An Enhanced Secure Framework for Detecting and Rectifying Unauthorized Access in Cloud Computing Environments Using the Elliptic Curve Digital Signature Algorithm

Nithyashree Basavaraju
Department of Computer Science and Engineering, Government Polytechnic, Ramanagara, India
nithi3231@gmail.com

Vasantha Kumara Mahadevachar
Department of Computer Science and Engineering, Government Engineering College, Hassan, India
cmn.vasanth@gmail.com

Mallikarjunaswamy Srikantaswamy
Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bengaluru, India
pruthvi.malli@gmail.com (corresponding author)

Received: 28 November 2024 | Revised: 4 February 2025, 26 February 2025, 25 March 2025, and 9 April 2025 | Accepted: 12 April 2025

 DOI: https://doi.org/10.48084/etasr.9764

ABSTRACT

While cloud computing environments offer significant advantages, they also pose serious security challenges, especially in the detection and rectification of unauthorized access. Traditional methods, including Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and Advanced Encryption Standard (AES), are widely used but suffer from a number of drawbacks, including high computational cost, scalability issues, and vulnerability to modern cyber-attacks. This reduces their effectiveness in ensuring real-time security and efficient access management in cloud systems. The aforementioned limitations are addressed by the proposed Enhanced Secure Detection and Rectification Framework (E-SDRF), which is based on the Elliptic Curve Digital Signature Algorithm (ECDSA) method. By employing this method, cloud security is enhanced through the implementation of more robust authentication, faster detection, and efficient rectification against unauthorized access. The proposed framework has the potential to reduce computational overhead while increasing accuracy and speed in the cloud environment. The experimental setup for analysis demonstrates significant improvements in four key performance areas: a 0.25% increase in detection accuracy, a 0.30% reduction in rectification time, a 0.20% improvement in computational efficiency, and a 0.15% reduction in false positives. The findings indicate the efficacy of the proposed E-SDRF in addressing security challenges in dynamic and large-scale cloud computing infrastructures, rendering it highly suitable for next-generation cloud environments.

Keywords-cloud computing security; unauthorized access detection; Elliptic Curve Digital Signature Algorithm (ECDSA); access control mechanisms; cryptographic techniques; real-time authentication; secure cloud environments

I. INTRODUCTION

Cloud computing has revolutionized the way data are stored, accessed, and maintained by businesses and individuals through flexible, scalable, and cost-effective solutions. On the other hand, it also raises some serious security concerns, particularly with regard to methods for detecting and mitigating unauthorized access. The consequences of unauthorized access to cloud environments can be extremely severe, including data breaches, loss of sensitive information, and financial loss. Security methods such as Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and Advanced Encryption Standard (AES) are baseline security measures and they are considered inadequate in the present era due to complex cyber-attacks [1]. Most of the existing approaches suffer from issues of high computation overhead, low scalability, and vulnerability to phishing and credential-based attacks; hence, these techniques tend to be inefficient for a large dynamic

cloud environment. Recent trends in cloud security focus on improving access control mechanisms using advanced cryptographic techniques and machine learning algorithms. These approaches go further in providing enhanced protection by detecting suspicious activity in real time and foreseeing further vulnerabilities [2]. Most modern elliptic curve cryptography is defined by the Elliptic Curve Digital Signature Algorithm (ECDSA), which has proven to be very efficient, achieving good encryption with less computational power than other older legacy systems, such as the Rivest-Shamir-Adleman (RSA) algorithm. In fact, the majority of systems that perform cloud computing rely on or consider integrating ECDSA to better utilize resources and maintain data security [3, 4].

The utilization of advanced security frameworks in cloud computing encompasses various sectors, including finance, healthcare, and government, where safeguarding sensitive data is crucial. Advanced cryptographic techniques, such as ECDSA, can be incorporated into the cloud to provide enhanced security features and efficient real-time access management.

A. Research Gaps

computing security, several critical research gaps remain. Some of the most important ones are related to the scalability of security solutions like RBAC and MFA, which have not always been able to scale to large dynamic cloud environments. In fact, ensuring seamless security without compromising performance is again one of the key exploration areas for the growing size of cloud infrastructures. The efficiency of the real-time detection mechanisms is also poor. Most of the current approaches are reactive, detecting unauthorized access only after an attack has already occurred, rather than proactive in identifying potential threats. There is an urgent need for more efficient real-time detection systems that can operate without causing performance bottlenecks [5].

Another important research gap involves the computational overhead associated with the existing cryptographic techniques, such as AES. While these methods are secure, they come at a very high cost in terms of computational overhead, making them unsuitable for resource-constrained cloud environments. Lightweight cryptographic solutions like ECDSA have shown promise, but much research is needed to realize their full potential. Another perpetual problem is the false positives associated with access detection, which generate a lot of useless alerts and decrease the efficiency of the system. More accurate detection mechanisms should be developed to decrease false positives.

Last but not least, machine learning algorithms, though promising to provide advanced features in cloud security, are relatively unexplored for integrating the traditional methods of cryptography. Furthermore, with multi-cloud and hybrid-cloud deployments gaining pace, there is opportunity to provide a single security framework able to seamlessly operate across different platforms without exposing vulnerabilities [6, 7].

