Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 1887–1898
DOI : 10.47974/JDMSC-2365

The secured authentication system : Integrated cyber security end-to-end based cyber-physical systems for improved DevOps resilience with authentication

Vishnu Priya Arivanantham *
Department of Computational Intelligence
School of Computer Science and Engineering
Vellore Institute of Technology
Vellore 632014
Tamil Nadu
India

Hayder M. A. Ghanimi †
Department of Information Technology
College of Science
University of Warith Al-Anbiyaa
Karbala 5751
Iraq

and

Department of Computer Science
College of Computer Science and Information Technology
University of Kerbala
Karbala 5751
Iraq

Vijaya Krishna Sonthi §
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram 522502
Andhra Pradesh
India

* *E-mail:* a.vishnupriya@vit.ac.in (Corresponding Author)
† *E-mail:* hayder.alghanami@uowa.edu.iq
§ *E-mail:* vijayakrishna1990@gmail.com

Firas Tayseer Ayasrah ‡
College of Education, Humanities and Science
Al Ain University
Al Ain 64141
United Arab Emirates

Reena Mahapatra Lenka @
Symbiosis Institute of Management Studies
Symbiosis International (Deemed) University
Pune 411020
Maharashtra
India

P. Hemalatha #
Department of Computer Science and Engineering
Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology
Chennai 600062
Tamil Nadu
India

Sudhakar Sengan $
Department of Computer Science and Engineering
PSN College of Engineering and Technology
Tirunelveli 627152
Tamil Nadu
India

Pankaj Dadheech ^
Department of Computer Science and Engineering
Swami Keshvanand Institute of Technology, Management & Gramothan (SKIT)
Jaipur 302017
Rajasthan
India

Abstract

The software development model is changing fast, and the challenge of security remains the primary attention, particularly with the implementation of Development

‡ *E-mail:* **firas.ayasrah@aau.ac.ae**
@ *E-mail:* **reena.lenka@sims.edu**
# *E-mail:* **drhemalathap@veltech.edu.in**
$ *E-mail:* **sudhasengan@gmail.com**
^ *E-mail:* **pankajdadheech777@gmail.com**

and Operations (DevOps), Distributed Ledger Technology (DLT), and other methods. Thus, when such technologies are integrated within organizations, it becomes essential to measure the use of the technologies in Anomaly Detection (AD) and access management. This research work evaluates the competence of these technologies based on measures such as the Detection Rate (DR) and the False Positive Rate (FPR). Statistics reveal that as the number of records increases. DR improves across all methods, with DevOps Resilience with Authentication (DevOps-RAS) achieving the highest DR of 95.94% at 500 records, compared to 81.23% for CAMS and 85.43% for DLT. Conversely, FPR increases with record size, with DevOps RAS presenting a higher FPR of 95.78% at 500 records, compared to 76.45% for CAMS and 83.56% for DLT. These visions should help organizations determine the most effective security method for Cyber-Physical Systems (CPS), thereby maximizing DR while minimizing the FPR required to enhance the system's overall robustness.

Subject Classification: *93E10, 94A13.*

Keywords: *DevOps, Security, Privacy, Detection, Positive rate, Blockchain, Access control.*

1. Introduction

The DevOps practice is a vital component in the software development life cycle, enhancing the speed, flexibility, and reliability of processes [1]. However, it is definite that the application of Cyber-Physical Systems (CPS) in this field is rapidly evolving, and questions related to security are becoming increasingly higher, which threatens the efficiency and stability of Development and Operations (DevOps). To counter these problems, an End-To-End (ETE) robust security model should be integrated to enhance the DevOps solution in terms of security, primarily by providing a more effective means of Anomaly Detection (AD). It assumes the improvement of the software development cycle, which includes implementing a set of measures to prevent attacks from the setup phase by implementation and subsequent updates [2]. The primary reason for ETE security in DevOps is to implement a CPS with a web of security measures that would secure it from attacks such as intrusions, data loss, and hacking [3]. This involves implementing measures that reduce users' and systems' access to critical resources or areas. Traditional AD, such as usernames and passwords, are gradually observed as inadequate in addressing evolving attacks. Therefore, modern security methods are based on complex methods such as Multi-Factor Authentication (MFA), biometric identification, and behavioral modeling to enhance security and privacy against attacks [4]. The MFA is one of the most vital methods applied in contemporary enterprise CPS. MFA is a method that increases security by requiring users to enter more than one method of AD, such as a password and a passcode received on a mobile device for a limited time, thereby enhancing security. This added layer of security is significant, especially in DevOps, since frequent changes and integration may lead to such vulnerabilities.

