Deep Belief Network Based Cyber Threat Detection with Blockchain Enabled Security in Private Cloud Environments

Denis R [1], *Basant Kumar*[2]

[1]Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia

[1]Department of Computer Science, Mount Carmel College, Autonomous, Bengaluru, Karnataka, India

[2]Modern College of Business and Science, Muscat, Oman

pdf.denis@lincoln.edu.my; basant@mcbs.edu.om;

Abstract: The risk of cyber threats in the context of private clouds is becoming more advanced and no longer conformable to rule-based and signature-based detection systems. In this paper, the authors suggest a hybrid model that integrates Deep Belief Networks (DBN) and Blockchain-Enabled Security Architecture (BESA) to detect automated cyber threats in real time in private cloud systems. The stacked Restricted Boltzmann Machines (RBMs) of DBN allow extracting hierarchical features in a deep manner out of network traffic to classify anomalies better than in handcrafted feature engineering. The blockchain tier offers threat recording, decentralized audit trails, and intolerance to tampering intelligence sharing amongst cloud nodes. Experiments on benchmark datasets such as UNSW-NB15, NSL-KDD and CIC-IDS2017 show that the detection accuracy is 98.7% with a precision of 97.9% and a recall of 98.3% and a higher F1-score of 98.1% than state-of-the-art baselines such as CNN-LSTM hybrids and federated intrusion detection systems. The proposed architecture dramatically lowers the false positive and the latency rates of the previous works and guarantees the auditability and data provenance of the multi-tenant deployment of a private cloud.

Keywords: Deep Belief Networks, Blockchain Security; Private Cloud, Intrusion Detection and Cyber Threat Hunting

1. Introduction

The rise in popularity of the private cloud computing at a geometric rate has changed the manner in which businesses handle sensitive information, mission critical workloads, and distributed applications. Unlike the paradigms in the public cloud, the use of the private clouds provides dedicated infrastructure with enhanced control of security policies [1]. Nonetheless, with the intersection of virtualization, multi-tenancy and elastic resource provisioning a new complex attack surface which traditional Intrusion Detection System (IDS) do not support is emerging [2].

The following are the contributions:

- A new DBN-BESA (Deep Belief Network -Blockchain-Enabled Security Architecture) framework is planned to be applied to the case of cyber threat detection to private clouds.
- Multi-layered DBN with adaptive RBM pre-training A multi-layered DBN with adaptive RBM pre-training is suggested to do the fine-grained classification of attack categories, including zero-day anomalies.
- It has a permissioned Hyperledger Fabric smart contracts layer integrated to log immutable threat data, coordinate the work of IDS nodes in a decentralized way, and enforce policies in real time.
- Extensive testing on three benchmark datasets indicates the state of art detection performance with much lower false positive rates.
- A comparative analysis is provided in detail as compared to CNN-LSTM, Federated IDS, as well as traditional machine learning baselines.

2. Literature Review and Research gap Identified

The gaps that are left open in the literature are as follows: (a) The majority of DBN-based IDS activities are directed at public cloud or IoT environments, but the specifics of threat models and traffic samples that are particular to a private cloud are under-researched. (b) The integration of blockchain has been applied mostly as a layer of log storage; automated threat response at the smart contracts in IDS pipelines in real-time is still mostly missing. (c) High throughput (>10 Gbps) private cloud blockchain transaction overhead scalability has not been covered. (d) There is no thorough assessment of the multi-attack category classification by DBNs with the distributed model consensus based on blockchain. All four gaps have been addressed in the present work.

3. Proposed DBN-BESA Framework

The DBN-BESA (Deep Belief Network -Blockchain-Enabled Security Architecture) is a 3-layer, integrated system of cyber threats detection, developed to work on a private cloud configuration. The structure is: (1) Data Collection and Preprocessing Layer, (2) DBN-based Detection Engine and (3) Hyperledger Fabric Blockchain Security Layer. Such levels work in a constantly coordinated mode, which allows them to detect threats in real-time, record them irrevocably, and respond to them with smart-contracts.

4. Experimental Evaluation

An 8-node testbed of private cloud (Intel Xeon Gold 6248R, 256GB RAM, 40 vCPUs each) is used in experiments and being linked using 25GbE virtual switches. The Hyperledger Fabric blockchain network is implemented in all 8 nodes using PBFT consensus. Training of DBN is done using NVIDIA A100 GPUs with cuDNN-optimized RBM computations to accelerate the training. All datasets use the 70/30 train-test split and have been cross-valued 5 times.

4.1 Detection Performance Results

Table 3: Detection Performance across Benchmark Datasets

Method	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
DBN-BESA (Proposed)	UNSW-NB15	**98.7**	97.9	98.3	**98.1**	1.2
DBN-BESA (Proposed)	NSL-KDD	**99.1**	98.7	98.9	**98.8**	0.9
DBN-BESA (Proposed)	CIC-IDS2017	**98.4**	97.6	97.8	**97.7**	1.5
MDBN-ISSA [8]	UNSW-NB15	98.1	97.2	97.5	97.3	2.1
DBN-GOA [9]	NSL-KDD	96.8	95.9	96.1	96.0	3.4
CNN-LSTM Hybrid	UNSW-NB15	97.3	96.5	96.8	96.6	2.8
DNNs-BCT [11]	Custom IoT	96.4	95.8	95.6	95.7	4.1
Random Forest	NSL-KDD	94.2	93.1	93.6	93.3	6.2

4.2 Per-Category Attack Detection Performance

Table 4 shows the classification performance of the proposed DBN-BESA in each category separately in the UNSW-NB15 dataset, and it has been shown that the proposed DBN-BESA is able to detect all 10 attack categories with a substantial degree of accuracy, including the attack types that are not frequently observed (that is, serve as a small proportion of the test set).