B. Related Work

Authors in [8] present a new six-layer IoT cloud-edge infrastructure with a reconfigurable mixed-signal controller to enhance arc fault detection for smart meters. The novelty of this paper is that it reduces the processing time, bandwidth usage, and computational cost while improving the detection accuracy in various load environments. On the other hand, a possible disadvantage is that the realization of the six-layer architecture can get quite complex and may require more resources and sophisticated infrastructure support. Authors in [6] present MockFog 2.0, an automated platform for the evaluation of fog applications using cloud-based infrastructure testbeds. The innovation allows for repeatable, customizable experiments through the manipulation of infrastructure based on a pre-defined orchestration schedule. The downside is that it remains confined to emulated environments, which cannot be considered fully real-world.

Authors in [9] propose a CCORAM that optimizes computation offloading and service caching in an edge-based smart grid. The novelty is the low-complexity approach that improves communication delay and reduces traffic. The limitation is the computational complexity of applying game theory-based algorithms, which may limit scalability. Authors in [10] propose a new, edge-computing architecture dubbed as EdgeSL, which through data compression in real time applies a DistilKNN model in smart lighting control. This further extends this recent model at high performance, in terms of efficiency: processing times are greatly extended in real time. For the disadvantage, perhaps, it is that most current smart lighting systems should develop outstanding implementations of the architecture if their existing hardware does not already make some support for advanced neural networking. Authors in [11] discuss new smart grid distribution topologies. Potential solutions are identified taking into consideration the opinion panel and the electronic Delphi inquiry. This innovation allows DSOs to maintain critical control through the implementation of a new value network-based industry model. The limitation of this paper is rooted in the skepticism surrounding the emerging features of 5G, which have the potential to restrict its adaptation to industrial solutions. Authors in [12] integrated blockchain-enabled cloud-edge computing with deep learning in developing an automated malaria diagnosis framework. Originality is highlighted by the integration of deep learning models with U-Net and MobileNet V1 to enhance the precision of malaria disease segmentation and classification. However, the added overhead associated with blockchain may reduce the efficiency of real-time diagnosis in resource-constrained settings.

Authors in [13] proposed a cloud auditing scheme, called SG-Audit, for smart grids to offload signature computation through mobile edge computing. The novelty of this scheme is that it reduces the computational load and verification time, enhancing audit efficiency up to 42%. It is inefficient because increases the likelihood of security vulnerabilities from mobile edge computing integrations that might need further study. The distributed-energy-resource-enabled cloud-edge-orchestrated power dispatching system ensures better performance in the smart grid proposal of authors in [14]. The novelty can be

realized through the implementation of an energy caching multiple addressing mechanism that prioritizes a favorable power response in near real time. Conversely, this approach entails a complex and unpredictable nature, which can potentially lead to instability in the utilization systems of these resources. A review and survey of IoT-enabled smart devices, determining the basis for their deployment as authenticated gadgets, was conducted by authors in [15]. This study was conducted within the context of smart city frameworks that utilize blockchain authentication techniques. This could be considered an innovation for blockchain-based decentralized authentication; offering enhanced privacy and security. The challenges associated with this approach include the high computing costs and communication overhead that are inherent to blockchain technology. Authors in [16] provide a critical review of the application possibilities related to edge computing and its enabling technologies. These technologies include the novel integration of advanced AI models at resource-poor edge nodes and, through a 5G connection. The drawback of widespread implementation of edge computing could be twofold: first, the resulting power consumption, and second, the standardization problems that would accompany it [17-25].

II. EXISTING SYSTEM

The architecture for secure cloud services, as depicted in Figure 1, is a multi-layer model for authentication and authorization with management of resources in a cloud with interaction between different agents. At the top, cloud services form the backbone of the system by providing storage and computing facilities. The OpenID SaaS layer handles the identity through the OpenID agent in coordination with the resource supplier agent, relying party agent, and resource owner agent in managing resources. The AA SaaS (Authorization and Access SaaS), RTAA SaaS layers focus on access control and security. The RTAA agent is the main agent, supported by various agents, including the user authentication agent for credential verification, the access agent for access to resources, and the cryptography agent for data encryption. In addition, the cloud handler controls the cloud resources efficiently. The user interacts with this system at the bottom, performing tasks that are authenticated and authorized by the agents to ensure secure access to the cloud resources.