Additionally, fingerprint or face recognition enhances security by verifying the user's identity by physical features [5]. Another component of an ETD security system is Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), which define a user's access control in the system. RBAC restricts a user's operations with the CPS based on the roles they have in the organization; thus, the user cannot exceed their assigned function and privileges [6]. ABAC is more elaborate in its implementation because it employs attributes such as user identity, time, and location to compute access control. These methods enhance security by decreasing the attack surface and ensuring access rights are limited and monitored [7]. Monitoring and automated AD are also behaviors that sustain the DevOps practice apart from authentication. SIEM and IDS monitor traffic and users' activities and identify suspicious activity. Such CSPs employ ideas like Machine Learning (ML) and Artificial Intelligence (AI) to identify and mitigate attacks and suspicious activities as they occur, allowing for an appropriate response to be completed.

DevSecOps, or the inclusion of security into the development lifecycle, is a method of attaining security rather than a mere afterthought at the development stage. This approach encourages the integration of security solutions in all development phases, from coding and testing to deployment and CSP updates. Static and dynamic code analysis tools perform testing during the development phase, minimizing security attacks in real-time applications [8]. The resistance of a DevOps environment also depends on the volume of expertise required to recover from security attacks. This requires effective incident handling and disaster management policies that describe how to recognize, halt, and minimize the effects of an actual or perceived security attack. Maintenance of the updated and tested incident response plan ensures that teams are ready to respond to any security incident with less or no impact on system Confidentiality, Integrity, and Availability (CIA). Constructing an ETE comprehensive security model that targets boosting DevOps' reliability can't be achieved without a range of methods that deal with advanced AD, continuous monitoring, and proactive security measures in each SDLC phase [9].

With the adoption of defense-in-depth, the integration of security into DevOps, and a distinct task response approach, organizations can achieve a more secure DevOps environment without compromising the efficiency of software delivery. The DevOps paradigm is rapidly gaining acceptance in the software industry; thus, organizations are required to change their culture and automate and implement measurement practices and knowledge sharing to sustain their performance. The guidelines for sustainable DevOps were found from the literature review and survey conducted in this research, and it was determined that culture is the most essential data, with 48 guidelines identified. Some fundamental guidelines include developing principles of collaboration by the microservices model, evaluating the readiness of the microservices model, and training heads to gain support [10]. Furthermore, a proposal for DevOps for Blockchain (BC) use cases has been presented, focusing on contribution transparency and traceability, tamper-proofness, immutability, and compliance with standards to foster consensus in the practice and development of BC, as well as its integration with industry and academia [11].

Moreover, Distributed Ledger Technology (DLT) also presents an opportunity for DISs, as it addresses key model features and operates globally. This paper presents a real-life application of DLT in DIS [12]. The research work is divided into the following sections: Section 1 provides a summary of DevOps-RAS + BC, examining past similar studies; Section 2 presents the recommended CPS; Section 3 presents the results with analysis; and Section 4 concludes the work.

2. Proposed DevOps-RAS Model

To create an effective model for strengthening security in DevOps, focusing on authentication, one can utilize a mathematical model to quantify qualities, features, or security factors and their relationships and interactions and recommend an optimal setup. The following is a brief mathematical model that incorporates components such as risk evaluation, authentication speed, and AD [13-14]. With the help of this model, it is possible to evaluate the use of security results within the DevOps context. The risk assessment model measures the risk connected to definite probable weaknesses. The risk '**R**' as Eq. (1), where the probability of a task, the severity of the result of a task, and the probability of the event occurring are considered.

$$R = S \times V \times I \tag{1}$$

Where, S→Severity and ranges between 0 to 1, with 0 being no impact and 1 being the catastrophic impact; V→stands for the vulnerability of misuse, ranging between 0 and 1 where 0 means no probability of exploitation and 1 being specific exploitation, I→The impact of exploitation ranging between 0 to 1 with 0 being no impact and 1 being maximum impact. The effectiveness of an authentication system can be determined using the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). The objective is to reduce both rates to the required levels while ensuring that the model is secure and usable. The overall efficiency '**E**' of the authentication system can be modeled, as it was in Eq. (2).

