International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 21, Issue 4 (April 2025), PP 151-153

An AI-Powered Decentralized Operating System: Architecture and Security

[1]HarshPandey&[2*]YashSrivastav
[1]Bansal Institute of Engineering and Technology, Lucknow,Uttar Pradesh, India.
[2]Shri Venkateshwara University, Gajraula, Uttar Pradesh, India.
Corresponding Author: YashSrivastav
Shri Venkateshwara University, Gajraula, Uttar Pradesh, India.

Abstract
ThispaperintroducesanewdecentralizedOSthatusesAItosecure,manageresources, and be autonomous.With federated learning, reinforcement learning, and blockchain- based security protocols, it proactively detects and mitigatesthreats, allocates resources efficiently,andhasnocentralpointsofcontrol. KeyfeaturesincludeAI-optimizeddynamic resource allocation, asynchronous parallel processing with microservices-based execution, intelligentnetworkoptimizationwithdecentralizedloadbalancing,andadecentralizedAI securityorchestrationframework. Zero-knowledgedecentralizedidentityfortrustlessauthentication and blockchain-based decentralized governance with self-healing protocols. Applicationsincludecriticalinfrastructure,healthcaresystems,smartgrids,IoTnetworks, financialservices, autonomousvehicles, andedgecomputingenvironments.Bycombining AI-driven security, decentralized consensus, and efficient resource management, this OS provides a secure, efficient, and autonomous digital infrastructure for high security, privacy, and performance.

Keywords: *DecentralizedOS,AI security, federated learning, blockchain, microservices, edge computing, zero-knowledge authentication*

Date of Submission: 05-04-2025 Date of acceptance: 15-04-2025

I. Introduction

Makingitfullyadaptabletothechangingtimesof2023,thisversionbringsaboutpresent-day transformationsalignedwithtrendsinthemoderndigitalworld—newoperatingsystemarchitecturesandcyberthreatcountermeasures.Increasinglysophisticatedcyberthreats,alongside incessantly eroding user privacy and inefficiencies of traditional, monolithic OS frameworks, demand transformation in OS architecture and security [1].

Conventionaloperatingsystemsaregenerallycentralized,limitinganonymity,datasovereignty, and system resilience.Their reactive security mechanisms are ill-equipped to preempt zero-day vulnerabilities, advanced malware, and state-sponsored cyber intrusions [2].

ThispaperdescribestheconceptionanddevelopmentofaLinux-basedfullydistributedand decentralizedoperatingsystemthatovercomestraditionalarchitecturelimitationsandadoptsa proactiveparadigmforcybersecurity.TheproposedOSincludesanadvancedAI-drivensecuritymodelthatautonomouslydetects,analyzes,andneutralizescyberthreatsinrealtime. This self-adaptive,self-healingsystemisimmunetoviruses,malware,andunauthorizedintrusions. Unlike centralized OS models, this system avoids storing user data, eliminating attack vectors related to data breaches and surveillance.Its decentralized architecture intrinsically enhancessecuritybydistributingcomputationalresourcesandsecurityintelligenceacrossatrustless,autonomousnetwork.Cryptographicallysecure,consensus-drivenresourcemanagement ensuresresilienceagainstsingle-pointfailures[3].

TheOSfeaturesultra-efficientresourceallocation,high-speedcomputationalperformance, andoptimizedworkloaddistribution.Itsupportsscalability, deterministicbehavior, andmax- imum throughput—ideal for future computing environments, high-security enterprises, and mission-critical applications.

II. System Architecture

The OS is built on a microservices-based architecture allowing dynamic modular functionality.Eachcomponentoperatesindependentlyyetcollaboratesthroughintelligentorchestration layers.Distributed nodes host modular OS components using containerization to achieve fast deployments, failure isolation, and seamless upgrades [4].

TheOSkernelislightweightanddesignedtobedistributed. CoreOSserviceslikeschedul- ing, memory management, and I/O are abstracted as microservices.Reinforcement learning optimizes resource scheduling, ensuring efficiency and fairness across all nodes.

Parallelism is achieved through asynchronous execution and event-driven programming. Nodescommunicateviasecure,lightweightmessagingprotocols. AIagentsembeddedineach node manage tasks such as performance monitoring, load balancing, and threat detection.

III. Security Framework

Security is the cornerstone of the proposed OS. It incorporates multi-layered defense mecha- nisms:

- **AI-BasedThreatDetection:** TheOScontinuouslymonitorssystembehaviorusingma- chine learning models to detect anomalies and malicious activities.
- **Federated Learning:**Distributed nodes train local models and contribute to a global model without sharing raw data, enhancing both accuracy and privacy.
- **Zero-KnowledgeProofs:** Authenticationmechanismsrelyonzero-knowledgecryptog- raphy to validate identity without revealing credentials [5].
- **BlockchainGovernance:**Adecentralizedledgerrecordstransactions,updates,andpoli- cies. Consensus mechanisms ensure integrity and transparency [6].
- **Self-Healing Protocols:** Upon detecting anomalies, the system initiates corrective ac- tions such as isolating nodes, rebooting services, or patching vulnerabilities.

The security orchestration framework coordinates responses between AI agents, minimiz- ing human intervention and response time.

Use Cases and Applications

TheOShasbroadapplicabilityacrosssectors:

- **CriticalInfrastructure:** Enablessecure,autonomouscontrolofutilitiesandenergysys- tems.
- **Healthcare:**Protectssensitivemedicaldataandensurescompliancewithregulatory standards.
- **FinancialServices:** Safeguardstransactionintegrityandpreventsfraud.
- **Autonomous Vehicles:**Provides reliable,real-time decision-making in edge environ- ments.
- **Smart Grids and IoT:** Manages distributed sensors and actuators with secure commu- nication.

IV. Conclusion

Thispaperpresentedanext-generationdecentralizedoperatingsystemthatleveragesAI,blockchain, and distributed computing to provide an autonomous, secure, and high-performance environ-ment.By moving beyond centralized limitations, the system embodies resilience, scalability, andprivacy,addressingmodernchallengesincomputinginfrastructure.Itsinnovativearchitec- ture holds promise for shaping future digital ecosystems across various industries.

Appendix

- **AI Models Used:**Reinforcement Learning (RL), Federated Averaging (FedAvg), and Unsupervised Anomaly Detection.
- **Microservice Tools:**Docker,Kubernetes, andgRPC-based communication.
- **BlockchainFramework:**HyperledgerFabric,EthereumSmartContracts.
- **SimulationEnvironment:**GNS3fornetworkemulationandMininetfordistributed system behavior.

References

[1] Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Sys- tems*, 3rd ed., Wiley, 2020.

[2] Zhao,L.,Wang,X.(2018).Areviewofcyberthreatsandcountermeasuresinthecontext of critical infrastructure. *IEEE Access.*

[3] Xu, H.,Zhang, Y. (2021). AI-enabled secure distributed systems: Challenges and solu- tions. *Journal of Systems Architecture*.

[4] N.Dragonietal.,"Microservices:Yesterday,Today,andTomorrow,"in*PresentandUlte- rior Software Engineering*, Springer, 2017.

[5] Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E.,Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In *IEEE Symposium on Security and Privacy*.

[6] SatoshiNakamoto."Bitcoin: APeer-to-PeerElectronicCashSystem."2008.