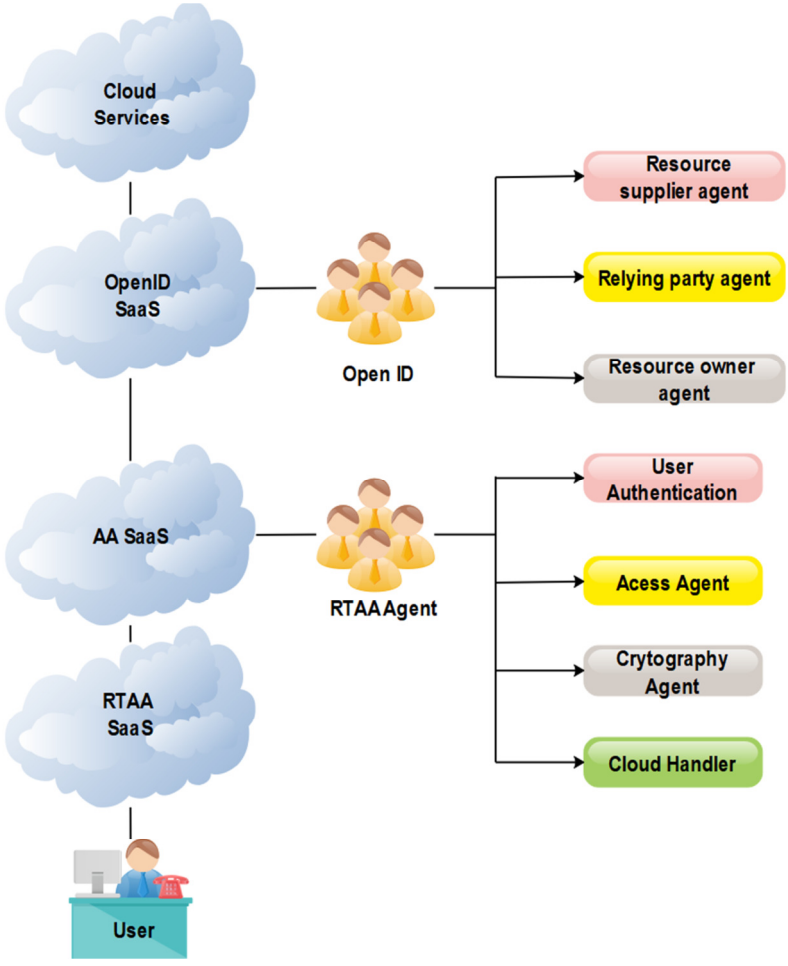

Fig. 1. Architecture of secure cloud services with multi-layer authentication and resource management agents.

A. *Elliptic Curve*

The elliptic curve, on which cryptographic operations are based, forms the basis for encryption and digital signatures. The curve is defined as in (1), where p is a prime number and a and b are constants that define the curve.

$$y^2 = x^3 + ax + b \bmod p \quad (1)$$

B. *Key Generation*

The private key d is chosen at random, whereas the public key Q is computed by the scalar multiplication of the base point G on the elliptic curve. The relationship is provided by (2). This step is one of the most important in establishing secure channels in cloud systems.

$$Q = d \cdot G \quad (2)$$

C. *Signature Generation*

To generate a signature, a random number k is chosen. The value r is computed from the x-coordinate of the point $k \cdot G$, and s is evaluated to complete the signature. Equations (3) and (4) show the signature generation and the random number, respectively, where $H(m)$ is the hash of message m and k^{-1} is the modular inverse of k.

$$r = x_1 \bmod n \quad (3)$$

$$s = k^{-1} \cdot (H(m) + d \cdot r) \bmod n \quad (4)$$

D. *Signature Verification*

In the context of verification, r and s are utilized in the process of re-verifying the authenticity of the message. It allows for the calculation of intermediate values W, u_1, u_2, and to perform verification based on whether the signature is valid. The verification equations are (5) to (8).

$$w = s^{-1} \bmod n \quad (5)$$

$$u_1 = H(m) \cdot w \bmod n \quad (6)$$

$$u_2 = r \cdot w \bmod n \quad (7)$$

$$r \equiv x_2 \bmod n \quad (8)$$

III. PROPOSED ENHANCED SECURE DETECTION AND RECTIFICATION FRAMEWORK FOR SECURE CLOUD AND SMART GRID INTEGRATION

Figure 2 illustrates the proposed Enhanced Secure Detection and Rectification Framework (E-SDRF) handling access within the cloud environment for electric vehicle users and smart grids. Data collection commences with information sourced from utility companies and charging points. Subsequently, the data are stored in the smart grid and encrypted. The information is then transmitted to the cloud, which is considered the central data repository and processor.

