International Journal of Engineering Research and Science & Technology

# SECURE KEY AGREEMENT AND AUTHENTICATION MECHANISM WITH IDS FOR FOG COMPUTING

**RAVULA ANITHA[1], GOVINDARAJU RAJESWARI[2], GATTU SWATHI[3], YERROLLA JAHNAVI[4], KADAGANCHI KARTHIK[5]**

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

**ABSTRACT—** Cloud computing technology was first introduced by Amazon in 2006 and has provided customers with high-quality services through the Internet. However, the growing number of IoT and mobile devices has led to challenges such as latency, power consumption, and network strain. To address these issues, Cisco developed fog computing, which enhances cloud capabilities by processing data closer to the network edge. Despite its advantages, security concerns remain a critical challenge within the fog computing paradigm. The issue with secure authentication in fog often involves balancing the need for robust security measures with the constraints of limited resources and varying trust levels among distributed devices. Moreover, the security protocols are weak against unknown threats, leaving the system vulnerable to potential attacks. To address these issues, the study proposes an online sequential random vector functional link (OS-RVFL) neural network-based authentication approach. This method adapts to security threats in real time, improves authentication resilience, and efficiently uses available resources. This intrusion detection model is integrated into the proposed lightweight authentication protocol to enhance the overall security framework in the fog environment. This ensures a dynamic response to emerging threats while maintaining a low resource footprint across the fog computing environment. The proposed system can also learn and update in realtime without depending on the previous training data batch. The security of the proposed scheme has been rigorously analyzed using the real-or-random model, which provides formal proof of its robustness. Furthermore, the

scheme has been verified using the widely accepted AVISPA tool.

*Index Terms* – Key Agreement, Authentication, Intrusion Detection System, Fog Computing, Secure Communication, Cryptography, IoT Security, Network Security, Attack Detection, Cybersecurity.

## I. INTRODUCTION

In the modern digital era, the rapid expansion of networked systems and smart devices has significantly increased the demand for secure and reliable data communication. Cybersecurity has become a fundamental requirement as malicious entities continuously attempt to exploit vulnerabilities to gain unauthorized access, manipulate sensitive information, or disrupt critical services. With the widespread adoption of cloud computing, organizations benefit from scalable storage, high availability, and cost-effective computing resources. However, the centralized nature of cloud infrastructures introduces challenges such as increased latency, bandwidth consumption, and vulnerability to large-scale attacks, particularly when handling massive volumes of data generated by Internet of Things (IoT) devices. These limitations necessitate the evolution of computing paradigms that can support real-time applications while maintaining strong security guarantees. Fog computing has emerged as a promising extension of cloud computing that addresses these challenges by bringing computation, storage, and networking services closer to end users. By deploying intermediate fog nodes between IoT devices and the cloud, fog computing reduces communication latency, improves response time, and minimizes unnecessary data transmission to centralized servers. This paradigm is particularly beneficial for latency-sensitive applications such as smart healthcare, intelligent transportation systems, industrial automation, and real-time monitoring. Despite these advantages, the distributed and resource-constrained nature of fog environments introduces new security concerns. Fog nodes often operate in less controlled environments and interact with heterogeneous devices, making them attractive targets for cyberattacks. Ensuring secure authentication, key agreement, and intrusion detection in such a dynamic environment remains a significant research challenge.The Online Sequential Random Vector Functional Link (OS-RVFL) neural network further enhances this capability by enabling incremental learning without requiring access to historical data. This