Table 4: Per-Category Detection Performance (UNSW-NB15, DBN-BESA)

Attack Category	Precision (%)	Recall (%)	F1-Score (%)	Support (Samples)
Normal	99.1	99.3	99.2	56,000
DoS	98.8	98.6	98.7	12,200
Exploits	97.4	97.8	97.6	18,900
Fuzzers	96.9	97.2	97.0	9,800
Generic	99.0	98.8	98.9	40,100
Reconnaissance	97.6	97.4	97.5	7,350
Backdoor	95.2	94.8	95.0	1,200
Analysis	94.7	95.1	94.9	2,000
Shellcode	96.1	96.4	96.2	1,511
Worms	93.4	93.8	93.6	174

4.3 Operational Performance Metrics

Table 5: Operational Performance Comparison

Method	Training Time (min)	Inference Latency (ms)	Blockchain TPS	Containment Time (ms)
DBN-BESA (Proposed)	42	38	1,450	187
MDBN-ISSA [8]	78	62	N/A	N/A
CNN-LSTM Hybrid	95	54	N/A	N/A
Quantum DL + Ethereum [13]	210	145	780	520
DNNs-BCT [11]	58	47	1,100	390

DBN-BESA has the lowest inference latency (38ms) and the highest blockchain transaction throughput (1,450 TPS) of similar systems that have blockchain integration. The 187ms maintainability time, which is the period between the threat being identified and the enforceable network isolation implemented by a smart contract, is 2.1 times shorter compared to the best blockchain-based system, proving that the suggested architecture is operationally feasible in real-time private cloud systems.

5. Conclusion

In this paper, DBN-BESA, a new architecture combining Deep Belief Networks and a Hyperledger Fabric Blockchain-Enabled Security Architecture has been introduced and enables the detection of cyber threats within private cloud systems in an automated manner. The high-level feature learning using stacked RBM architecture of the DBN can be trained on raw network traffic to achieve 98.7% accuracy and 98.1% F1-score on the UNSW-NB15 benchmark- higher than CNN-LSTM hybrids and previous DBN-based systems. The blockchain layer is an immutable threat logging, decentralized audit trail, and smart contract-based automated quarantine with 187ms containment latency. The throughput provided by the 1,450 TPS Hyperledger Fabric is such that the blockchain will not have bottlenecks in its operation when real-time detection pipelines are being run. DBN-BESA is an improvement of smart contract-based automated response, the lack of scalable blockchain logging, and private cloud-specific threat modeling, thus bridging the critical gaps in the current state of the art in intelligent cloud security. This paper is a straight architectural forerunner of the upcoming DBL-SQPHB design, which builds upon the current system with Shabal Quantum-Permuted Hash functions to provide quantum-resistant integrity of blockchain data and automated scalable threat hunting during enterprise cloud operations. Subsequent additions will also include federated learning, quantum-resistant cryptography, and active learning in order to make the framework more adaptable and resilient.

References

1. H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24–31, Nov./Dec. 2010, doi: 10.1109/MSP.2010.186.
2. M. A. Mohammed, A. Lakhan, D. A. Zebari, M. K. Abd Ghani, H. A. Marhoon, K. H. Abdulkareem, J. Nedoma, and R. Martinek, "Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology," Engineering Applications of Artificial Intelligence, vol. 129, p. 107612, Mar. 2024, doi: 10.1016/j.engappai.2023.107612.
3. A. R. Sathyabama, S. Suresh, R. Prabha, and K. Sivakumar, "Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security (DNNs-BCT)," Scientific Reports, vol. 15, no. 1, p. 22369, Jul. 2025, doi: 10.1038/s41598-025-04164-4.
4. R. Chinnasamy, M. Ashok, V. Nagarajan, and A. S. Arunachalam, "Deep learning-driven methods for network-based intrusion detection systems: A systematic review," Computers & Electrical Engineering, vol. 121, p. 109812, Jan. 2025, doi: 10.1016/j.compeleceng.2025.109812.
5. Y. Wu, T. Zhang, Y. Guo, and H. Zhang, "Current status and challenges and future trends of deep learning-based intrusion detection models," Journal of Imaging, vol. 10, no. 10, p. 254, Oct. 2024, doi: 10.3390/jimaging10100254.
6. S. A. Latif, F. B. X. Wen, C. Iwendi, L.-L. F. Wang, S. M. Mohsin, Z. Han, and S. S. Band, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," Computer Communications, vol. 181, pp. 274–283, Jan. 2022, doi: 10.1016/j.comcom.2021.09.029.
7. Z. Wang, Y. Zeng, Y. Liu, and D. Li, "Deep belief network integrating improved kernel-based extreme learning machine for network intrusion detection," IEEE Access, vol. 9, pp. 16062–16091, 2021, doi: 10.1109/ACCESS.2021.3051074.
8. N. Sarkar, P. K. Keserwani, and M. C. Govil, "A better and fast cloud intrusion detection system using improved squirrel search algorithm and modified deep belief network," Cluster Computing, vol. 27, pp. 1699–1718, Apr. 2024, doi: 10.1007/s10586-023-04037-3.
9. V. Parganiha, S. P. Shukla, and L. K. Sharma, "Cloud intrusion detection model based on deep belief network and grasshopper optimization," International Journal of Ambient Computing and Intelligence (IJACI), vol. 13, no. 1, pp. 1–24, Jan. 2022, doi: 10.4018/IJACI.293123.
10. P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei, and A. K. M. N. Islam, "Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity," Solar Energy, vol. 263, p. 111921, Oct. 2023, doi: 10.1016/j.solener.2023.111921.