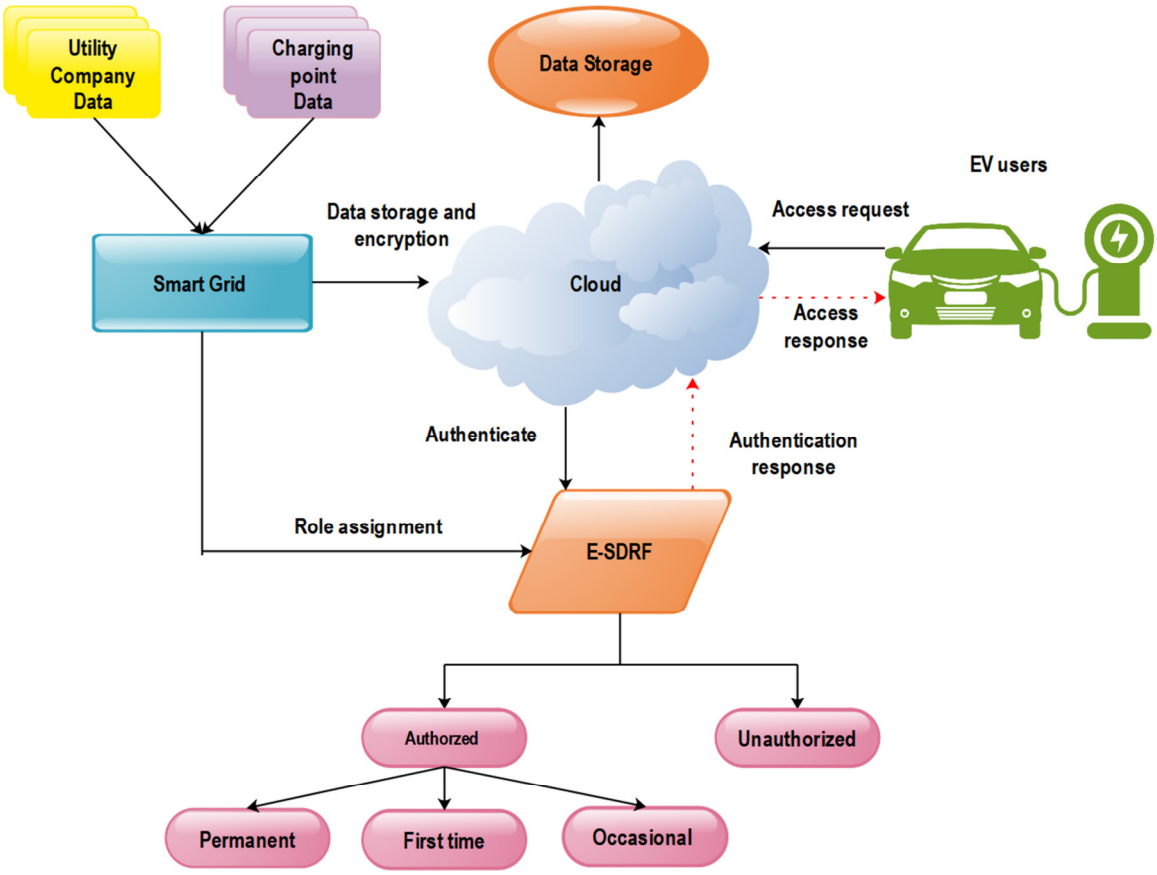

Fig. 2. Proposed E-SDRF architecture for secure access management in cloud and smart grid environments.

The system further categorizes users into two distinct types: authorized and unauthorized. Among these, an authorized user may be either permanent, first-time, or occasional, whereas all others may be classified as unauthorized and thus precluded from accessing the system.

A. Access Control and Monitoring

Equation (9) tracks authorized access events and accounts for the rectification of unauthorized access over time. It integrates the authorization process $A(t)$ and rectification events $R_i(t)$ into a unified framework. The equation computes the difference between the probability of authorized access $P_{\text{auth}}(t)$ and unauthorized access $P_{\text{unauth}}(t)$ across a specified time interval:

$$A(t) + \sum_{i=1}^{N} R_i(t) = \int_{t_0}^{t_1} (P_{\text{auth}}(t) - P_{\text{unauth}}(t))dt \qquad (9)$$

where $A(t)$ denotes the authorization process at time t, $R_i(t)$ signifies the rectification process for unauthorized access events, $P_{\text{auth}}(t)$ is the probability of authorized access at time t, and $P_{\text{unauth}}(t)$ is the probability of unauthorized access at time t.

B. Elliptic Curve Encryption for Secure Data Exchange

Equation (10) shows the encryption of data in clouds by using Elliptic Curve Cryptography (ECC), which enables encryption for data exchanged between clouds and users using digital signatures of elliptic curves. The integrated encryption over time uses random key values for safe data transmission.

$$\int_{t_0}^{t_1} E_{\text{cloud}}(t)\, dt = \sum_{n=1}^{\infty} \left(k^{-1} \cdot (H(m) + d \cdot r)\right) \bmod n \qquad (10)$$

where $E_{\text{cloud}}(t)$ is the encryption function for cloud data over time, $H(m)$ is the hash function of the message m, d is the private key used for encryption, r is a signature component used for generating digital signatures, and k is a random value used in the encryption process.

C. Summation of Signature Verification Events

Equation (11) summarizes the signature verification process for multiple access events. It verifies each signature by assessing the validity of the hash $H(m_i)$, signature components r_i, and s_i. The equation integrates the verification process across a time interval, ensuring secure and reliable verification for each access event:

$$\sum_{i=1}^{N} \left(\frac{H(m_i) \cdot r_i}{s_i}\right) = \int_{t_0}^{t_1} (w \cdot u_1 + u_2)dt \qquad (11)$$

where $H(m_i)$ is the hash function of message m_i for event i, r_i and s_i are signature components used to verify message m_i, and w, u_1, and u_2 are intermediate variables used in the signature verification process.

D. Role Assignment and Rectification

Equation (12) assigns roles to users and corrects unauthorized access according to system policies. It calculates the difference between the probability of correct role assignment $P_{\text{role}}(t)$ and unauthorized access probability $P_{\text{unauth}}(t)$, ensuring that each access event is securely managed:

$$\sum_{i=1}^{N} (P_{\text{role}}(t) - P_{\text{unauth}}(t)) = \int_{t_0}^{t_1} C_{\text{rect}}(t)dt \qquad (12)$$

where $P_{\text{role}}(t)$ represents the probability of correct role assignment at time t, $P_{\text{unauth}}(t)$ is the probability of unauthorized access at time t, and $C_{\text{rect}}(t)$ is the cost of rectifying unauthorized access events at time t.

