

# Utilizing Machine Learning for Intrusion Detection Systems in the Context of Cloud Computing

Mohammed Akif, Anuj Nakka, Solanki Prakash, Vijay N, Dr Suresh Kallam

Department of CSE  
Jain University, Bangalore, India

**Abstract:** *The rapid advancements in the internet and communication sectors have led to a huge expansion in the network dimension and the related data. The proliferation of new assault kinds as a result makes it challenging for community safety to accurately identify invasions. Furthermore, the presence of intruders who want to launch a lot of attacks against the network cannot be ignored. An intrusion detection device (IDS) is one such instrument that protects against prospective intrusions by monitoring community communication to guarantee its confidentiality, integrity, and availability. IDS continues to struggle with innovative intrusion detection, lowering false alarm rates, and improving detection accuracy despite substantial research backing. An intrusion detection system's main job is to protect resources against threats. It predicts user behaviour based on analysis, and determines whether that behaviour constitutes an assault or is simply normal behaviour. We use Support Vector Machine (SVM) and Rough Set Theory (RST) to detect network breaches (SVM). Computer learning (ML) and Python-based total IDS systems are recently being employed to identify intrusions across the network in an ecologically friendly manner. The taxonomy presented in this article is mostly based on the impressive machine learning and Python approaches used to develop network-based IDS (NIDS) systems. The article begins by defining IDS.*

**Keywords:** Machine learning Techniques, Cloud Computing infrastructure, Node:-Physical virtual device  
Datasets:-Consists of data, Protocol - A standard way of performing a task

## REFERENCES

- [1]. D. Anderson, T.F. Lunt, H. Javitz, A. Tamaru, and A. Valdes (1995) Detecting unusual program behavior using the statistical component of Next-generation Intrusion Detection Expert System (NIDES) SRI International Computer Science Laboratory
- [2]. Christopher Kruegel, Giovanni Vigna (2003) Anomaly detection of web-based attacks, Proceedings of 10th ACM conference on Computer and communication security (Washington D.C., USA), ACM Press pp 251–261
- [3]. HS Teng, K. Chen, SC Lu (1990) Adaptive real-time anomaly detection using inductively generated sequential patterns, Proceedings of Symposium on Research in Security and Privacy (Oakland, CA) pp 278–284
- [4]. Wang, Ke, Gabriela Cretu, Salvatore J. Stolfo (2006) Anomalous payload-based worm detection and signature generation, Recent Advances in Intrusion Detection Springer Berlin Heidelberg Kruegel, Christopher, Thomas Toth (2002) Flexible, mobile agent based intrusion detection for dynamic networks European Wireless
- [5]. Mark Crosbie and Gene Spafford (1995) Active defense of a computer system using autonomous agents, Technical Report 95-008, COAST Group Department of Computer Sciences Purdue University West Lafayette IN 47907-1398
- [6]. Wayne Jansen, Wayne Jansen, Timothy Grance, Rebecca M. Blank ((2011) NIST- Guidelines on Security and Privacy [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/summary> [Accessed in September 2012]
- [7]. Oktaya, U. And Sahingoz (2013) „Attacks types and intrusion detection systems in cloud computing“, Proceedings of 6th International Information Security & Cryptography Conference (ISC) pp 71-76

- [8]. Zarrabi, A. and Zarrabi, A. (2012) Internet intrusion detection system service in a cloud, International Journal of Computer Science Issues Volume 9 pp 694-814
- [9]. PeeyushMathur, Nikhil Nishchal (2010) Cloud Computing: New challenge to the entire computer industry, 1st International Conference on Parallel, Distributed and Grid Computing pp 223-228
- [10]. LoubnaDali,AhmedBentajer,ElmoutaoukkilAbdelmajid, Karim Abouelmehdi, HodaElsayed, EladnaniFatiha, BenihssaneAbderahima (2015) A survey of intrusion detection system ,IEEE 2nd World Symposium on Web Applications and Networking (WSWAN)
- [11]. Ch. Cachin and M. Schunter (2011) A Cloud You Can Trust, IEEE Spectrum 48(12) pp 28-51
- [12]. Jun-jie, W. And Sen (2011) Security issues and countermeasures in cloud computing, IEEE International Conference on Grey Systems and Intelligent Services (GSIS) Nanjing pp 843-846