$$E = 1 - \frac{FAR + FRR}{2} \tag{2}$$

Where, **FAR**→The chance that an unauthorized user is wrongly approved access **FRR**→The chance that an authorized user is wrongly denied access). The DR and FPR are analyzed to measure the accuracy of the AD. The DR illustrates the system's ability to detect real security attacks, which is achieved by dividing the sum of true attacks by the sum of AD, as determined by the CPS. On the other hand, FPR measures the fraction of benign activities the system labels as attacks, which can be used to assess the system's capability to generate false alarms. To measure the effect of the DR on the overall AD performance, 'P' as Eq. (3).

$$P = \frac{DR - FPR}{1 - FPR} \tag{3}$$

This Eq. (3) modifies the DR by subtracting the FPR from it, thereby providing a more accurate representation of the overall use of the CPS in AD while minimizing false alarms. A cost-benefit analysis can be used to compare the cost of employing all the security measures. The cost 'C' and benefit 'B' are related to the security CPS as Eq. (4) and Eq. (5).

$$C = C_{implementation} + C_{maintenance} \tag{4}$$

$$B = B_{risk_{reducation}} + B_{incident_{mitigation}} \tag{5}$$

where, $C_{implementation}$ →*The cost of implementing security measures* (hardware, software, costs), $C_{maintenance}$ →*The Ongoing Maintenance Cost* (updates, monitoring, training), $B_{risk_{reducation}}$ →*Benefit from reduced risk* (the reduction in the risk RRR), $B_{incident_{mitigation}}$ →*Benefit from an improved incident response* (reduced impact of security incidents)

The **Net Benefit (NB)** can be computed in Eq. (6).

$$NB = B - C \tag{6}$$

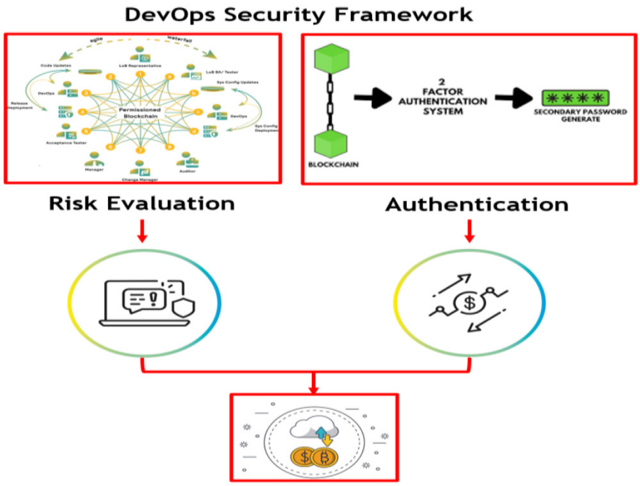

Figure 1

Proposed DevOps-RAS Model

The goal is to achieve the maximum cost benefit, increasing the use of the preferred authentication system while introducing security measures. Therefore, the specific optimization problem is Eq. (7).

$$Maximize\, NB = (B_{riskreduction} + B_{incidentmitigation}) - (C_{implimentation} + C_{maintenance})) \tag{7}$$

- *Authentication Efficiency* $E \geq E_{min}$ *(Emin shows the minimal acceptable efficiency)*
- *Detection Performance* $P \geq P_{min}$ *(Pmin specifies the minimal acceptable performance)*

The overall summary in Fig. 1 of the DevOps-RAS for enhancing security within DevOps encompasses several key features. Security evaluation identifies weaknesses in the system by computing the risk in terms of the severity of the security attack, susceptibilities, and consequences. The effectiveness of an authentication system is assessed by evaluating the efficiency of user authentication methods using FAR and FRR. And tries to find the best compromise between security and accessibility. AD mechanisms focus on the system's results of attack detection with parameters that would have been perceived as attacks in the actual environment, as well as the number of false alarms. The cost-benefit analysis provides a comprehensive assessment of the costs

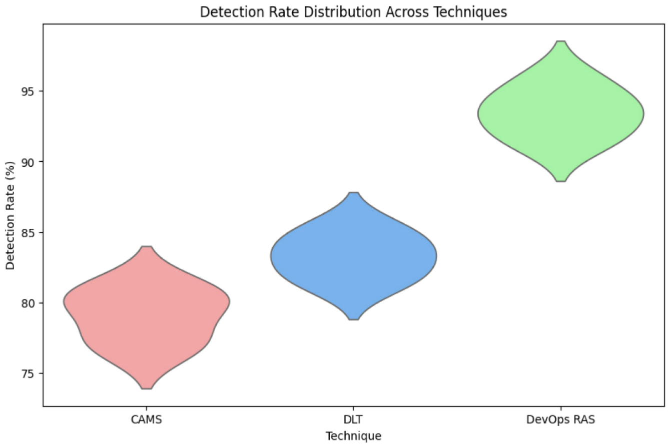

Figure 2

Comparison of DR

associated with implementing and maintaining security measures, as well as the benefits derived from risk mitigation and enhanced incident management. The optimization problem that attentions on maximizing the net benefit from security measures has constraints that ensure authentication efficiency and attack detection performance are not less than the predefined level.