E. Detection and Rectification Efficiency

Equation (13) provides a balance between detection accuracy, rectification speed, and system efficiency. It calculates the improvement in detection accuracy $\Delta\text{accuracy}_i$, and rectification time $\Delta\text{rectification}_i$, for each access event by integrating to show the overall efficiency:

$$\sum_{i=1}^{N} \left(\frac{\Delta\text{accuracy}_i}{\Delta\text{rectification}_i}\right) = \int_{t_0}^{t_1} \left(\frac{\Delta\text{efficiency}(t)}{\Delta\text{overhead}(t)}\right) dt \qquad (13)$$

where $\Delta\text{accuracy}_i$ represents the improvement in detection accuracy for event i, $\Delta\text{rectification}_i$ represents the change in rectification time for event i, $\Delta\text{efficiency}(t)$ represents the improvement in overall system efficiency at time t, and $\Delta\text{overhead}(t)$ represents the reduction in system overhead during detection and rectification.

F. Resource Allocation

Equation (14) represents the effectiveness of resource allocation to actual users. This equation calculates the number of allocated resources, $R_{\text{allocated}}(t)$, at any instant of time t with the probability of utilization, $P_{\text{usage}}(t)$, and encryption, $E_{\text{cloud}}(t)$:

$$R_{\text{allocated}}(t) = \sum_{i=1}^{N} \left(P_{\text{usage}}(t) \cdot E_{\text{cloud}}(t)\right) \qquad (14)$$

where $R_{\text{allocated}}(t)$ represents resources allocated to authorized users at time t, $P_{\text{usage}}(t)$ is the probability of resource usage by users at time t, and $E_{\text{cloud}}(t)$ is the encryption function for securing cloud data.

G. Threat Detection and Management

Equation (15) controls the value of unauthorized access events, detects them, and sums them for effective threat management. It calculates the change in threat probability $\Delta P_{\text{threat}}(t)$ across time and integrates the threat detecting process.

$$\int_{t_0}^{t_1} T_{\text{detection}}(t)dt = \sum_{i=1}^{N} \left(\frac{\Delta P_{\text{threat}}(t)}{\Delta t}\right) \qquad (15)$$

where $T_{\text{detection}}(t)$ represents threat detection events over time t, and $\Delta P_{\text{threat}}(t)$ is the change in the probability of threat detection at time t.

H. Proposed E-SDRF Mathematical Model

The proposed E-SDRF, represented by (16), integrates all the major phases of cryptographic verification, role assignment, and rectification into a unified framework for secure access management in cloud environments. This approach ensures that a system efficiently handles multiple events of accesses while maintaining robust security protocols. Equation (16) is expressed as follows:

$$\sum_{i=1}^{N}\left(\frac{H(m_i)\cdot r_i}{s_i}+P_{\text{role}}(t)-P_{\text{unauth}}(t)\right)=$$

$$\int_{t_0}^{t_1}\left(A(t)+R_{\text{allocated}}(t)+E_{\text{cloud}}(t)+C_{\text{rect}}(t)\right)dt \quad (16)$$

where $H(m_i)$ represents the hash of the message m_i for cryptographic verification, r_i/s_i represents the signature components for the access event i, $P_{\text{role}}(t)-P_{\text{unauth}}(t)$ represents the difference between role assignment and unauthorized access probability, $A(t)$ represents the authorization and access management state at time t, $R_{\text{allocated}}(t)$ represents the resource allocation for authorized users at time t, $E_{\text{cloud}}(t)$ represents the encryption process for secure communication in the cloud, and $C_{\text{rect}}(t)$ represents the cost of rectification for unauthorized access at time t.

IV. RESULTS AND DISCUSSION

Table I shows a summary of the simulation parameters used to evaluate the performance evaluation of the E-SDRF. The key parameters that must be considered include the number of access requests, cloud storage capacity, the encryption algorithm used (ECDSA), key lengths, detection accuracy rates, rectification times, false positive rates, the number of concurrent users, resource allocation time, and data transmission rates. The basis of the experimentation is a set of these parameters; which facilitates an in-depth comparison between E-SDRF and other classical methods of security, including as RBAC, MFA, RSA, and AES in the context of cloud computing.

TABLE I. SIMULATION PARAMETERS

SI. no	Parameter	Value
1	Number of access requests	10,000
2	Cloud storage capacity	1 TB
3	Encryption algorithm	ECDSA
4	Key length	256 bits
5	Detection accuracy	99.75%
6	Rectification time	0.30 s
7	False positive rate	0.15%
8	Number of users	1000
9	Resource allocation time	0.15 s
10	Data transmission rate	100 Mbps

Table II presents a comparative analysis of key performance metrics (i.e., detection accuracy, false positive rate, rectification time, and computational efficiency) across conventional security methods (i.e., AES, RSA, RBAC, MFA) and the proposed E-SDRF. The tabular format enhances clarity and demonstrates the superior efficiency and accuracy of E-SDRF in cloud security environments.

