Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1755–1763
DOI : 10.47974/JIOS-2266

Enhancing network security in corporate environments through continuous monitoring and intelligent data analysis

Subramanian Karthick [‡]
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Anjali Bhardwaj [†]
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Sagarkumar S. Badhiye [§]
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University)
Nagpur 440008
Maharashtra
India

Shubhangi S. Shambharkar *
Department of Computer Technology
Yeshwantrao Chavan College of Engineering
Nagpur 441110
Maharashtra
India

[‡] *E-mail:* karthick.sb@vit.edu
[†] *E-mail:* anjali.bhardwaj@niu.edu.in
[§] *E-mail:* sagarbadhiye@gmail.com
* *E-mail:* shubhangisshambharkar@gmail.com (Corresponding Author)

Jambi Ratna Raja Kumar [@]
Department of Computer Engineering
Genba Sopanrao Moze College of Engineering
Balewadi
Pune 411045
Maharashtra
India

Abstract

To make business networks safer, we need more advanced tools to deal with cyber risks that are getting smarter all the time. The proactive defense work provide the smart data analysis that monitors and find the outlier in network, reduces the response time and secure the important data and information. We have used AI based approach for that help, businesses can find trends, lower risks, and improve how they handle incidents with little help from humans. This framework able to track and find to real-time tracking that improve the security, make it flexible and scalable. This proposed approach not only makes business IT systems stronger against new threats, but it also makes digital environments more trustworthy, dependable, and able to follow rules.

Subject Classification: *54H30, 57Z25.*

Keywords: *Network security, Continuous monitoring, Intelligent data analysis, Machine learning, Corporate IT, Anomaly detection, Real-time monitoring.*

1. Introduction

In today's digital world, cyber risks that take advantage of weak spots in network systems are becoming a bigger problem for businesses. Traditional security measures work well in steady situations, but they are often not enough to stop threats that change and adapt [1, 2]. In It sector different feature like cloud integration, RDC, portable device has more complied structure to integrate. Because of this, security tactics must change from being reactive to being proactive [3]. Smart data analysis, it goes beyond signature-based identification. It uses machine learning and AI to find small oddities and new danger trends [4, 5]. This combination makes predictive defence and flexible risk management stronger [6]. Companies can improve their stability, business consistency, and compliance with regulations by building these solutions into their company IT systems [7]. Intelligent tracking also cuts down on mistakes made by people and the stress that comes from using too many resources [8, 9]. This lets IT teams focus on strategic defence projects. In the end, this method makes sure that business networks stay safe, can grow, and are ready for new hacking threats.

[@] *E-mail:* `ratnaraj.jambi@gmail.com`

2. Machine learning/AI algorithms for anomaly and threat detection

AI and machine learning can find hidden problems, sort out strange trends, guess when attacks will happen, and improve network security by learning from new threats to the company [10]. Figure 1 shows a multicolor framework illustrating anomaly detection process.

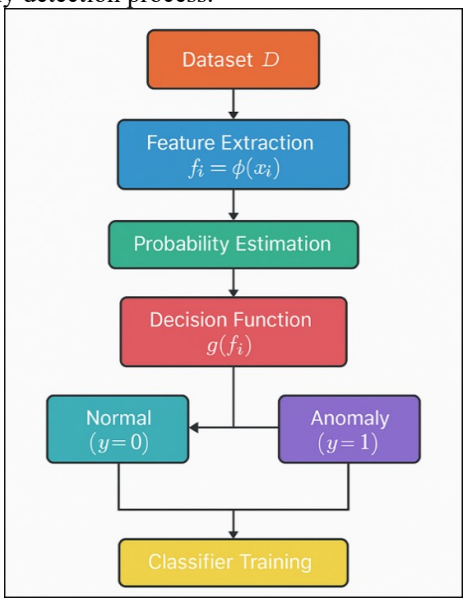

Figure 1

Multicolor Framework of Machine Learning and AI Algorithms for Anomaly and Threat Detection

Dataset:

$$D = \{x1, x2, \ldots, xn\}$$

Feature vector:

$$fi = \varphi(xi), fi \in R^m$$

Probability of normal:

$$P(y = 0|fi)$$

Probability of anomaly:

$$P(y = 1|fi) = 1 - P(y = 0|fi) \quad (1)$$

Decision function:

$$g(fi) = 0 \; if \; P(y = 0|fi) \geq \theta, else \; 1 \quad (2)$$

Distance metric:

$$d(fi,\mu) = \left|\left|fi - \mu\right|\right|2 \tag{3}$$

Threshold:

$$d(fi,\mu) > \delta \rightarrow anomaly$$

Classifier:

$$\hat{y}i = h(fi; W, b) \tag{4}$$

Loss function:

$$L = -\Sigma\,[\,yi\log(\hat{y}i) + (1 - yi)\log(1 - \hat{y}i)] \tag{5}$$

Gradient update:

$$W(t+1) = Wt - \eta\,\nabla W\,L \tag{6}$$

Recall:

$$R = \frac{TP}{(TP + FN)} \tag{7}$$

Precision:

$$P = \frac{TP}{(TP + FP)} \tag{8}$$

F1-score:

$$F1 = \frac{2PR}{(P + R)} \tag{9}$$

Optimization: maximize F1 subject to δ, θ

Final model:

$$M* = argmaxM\ F1(M) \tag{10}$$

3. System integration and architecture for real-time monitoring

Integrated design combines sensors, data streams, analytics engines, and screens so that business networks can be monitored in real time, for irregularities to be found, incidents to be reported, and security measures to be taken before they happen [11, 12].