3. Result and Discussion

In the simulation of DevOps and security systems, powerful servers with multi-core processors and enough RAM should perform complex computations. The software setup includes virtualization tools, such as Virtual Machine (VMware), which creates an isolated environment, and Continuous Integration and Continuous Delivery/Deployment (CI/CD) tools like Jenkins, used for automation, as well as monitoring tools like Prometheus, which track real-time performance. Security tools, such as Security Information and Event Management (SIEM) and AD, are also integrated to assess and improve CPS security. The DR and FPR measure the efficiency of AD's performance. The effectiveness of the DevOps-RAS is compared with existing methods, namely CAMS [10] and DLT [12]. To assess the functionality of security models, several parameters are used to measure the level of attack found and the level of access provided. DR determines the degree to which the system successfully finds true attacks and indicates the CPS's ability to detect real-time attacks as Eq. (8).

$$DR = \frac{TP}{TP+FN} \tag{8}$$

Where, TP→True Positive, the true attacks that have been detected; FN→False Negative, the true attacks that have been missed (Table 1 and Figure 2)

Table 1

Comparison of DR

Records	CAMS	DLT	Proposed DevOps-RAS
100	76.67	81.21	91.23
200	77.56	82.23	92.34
300	79.78	83.36	93.67
400	80.23	84.24	94.23
500	81.23	85.43	95.94

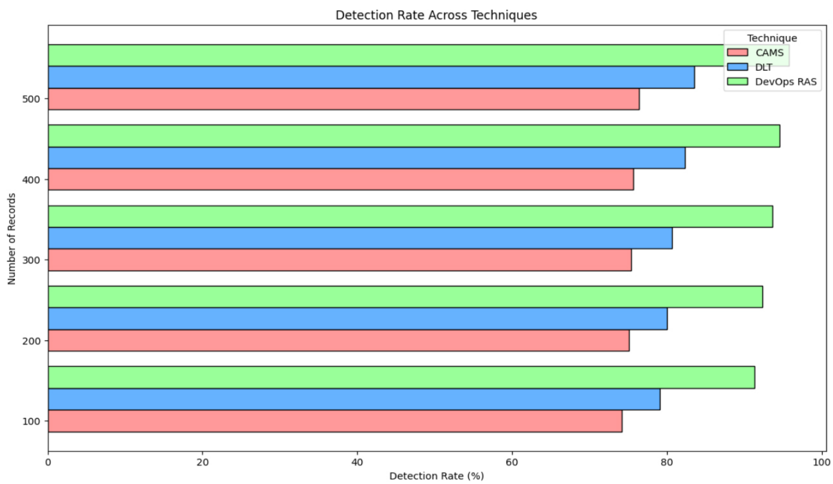

Figure 3

Comparison of FPR

Table 2 and Figure 2 compare DR's other methods: CAMS, DLT, and DevOps-RAS. As shown, a general trend of the DR is rising with the sum of records for all the techniques applied. As for the DR, DevOps-AS generates the highest DR, higher than CAMS and DLT. For example, at 500 records, DevOps-RAS achieves DR of 95.94%, compared to 81.23% for

CAMS and 85.43% for DLT. This trend reveals that the DevOps-RAS is more effective at AD with enhanced efficiency across different dataset dimensions. The results reveal that the DevOps-RAS outperforms the other methods in terms of AD effectiveness. FPR measures the ratio of FP activities, which means the CPS number of alarms increases, Eq. (9).

$$FPR = \frac{FP}{FP+TN} \tag{9}$$

Where, FP→False Positives, benign activities are classified as attacks, TN→True Negatives, the number of benign activities is correctly classified. These metrics help to find how effectively the model can identify real attacks while avoiding false alarms (Tab. 2 and Fig. 3). Fig. 3 and Tab. 2 show the FPR achieved by CAMS, DLT, and DevOps-RAS as the record size is varied. From the FPR, it was evident that the FPR of all methods increases with the number of records, which represents an increasing the FPR. DevOps-RAS proves the highest FPR, reaching 95.78% at 500 records, significantly higher than CAMS at 76.45% and DLT at 83.56%. This implies that, although DevOps-RAS is highly efficient in AD, it is also likely to label harmless activities as attacks more frequently. The data indicate a compromise between AD accuracy and FPR among the compared methods.