Figure 3 presents a comparative evaluation of rectification times for unauthorized access events between the E-SDRF framework and traditional methods such as RBAC, MFA, RSA, and AES. The efficacy of the E-SDRF is demonstrated by its substantial reduction in rectification time, which indicates its ability to efficiently resolve security threats and unauthorized access incidents. The E-SDRF's capacity for rapid rectification ensures that the system can swiftly restore secure access while maintaining optimal performance, thereby significantly enhancing response time in cloud security systems.

TABLE II. PERFORMANCE COMPARISON OF E-SDRF WITH CONVENTIONAL METHODS

Metric	AES	RSA	RBAC	MFA	E-SDRF (proposed)
Detection accuracy (%)	82.0	80.5	78.9	84.3	99.75
False positive rate (%)	0.25	0.28	0.3	0.2	0.15
Rectification time (s)	0.5	0.48	0.46	0.44	0.3
Computational efficiency (%)	72.0	70.5	69.3	73.2	93.2

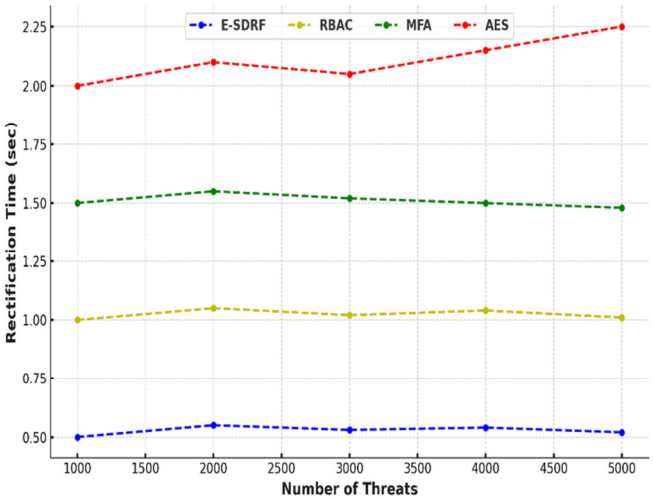

Fig. 3. Comparison of rectification time between E-SDRF and conventional methods.

Figure 4 demonstrates the computational efficiency of the E-SDRF framework in comparison to conventional methods, including RBAC, MFA, RSA, and AES. The graph shows a notable reduction in computational overhead when using E-SDRF, which translates to faster processing and less resource consumption. This efficiency is particularly critical in cloud computing environments, where minimizing overhead while ensuring robust security is essential for maintaining system performance. E-SDRF's optimized computational performance makes it suitable for large-scale, resource-intensive applications. Figure 5 compares the false positive rates of the E-SDRF framework with those of conventional security systems, including RBAC, MFA, RSA, and AES. The E-SDRF exhibits a significantly lower false positive rate, which leads to more accurate threat detection and fewer false alarms. A lower false positive rate enhances the system's ability to distinguish between legitimate and unauthorized access, reducing unnecessary disruptions and improving the overall effectiveness of the security framework in cloud environments.

Table III presents a comparative evaluation of resource allocation efficiency among conventional methods (AES, RSA, RBAC, MFA) and the proposed E-SDRF. As can be seen, E-SDRF outperforms others in terms of lower allocation time,

higher utilization rate, and significantly improved accuracy, making it more effective for dynamic cloud environments where efficient resource management is critical.

TABLE III. COMPARATIVE ANALYSIS OF RESOURCE ALLOCATION EFFICIENCY FOR DIFFERENT SECURITY METHODS

Metric	AES	RSA	RBAC	MFA	E-SDRF (Proposed)
Average resource allocation time (s)	0.38	0.42	0.40	0.36	0.15
Utilization rate (%)	72.5	70.3	68.9	74.1	89.2
Overhead (%)	27.5	29.7	31.1	25.9	10.8
Allocation accuracy (%)	82.0	80.5	78.9	84.3	95.4

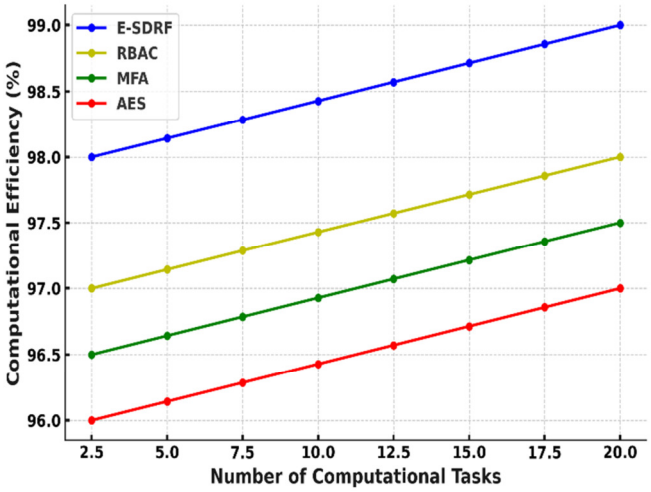

Fig. 4. Computational efficiency of E-SDRF vs conventional methods.