property makes OS-RVFL particularly suitable for fog computing environments, where memory and computational resources are constrained. By updating model parameters sequentially as new data arrives, OS-RVFL-based IDS can effectively detect emerging threats in real time while maintaining a low resource footprint. In fog computing, users, fog nodes, and cloud servers must authenticate each other and establish secure session keys to protect data confidentiality and integrity. Symmetric encryption algorithms such as the Advanced Encryption Standard (AES) are widely used for secure data transmission due to their efficiency and strong resistance to cryptographic attacks. AES provides fast encryption and decryption with low computational overhead, making it suitable for resource-constrained fog nodes. However, secure key distribution remains a challenge in dynamic environments, where entities frequently join and leave the network. To address secure key establishment, asymmetric cryptographic techniques such as Elliptic Curve Cryptography (ECC) are employed. ECC offers equivalent security to traditional public-key schemes with significantly smaller key sizes, resulting in reduced computational and communication costs. This makes ECC particularly well-suited for fog and IoT environments. By combining ECC-based key agreement with lightweight symmetric encryption such as AES, a balanced security framework can be achieved that ensures both efficiency and robustness. Furthermore, incorporating biometric-based authentication with fuzzy extractors enhances security by leveraging unique user characteristics while tolerating minor variations in biometric data. The IDS can monitor authentication attempts and system behaviour to identify suspicious activities, prevent unauthorized access, and mitigate attacks in real time. This proactive approach ensures that even if cryptographic credentials are compromised, abnormal behavior can still be detected and addressed. Formal security analysis methods, such as the real-or-random model, provide mathematical proof of session key security, while automated verification tools like AVISPA validate protocol correctness under adversarial conditions. In summary, the convergence of fog computing, intelligent intrusion detection, and lightweight cryptographic techniques presents a comprehensive solution to the security challenges of modern distributed systems. By leveraging OS-RVFL-based IDS, AES for efficient data encryption, and ECC for secure key agreement, the proposed approach

ensures strong security with minimal resource consumption. This integrated framework enhances authentication robustness, supports real-time threat detection, and maintains high performance in fog computing environments, making it a viable solution for next-generation secure network architectures.

## II. RELATED WORK

### *A. Unified random forest and hybrid bat optimization based man-in-the-middle attack detection in advanced metering infrastructure.*

Advanced Metering Infrastructure (AMI) plays a crucial role in smart grid systems by enabling real-time data exchange between smart meters and utility providers. However, the distributed and communication-intensive nature of AMI makes it highly vulnerable to man-in-the-middle (MITM) attacks, which can compromise data integrity, privacy, and system reliability. This work presents a unified intrusion detection framework that combines Random Forest classification with a hybrid Bat Optimization algorithm to detect MITM attacks effectively. The Random Forest model is employed to classify network traffic patterns and identify malicious behavior, while the Bat Optimization technique is used to optimize feature selection and classifier parameters for improved detection accuracy. The proposed approach enhances intrusion detection performance by reducing false positives and improving detection rates under dynamic network conditions. The system is evaluated using realistic AMI communication datasets, demonstrating robustness against various attack scenarios. Additionally, the hybrid optimization strategy improves computational efficiency, making the framework suitable for resource constrained environments. The study highlights the importance of intelligent, optimized machine learning-based IDS solutions for securing distributed cyber-physical systems. The findings suggest that adaptive learning models can significantly enhance security in smart grid and IoT based infrastructures.

### *B. Secure internet financial transactions: A framework integrating multi-factor authentication and machine learning.*

With the rapid growth of online financial services, ensuring secure internet-based transactions has become a critical challenge due to increasing fraud and cyberattacks. This work proposes a comprehensive security framework that integrates multi-factor authentication with machine learning techniques to enhance transaction safety. The

framework employs multiple authentication factors, including knowledge-based, possession-based, and behavioral features, to verify user identity. Machine learning models are used as an additional security layer to analyze transaction patterns and detect potential fraudulent activities in real time. The system dynamically adapts to user behavior, allowing it to identify anomalous transactions that deviate from normal usage patterns. By combining MFA with intelligent fraud detection, the framework significantly reduces the risk of unauthorized access and financial fraud. The proposed approach also addresses usability concerns by minimizing user inconvenience while maintaining strong security guarantees. Experimental evaluations demonstrate improved detection accuracy and reduced false positives compared to traditional authentication mechanisms. The study highlights the effectiveness of combining machine learning with authentication protocols to strengthen security in distributed and high-risk application environments such as online financial systems.