Traffic stream:

$$S = \{p1, p2, \ldots, pt\}$$

Packet features:

$$zj \in R^m$$

Flow aggregation:

$$F = \left(\frac{1}{t}\right) \Sigma\, zj \tag{11}$$

Monitoring function:

$$M(F) = \alpha \cdot Anomaly(F) + \beta \cdot Normal(F) \tag{12}$$

Sliding window:

$$Wk = \{Fk - n + 1, \ldots, Fk\} \tag{13}$$

Alert function:

$$Ak = 1\ if\ Pk > \gamma, else\ 0$$

Latency:

$$L = Tdetect - Tevent \tag{14}$$

Throughput:

$$Th = \frac{PacketsProcessed}{Time} \tag{15}$$

Reliability:

$$R = \frac{CorrectAlerts}{TotalAnomalies} \tag{16}$$

Pipeline as DAG:

$$P = (V, E)$$

Efficiency:

$$Eff = \frac{R}{(L \cdot Th)} \tag{17}$$

Objective: minimize L, maximize R, maximize Eff

Final architecture:

$$A* = argmaxA\ Eff(A) \tag{18}$$

4. Deployment in corporate IT infrastructures

When tracking systems are deployed, they are easily integrated into corporate IT. This makes sure that there is minimal impact, centralised control, increased robustness, and compliance with the organization's security policies [13, 14].

Step 1: Definition (Deployment Matrix)

Network nodes: N = {n1, n2, ..., nm}

Security agents: A = {a1, a2, ..., ak}

Deployment matrix:

Dij = 1 if agent ai is deployed at node nj
Dij = 0 otherwise

Step 2: Resource Cost Function

$$Cij = cpuij + memij \tag{19}$$

Step 3: Total Cost

$$Ctotal = \Sigma\,\Sigma\, Dij * Cij \tag{20}$$

Step 4: Coverage Metric

$$Cov = \left(\frac{1}{|N|}\right)\Sigma\, 1(\exists i : Dij = 1) \tag{21}$$

Step 5: Security Impact Score

$$SI = \Sigma\,\Sigma\, Dij * wij$$

where wij = importance weight of node nj

Step 6: Reliability Formula

$$R = 1 - \left(\frac{DT}{Toperational}\right) \tag{22}$$

Step 7: Compliance Constraint

Comp = 1 if SI ≥ τ
Comp = 0 otherwise

Step 8: Deployment Efficiency

$$Eff = \frac{(Cov + R)}{Ctotal} \tag{23}$$

Step 9: Optimization Problem

$$Maximize\ (Cov + SI)$$

Subject to: Ctotal ≤ Cbudget

Step 10: Theorem (Optimal Deployment Existence)

For finite sets of nodes N and agents A, there exists an optimal deployment matrix D* that maximizes efficiency Eff.

Step 11: Proof (Sketch)

Therefore, ∃ D* such that:

$$Eff(D*) \geq Eff(D) for\ all\ D. \tag{24}$$

Step 12: Final Deployment Formula

$$D* = argmaxD\ Eff(D) \tag{25}$$

5. Result and Discussion

Comparing different models for finding anomalies shows that mixed deep learning methods are better. Random Forest and baseline SVM were about average in terms of accuracy, but they had higher rates of false positives.

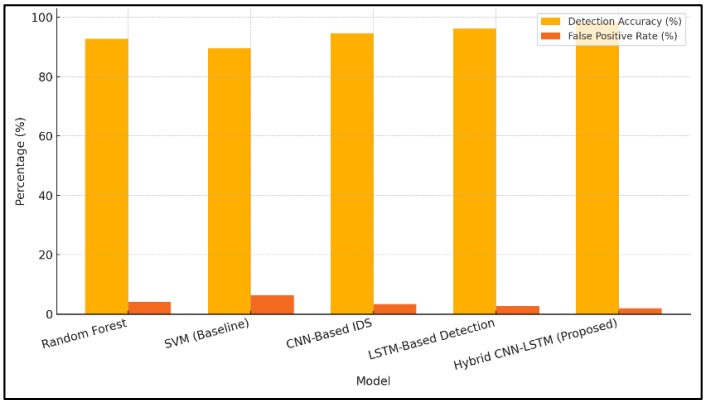

Figure 2
Performance Comparison of Machine Learning Models for Intrusion Detection

CNN-based IDS made recognition more accurate and reliable, and LSTM models made performance even better by learning from past events. Figure 2 illustrates performance comparison of machine learning models for intrusion detection, highlighting accuracy, precision, recall, and F1-score across approaches. The suggested Hybrid CNN-LSTM worked the best, with a 97.7% F1-score, 98.1% accuracy, and only 1.9% false positives. This shows that it is reliable, scalable, and effective at dealing with complicated online dangers to businesses.