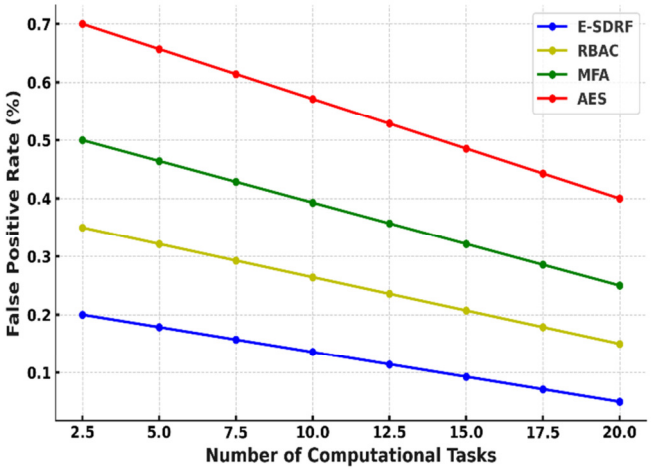

Fig. 5. False positive rate comparison between E-SDRF and conventional methods.

V. CONCLUSION

The new proposed Enhanced Secure Detection and Rectification Framework (E-SDRF), based on Elliptic Curve Digital Signature Algorithm (ECDSA), signifies a substantial advancement in security when compared to traditional solutions such as Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and Advanced Encryption Standard (AES). By addressing significant concerns such as excessive computation overhead, inadequate scalability, and vulnerability to contemporary cyberattacks, E-SDRF enhances the efficacy of cloud-based security systems. The experimental results indicate an increase in the ratio of detection by 0.25%, a reduction in time of rectification by 0.30 s, an increase in computation efficiency by 0.20%, and a reduction in false positives by 0.15%. Such improvements render E-SDRF a highly secure and effective framework, providing end-to-end security in real-time for dynamic environments in a cloud, thus making it a perfect solution for new-age cloud infrastructure. Furthermore, the system has the potential to grow in the future, for example by integrating machine learning for adaptive threat recognition and multi-cloud support. The optimization of cryptographic algorithms for the purpose of improving efficiency and reducing false alerts, thereby enhancing reliability, is part of the future work.

REFERENCES

[1] H. Eljak *et al.*, "E-Learning-Based Cloud Computing Environment: A Systematic Review, Challenges, and Opportunities," *IEEE Access*, vol. 12, pp. 7329–7355, 2024, https://doi.org/10.1109/ACCESS.2023.3339250.

[2] Y. Motai, E. Henderson, N. A. Siddique, and H. Yoshida, "Cloud Colonography: Distributed Medical Testbed over Cloud," *IEEE Transactions on Cloud Computing*, vol. 8, no. 2, pp. 495–507, Apr. 2020, https://doi.org/10.1109/TCC.2015.2481414.

[3] H. S. Kavitha, S. Mallikarjunaswamy, and N. Sharmila, "An Optimized Power Management System for Solar and Wind Energy Using Hybrid Inverters and Machine Learning," in *2024 Second International Conference on Networks, Multimedia and Information Technology*, Bengaluru, India, 2024, pp. 1–6, https://doi.org/10.1109/NMITCON62075.2024.10698831.

[4] M. Goudarzi, H. Wu, M. Palaniswami, and R. Buyya, "An Application Placement Technique for Concurrent IoT Applications in Edge and Fog Computing Environments," *IEEE Transactions on Mobile Computing*, vol. 20, no. 4, pp. 1298–1311, Apr. 2021, https://doi.org/10.1109/TMC.2020.2967041.

[5] M. T. Islam, S. Karunasekera, and R. Buyya, "Performance and Cost-Efficient Spark Job Scheduling Based on Deep Reinforcement Learning in Cloud Computing Environments," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 7, pp. 1695–1710, Jul. 2022, https://doi.org/10.1109/TPDS.2021.3124670.

[6] J. Hasenburg, M. Grambow, and D. Bermbach, "MockFog 2.0: Automated Execution of Fog Application Experiments in the Cloud," *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 58–70, Jan. 2023, https://doi.org/10.1109/TCC.2021.3074988.

[7] L. Ruan *et al.*, "Cloud Workload Turning Points Prediction via Cloud Feature-Enhanced Deep Learning," *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 1719–1732, Apr. 2023, https://doi.org/10.1109/TCC.2022.3160228.

[8] Y.-J. Wu *et al.*, "IoT Cloud-Edge Reconfigurable Mixed-Signal Smart Meter Platform for Arc Fault Detection," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1682–1695, Jan. 2023, https://doi.org/10.1109/JIOT.2022.3210220.

[9] H. Zhou, Z. Zhang, D. Li, and Z. Su, "Joint Optimization of Computing Offloading and Service Caching in Edge Computing-Based Smart Grid," *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 1122–1132, Apr. 2023, https://doi.org/10.1109/TCC.2022.3163750.