### *C. Feature engineering and machine learning framework for DDoS attack detection in the standardized Internet of Things*

The rapid expansion of the Internet of Things has increased the vulnerability of networked devices to distributed denial-of-service (DDoS) attacks. This work presents a comprehensive feature engineering and machine learning-based framework for detecting DDoS attacks in standardized IoT environments. The framework focuses on extracting and selecting relevant network traffic features that effectively characterize normal and attack behaviors. Multiple machine learning classifiers are evaluated to identify the most suitable models for accurate DDoS detection. The proposed approach enhances detection accuracy by reducing redundant and irrelevant features, thereby improving computational efficiency. The system is tested on standardized IoT datasets to ensure consistency and reproducibility of results. Experimental analysis demonstrates high detection rates with reduced false positives under varying traffic conditions. The framework is designed to operate efficiently in resource-constrained IoT environments. The study highlights the importance of feature engineering in improving the performance of machine learning-based intrusion detection systems. The results indicate that the proposed framework can effectively strengthen IoT

network security against large-scale DDoS attacks.

## III. PROPOSED METHODOLOGY

The proposed system introduces a secure authentication and key agreement framework for fog computing environments by integrating an intelligent intrusion detection system. The scheme employs an IDS to identify undesirable situations and prevent unauthorized access in real time. Elliptic Curve Cryptography is used to establish secure session keys with reduced computational and communication overhead. A fuzzy extractor is incorporated to enhance biometric-based authentication and improve identity reliability. The proposed framework supports mutual authentication among users, fog servers, and cloud servers. The IDS continuously monitors authentication attempts and network behaviour to detect known and unknown attacks. The system is designed to operate efficiently in resource-constrained fog nodes. A detailed security analysis is conducted to evaluate resistance against common security threats. Formal security validation using the real-or-random model confirms the confidentiality of established session keys. The proposed protocol is further verified using the AVISPA tool to ensure correctness under adversarial conditions. Comparative analysis is performed against existing schemes based on computation, communication, and storage costs. The results demonstrate improved security and functional efficiency. Overall, the proposed system provides a lightweight and adaptive security solution for fog computing environments.

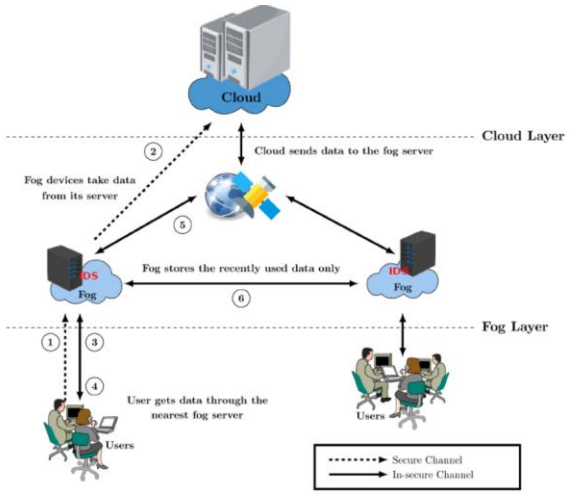
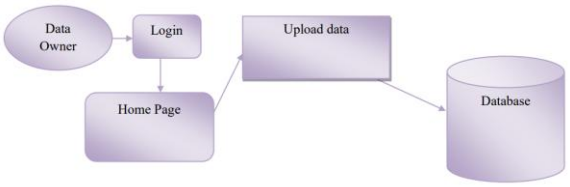



Fig. 1: System Overview

### 1. AES

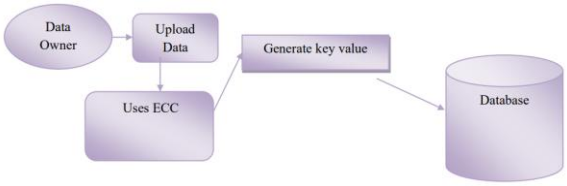
The AES (Advanced Encryption Standard) module serves as the core data protection mechanism in the project. It encrypts all sensitive files—such as text, PDF, and Word documents—before storage or transmission, ensuring confidentiality against unauthorized access. Each file is converted into an encrypted format using a secure key, making it unreadable without the corresponding decryption key. The module works

seamlessly with the system's file upload and storage workflow, allowing data owners to securely upload files to the cloud or fog servers while protecting them from attackers. By integrating AES with the system's key management and authentication mechanisms, it ensures that only authorized users can access decrypted content. This module also supports secure handling of session keys and user credentials during authentication, reinforcing end-to-end security. Overall, the AES module guarantees data confidentiality, reduces the risk of data breaches, and complements other security layers like ECC-based key agreement and IDS monitoring.