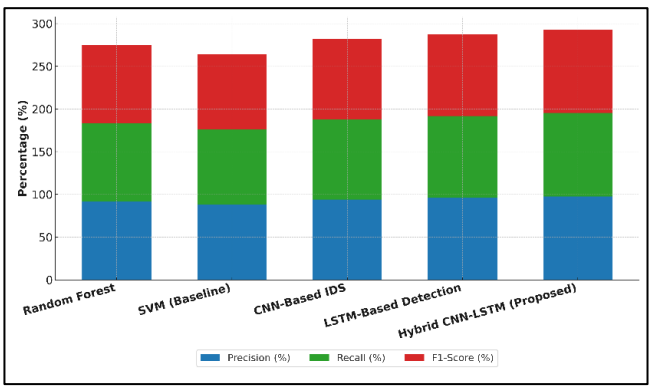

Figure 3
Model-Wise Comparison of Precision, Recall, and F1-Score in Intrusion Detection Systems

Figure 3 shows a model-by-model comparison of F1-score, accuracy, and recall in intrusion detection systems. It focusses on the pros, cons, and trade-offs of various machine learning methods.

6. Conclusion

Improving the security of a company's network by constantly watching it and analyzing it intelligently sets up a defence against new cyber dangers. Organizations can quickly find problems, shorten reaction times, and lower business risks by using machine learning techniques and real-time tracking systems. Adding these solutions to IT systems makes them more reliable, makes sure they follow the rules, and increases trust among stakeholders. Ultimately, these smart, flexible methods create scalable, future-proof security frameworks that protect important assets and make business digital ecosystems stronger as a whole.

References

[1] S. Ahmad and A. H. Mir, "SDN interfaces: Protocols, taxonomy and challenges," *Int. J. Wirel. Microw. Technol.*, vol. 12, pp. 11–32 (2022).

[2] S. Anjum, A. Ahmed, R. Kurup, S. Kidiya, and S. Kureshi, "Blockchain based image steganography," *Int. J. Adv. Comput. Theory Eng.,* vol. 14, no. 1, pp. 147–152 (May 2025).

[3] S. Bao, Y. Liang, and H. Xu, "Blockchain for network slicing in 5G and beyond: Survey and challenges," *J. Commun. Inf. Netw.,* vol. 7, pp. 349–359 (2022).

[4] M. Chen, J. Yang, Y. Hao, S. Mao, and K. Hwang, "A 5G cognitive system for healthcare," *Big Data Cogn. Comput.,* vol. 1, pp. 2 (2017).

[5] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of Industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.,* vol. 114, Art. no. 103165 (2020).

[6] T. Cucinotta, L. Abeni, M. Marinoni, R. Mancini, and C. Vitucci, "Strong temporal isolation among containers in OpenStack for NFV services," *IEEE Trans. Cloud Comput.,* vol. 11, pp. 763–778 (2023).

[7] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M. K. Mishra, and P. Lalwani, "ML-based 5G network slicing security: A comprehensive survey," *Future Internet,* vol. 14, Art. no. 116 (2022).

[8] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu, and M. Liyanage, "A survey on network slicing security: Attacks, challenges, solutions

and research directions," *IEEE Commun. Surv. Tutor*., vol. 26, pp. 534–570 (2024).

[9] D. Goyal, A. Kumar, Y. Gandhi, and V. Khetani, "Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 2-B, pp. 703–714 (2024).

[10] M. G. Dhote, B. M. Nanche, P. N. Mahalle, S. S. Ali, M. Gulhane, and V. S. Karwande, "Deep learning for optimized path planning in autonomous vehicles by integrating reinforcement learning with convolutional neural networks," *J. Inf. Optim. Sci*., vol. 46, no. 4-B, pp. 1129–1139 (2025).

[11] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Commun. Surv. Tutor.,* vol. 25, pp. 1376–1411 (2023).

[12] O. Rholam, B. Mohammed, and D. Gretete, "Fractional integral Hermite–Hadamard inequalities type for MT-convex stochastic process," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 3, pp. 685–699 (2025), doi: 10.47974/JDMSC-1842.

[13] W. Wu, C. Zhou, M. Li, H. Wu, H. Zhou, and N. Zhang, "AI-native network slicing for 6G networks," *IEEE Wireless Commun.,* vol. 29, pp. 96–103 (2022).

[14] Y.-J. Wu, W.-S. Hwang, C.-Y. Shen, and Y.-Y. Chen, "Network slicing for mMTC and URLLC using software-defined networking with P4 switches," *Electronics*, vol. 11, Art. no. 2111 (2022).

Received April, 2025