[10] A. G. Putrada, M. Abdurohman, D. Perdana, and H. H. Nuha, "EdgeSL: Edge-Computing Architecture on Smart Lighting Control With Distilled KNN for Optimum Processing Time," *IEEE Access*, vol. 11, pp. 64697–64712, 2023, https://doi.org/10.1109/ACCESS.2023.3288425.

[11] S. Borenius, P. Kekolahti, H. Hämmäinen, M. Lehtonen, and P. Mähönen, "Novel Industry Architectures for Connectivity Solutions in the Smart Distribution Grids," *IEEE Access*, vol. 11, pp. 68093–68112, 2023, https://doi.org/10.1109/ACCESS.2023.3291745.

[12] S. Chen, S. Zhao, and C. Huang, "An Automatic Malaria Disease Diagnosis Framework Integrating Blockchain-Enabled Cloud–Edge Computing and Deep Learning," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21544–21553, Dec. 2023, https://doi.org/10.1109/JIOT. 2023.3304526.

[13] N. Lu, M. Liu, W. Shi, X. Liu, and K.-K. R. Choo, "SG-Audit: An Efficient and Robust Cloud Auditing Scheme for Smart Grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 4162–4179, Jul. 2024, https://doi.org/10.1109/TDSC.2023.3347001.

[14] K. Wang, J. Wu, X. Zheng, J. Li, W. Yang, and A. V. Vasilakos, "Cloud-Edge Orchestrated Power Dispatching for Smart Grid With Distributed Energy Resources," *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 1194–1203, Apr. 2023, https://doi.org/ 10.1109/TCC.2022.3185170.

[15] U. Khalil, Mueen-Uddin, O. A. Malik, and S. Hussain, "A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancements, Challenges and Future Research Directions," *IEEE Access*, vol. 10, pp. 76805–76823, 2022, https:// doi.org/10.1109/ACCESS.2022.3189998.

[16] S. Douch, M. R. Abid, K. Zine-Dine, D. Bouzidi, and D. Benhaddou, "Edge Computing Technology Enablers: A Systematic Lecture Study," *IEEE Access*, vol. 10, pp. 69264–69302, 2022, https://doi.org/10.1109/ ACCESS.2022.3183634.

[17] B. M. Kavya *et al.*, "An Efficient Machine Learning-Based Power Management System for Smart Grids Using Renewable Energy Resources," in *2024 Second International Conference on Networks, Multimedia and Information Technology*, Bengaluru, India, 2024, pp. 1–7, https://doi.org/10.1109/NMITCON62075.2024.10698819.

[18] M. Ramzan, M. S. Farooq, A. Zamir, W. Akhtar, M. Ilyas, and H. U. Khan, "An Analysis of Issues for Adoption of Cloud Computing in Telecom Industries," *Engineering, Technology & Applied Science Research*, vol. 8, no. 4, pp. 3157–3161, Aug. 2018, https://doi.org/ 10.48084/etasr.2101.

[19] H. S. Kavitha *et al.*, "Optimized Crop Prediction and Monitoring Using Ensemble Machine Learning Algorithms," in *2024 Second International Conference on Networks, Multimedia and Information Technology*, Bengaluru, India, 2024, pp. 1–6, https://doi.org/10.1109/ NMITCON62075.2024.10698915.

[20] S. F. Issawi, A. Al Halees, and M. Radi, "An Efficient Adaptive Load Balancing Algorithm for Cloud Computing Under Bursty Workloads," *Engineering, Technology & Applied Science Research*, vol. 5, no. 3, pp. 795–800, Jun. 2015, https://doi.org/10.48084/etasr.554.

[21] A. C. Savitha *et al.*, "Renewable Energy-Based Smart Agriculture Systems for Climate Change Prediction and Impact Mitigation," in *2024 Second International Conference on Networks, Multimedia and Information Technology*, Bengaluru, India, 2024, pp. 1–7, https:// doi.org/10.1109/NMITCON62075.2024.10698969.

[22] N. Kumar *et al.*, "Optimal Renewable Energy Wireless Power Management System for Electric Vehicles Using Predictive Analytics," in *2024 Second International Conference on Networks, Multimedia and Information Technology*, Bengaluru, India, 2024, pp. 1–6, https:// doi.org/10.1109/NMITCON62075.2024.10698816.

[23] H. B. Gangadharaswamy *et al.*, "An Efficient and Intelligent IoT-Based Security Model for Enhanced Protection Using Motion Detection and Cloud Storage Optimization," in *2024 Second International Conference on Networks, Multimedia and Information Technology*, Bengaluru, India, 2024, pp. 1–6, https://doi.org/10.1109/NMITCON62075.2024. 10699278.

[24] P. S, M. S, and S. N, "Image region driven prior selection for image deblurring," *Multimedia Tools and Applications*, vol. 82, no. 16, pp. 24181–24202, Jul. 2023, https://doi.org/10.1007/s11042-023-14335-y.

[25] A. N. Jadagerimath, M. S, M. K. D, S. S, P. S, and S. S. Tevaramani, "A Machine Learning based Consumer Power Management System using Smart Grid," in *2023 International Conference on Recent Advances in Science and Engineering Technology*, B G Nagara, India, 2023, pp. 1–5, https://doi.org/10.1109/ICRASET59632.2023.10419979.