Table 2

Comparison of FPR

Records/Techniques	CAMS	DLT	DevOps RAS
100	74.23	79.09	91.32
200	75.12	79.99	92.34
300	75.43	80.67	93.67
400	75.67	82.32	94.55
500	76.45	83.56	95.78

Conclusion and Future Work

The CPS-based DevOps-RAS proves improved AD ability with the best DR while simultaneously achieving the highest FPR. This model indicates a direct relationship between TP and FP results. Therefore, the results of DR and FPR for CAMS, DLT, and DevOps-RAS reveal differences in the performance of these tools. The FPR of CAMS and DLT is lower, but the DR is also lower, indicating the pros and cons of CAMS and DLT. For future improvements, it is recommended that Machine Learning (ML) and more sophisticated AD be incorporated to fine-tune the DR and FPR ratio. Moreover, research on adaptive thresholds and security that adapts to the context of the implementation environment may also be beneficial in increasing performance, thereby minimizing FP while maximizing TP and TN. Further work is required to refine and optimize these methods, ensuring that the security solutions evolve in response to emerging attacks and do not adversely impact normal users.

References

[1] S. Bankar and D. Shah, "Decentralized Framework to Strengthen DevOps Using Blockchain," *In Computational Intelligence: Select Proceedings of InCITe 2022*, Singapore: Springer Nature Singapore, p. 517-525, (2023).

[2] R. Nasr, M. I. Marie and A. El Sayed, "A Hybrid Framework to Implement DevOps Practices on Blockchain Applications (DevChainOps)", *International Journal of Advanced Computer Science & Applications*, vol. *15, no.* 6, (2024)

[3] V. J. Tharini, "Cross-Entropy Assisted Optimization Technique for High Utility Itemset Mining from the Transactional Database", *Communications on Applied Nonlinear Analysis*, vol. *31, no.* 3s, p. 90-104, (2024).

[4] M. S. Farooq and U. Ali, "Harnessing the potential of blockchain in DevOps: a framework for distributed integration and development", arXiv preprint arXiv:2306.00462, (2023).

[5] G. Sriraman and R. Shriram, "Slide-block: End-to-end amplified security to improve DevOps resilience through pattern-based authentication", *Heliyon*, vol. *10,* no. 4, (2024)

[6] M. Zohaib, A. Alsanad and A. A. Alhogail, "Prioritizing DevOps Implementation Guidelines for Sustainable Software Projects", *IEEE Access*, vol. 12, no. 71109-71130, (2024).

[7] P. Jahanbin, R. S. Sharma, S. T. Wingreen, N. Kshetri and K. K. R. Choo, "Towards CRISP-BC: 3TIC specification framework for Blockchain use-cases", *IET Blockchain*, vol. 3, no. 3, p. 159-168 (2023).

[8] I. Aviv, A. Barger, A. Kofman and R. Weisfeld, Reference Architecture for Blockchain-Native Distributed Information Syste", *IEEE Access*, vol. 11, p. 4838-4851, (2023).

[9] M. A. Ghanimi, Hayder, P. Melgarejo-Bolivar, P. Romel et al., "Merkle-Damg; Rd hash functions and blockchains: Securing electronic health records," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, p. 237–248, (2024).

[10] M. A. Ghanimi, Hayder, T. Gopalakrishnan, G. Deol Joel Sunny, K. Amarendra, P. Dadheech and S. Sudhakar, "Chebyshev polynomial approximation in CNN for zero-knowledge encrypted data analysis," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, p. 203–214, (2024).

[11] P. Vidya Sagar, M. A. Ghanimi, Hayder, L. Prabhu Arokia Jesu Raja, D. Pankaj and & S. Sudhakar, "Secure multi-party computation in deep learning: Enhancing privacy in distributed neural networks," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, p. 249–259, (2024).

[12] R. Ganga Rama Koteswara, M. A. Ghanimi, Hayder, V. Ramachandran, D. Al-Qahtani, D. Pankaj and S. Sudhakar, "Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, p. 361–370, (2024).

[13] K. Raguru Jaya, T. Gopalakrishnan, M. Divyapushpalakshmi, K. Amarendra, D. Pankaj and S. Sudhakar, "Security and privacy concerns in social networks mathematically modified metaheuristic-based approach," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, p. 371–382, (2024).

Received November, 2024