security Symposium ({USENIX} Security 21), 2021.

[10] Viswanath, G., Abirami, V., & Prathyusha, G. (2024). Hybrid Feature Extraction With Machine Learning To Identify Network Attacks. International Journal Of Hrm And Organizational Behavior, 12(3), 217-228.

[11] L. Zhao and D. Lie, "Is hardware more secure than software?" IEEE Security & Privacy, vol. 18, no. 5, pp. 8–17, 2020.

[12] S. F. J. J. Ankergard, E. Dushku, and N. Dragoni, "State-of-the-art ˚ software-based remote attestation: Opportunities and open issues for internet of things," Sensors, vol. 21, no. 5, p. 1598, 2021.

[13] S. Ameer, L. Praharaj, R. Sandhu, S. Bhatt, and M. Gupta, "Zta-iot: A novel architecture for zero-trust in iot systems and an ensuing usage control model," ACM Transactions on Privacy and Security, 2024.

[14] Kalae, U. K. (2021). Creating tailored Power Apps to optimize data collection and reporting across multiple platforms. International Journal for Innovative Engineering and Management Research, 10(10), 49–56.

[15] Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.*

[16] Banda Saikumar. (2025). Integrating azure network rules for storage account through terraform in CI/CD pipelines: automating storage account access restrictions to public IP. Journal of Scien+B112ce & Technology, 10(2), 15–22. https://doi.org/10.46243/jst.2025.v10.i02.pp15-22.

[17] M, Chaithanya., Viswanath, G., Dunna, Nikitha Rao,, G, Prathyusha. (2023). A Real Time Online Food Ording Application Based Django Restfull Framework Juni Khyat journal, 13(9), 154-162.

[18] B. Shen, H. Yu, P. Hu, H. Cai, J. Guo, B. Xu, and L. Jiang, "A cloudedge collaboration framework for generating process digital twin," IEEE Transactions on Cloud Computing, 2024.

[19] R. Xin, P. Chen, P. Grosso, and Z. Zhao, "A fine-grained robust performance diagnosis framework for

run-time cloud applications," Future Generation Computer Systems, 2024.

[20] Kumar, K., Udaya Suriya Rajkumar, D., Viswanath, G., & Mahalakshmi, J. (2024). A Hybrid Particle Swarm Optimization and C4.5 for Network Intrusion Detection and Prevention System. International Journal of Computing, 23(1), 109-115. https://doi.org/10.47839/ijc.23.1.3442