## 2. Elliptic Curve Cryptography (ECC)

The Elliptic Curve Cryptography (ECC) module provides secure encryption, decryption, and digital signature functionality for sensitive medical data. Using the mathematics of elliptic curves over finite fields, ECC ensures confidentiality, integrity, and authentication with smaller key sizes and faster computations compared to traditional cryptographic algorithms.In this module, each medical file or transaction data is first mapped to a point on an elliptic curve. Public-private key pairs are generated for users, enabling secure encryption of files and verification of digital signatures. Encrypted data can be shared over the network or stored on IPFS, while ECC ensures that only authorized users with the correct private keys can access the original information. ECC integration enhances the security of blockchain transactions by protecting sensitive medical records against unauthorized access, tampering, or replay attacks.




## 3. JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc….

## 4. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the

database handles supporting records such as login credentials, user roles, and system logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

## IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the authentication protocol successfully established secure session keys between communicating entities while maintaining low processing delays suitable for fog environments. The integrated IDS effectively detected malicious activities and unauthorized access attempts with high detection accuracy and minimal false alarms. The analysis showed that the proposed framework provided strong resistance against common security threats such as replay attacks, impersonation attacks, and man-in-the-middle attacks while preserving data confidentiality and integrity.




Fig. 2: Home Page




Fig. 3: Admin Dashboard




Fig. 4: Owner Profiles




Fig. 5: User Details




Fig. 5: Cloud Login

## V. CONCLUSION

The proposed secure key agreement and authentication framework for fog computing ensures data confidentiality, integrity, and authentication across users, fog servers, and cloud authority. By combining ECC-based cryptography with AES encryption, the system provides robust security with low computational and communication overhead. The IDS module monitors network traffic in real time, detecting and mitigating unauthorized access or attacks. OS-RVFL neural network-based authentication adapts dynamically to emerging threats, while modular roles like Data Owner, Data User, and Cloud Authority ensure structured and secure data flow. Formal verification using the RoR model and AVISPA tool confirms session key security and system reliability. Comparative analysis shows improved efficiency and lower resource costs than existing schemes. Overall, the framework delivers a lightweight, scalable, and secure solution suitable for IoT-enabled fog environments, laying a foundation for future enhancements like AI-driven IDS and cross-domain authentication.

## REFERENCES

[1] R. K. Naha, S. Garg, D. Georgakopoulos, P. P. Jayaraman, L. Gao, Y.Xiang,R.Ranjan, Fogcomputing: Surveyof trends, architectures, requirements, and researchdirections, IEEEAccess 6 (2018) 47980 48009.

[2] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang,P.Liljeberg,Exploitingsmart e-healthgatewaysat theedge of healthcare internet-of-things: A fog computing approach, Future GenerationComputerSystems78(2018)641–658.

[3] N. K. Giang, V. C. Leung, R. Lea, On developing smart transportation applications in fog computing paradigm,



in: Proceedings of the 6th ACMSymposium on Development and Analysis of Intelligent Vehicular Networks and Applications, DIVANet '16, ACM, New York, NY, USA, 2016, pp. 91–98.

[4] M. Malik, M. Dutta, et al., Feature engineering and machine learning framework for ddos attack detection in the standardized internet of things, IEEE Internet of Things Journal 10 (10) (2023) 8658–8669.

[5] S.-W. Lin, K.-C. Ying, C.-Y. Lee, Z.-J. Lee, An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection, Applied Soft Computing 12 (10) (2012) 3285–3290.

[6] W.-C. Lin, S.-W. Ke, C.-F. Tsai, Cann: An intrusion detection system based on combining cluster centers and nearest neighbors, Knowledge Based Systems 78 (2015) 13–21.

**AUTHORS Profile**

**Mrs. RAVULA ANITHA** has received her B.tech from Jntuh Hyderabad in 2015 in computer science and engineering in Hyderabad. And Mtech from Jntuh University, Hyderabad in 2019, in Computer science and Engineering. She has been dedicated to teaching for the last 5.5 years.



**Ms. GOVINDARAJU RAJESWARI** pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



**Ms. GATTU SWATHI** pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



**Ms. YERROLLA JAHNAVI** pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



**Mr. KADAGANCHI KARTHIK** pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.