A Survey of Intrusion Detection Techniques

Deepthi Hassan Lakshminarayana
Department of Computer Science
East Carolina University
Greenville NC, USA
lakshminarayanad17@students.ecu.edu

James Philips
Department of Computer Science
East Carolina University
Greenville NC, USA
philipsj16@students.ecu.edu

Nasseh Tabrizi
Department of Computer Science
East Carolina University
Greenville NC, USA
tabrizim@ecu.edu

***Abstract*—With the growing rate of cyber attacks, there is a significant need for intrusion detection systems (IDS) in networked environments. As intrusion tactics become more sophisticated and more challenging to detect, this necessitates improved intrusion detection technology to retain user trust and preserve network security. Over the last decade, several detection methodologies have been designed to provide users with reliability, privacy, and information security. This paper reviews three intrusion detection techniques: blockchain technologies, machine learning, and deep learning.**

This survey overviews various machine learning and deep learning algorithms, summarizes blockchain technology, and discusses different blockchain methods used for intrusion detection and cybersecurity. We provide insight into their applications, drawbacks, and challenges.

***Index Terms*—Intrusion detection, cyber-security, collaborative system, blockchain, machine learning, deep learning, decentralized network, algorithm, smart contracts, security.**

I. INTRODUCTION

In this era of the Internet and digital medium, cyber threats are exponentially increasing in number. Intrusions are detected using various intrusion detection systems (IDSs), which are implemented in many networks (e.g., in banking and educational organizations). IDS consists of a software application to monitor and detect malicious activities within a network environment.

Even with advances in technology, cyber-attacks persist and require continual vigilance through the enhancement of existing IDS techniques and introduction of new approaches. A number of techniques are employed to prevent attacks and provide users with a secure network. This paper reviews three techniques used for intrusion detection, namely machine learning, deep learning, and emergent blockchain technologies [1]. Some of the other techniques for intrusion detection are statistical methods, data mining methods [2], and genetic algorithms [3].

Machine Learning is one of the most popular approaches in intrusion detection. Anomalies in the network can be detected through running various machine learning algorithms such as K-Nearest Neighbor (KNN), Support Vector Machine (SVM), etc. [4].

Another approach used to enhance the capabilities of IDS is deep learning techniques [5]. It is proven that deep learning based methods addresses the challenges of IDS efficiently [6].

First implemented in 2009, blockchain is the innovation behind cryptocurrencies like Bitcoin. In a blockchain, all the transactions are stored in blocks [7]. This paper provides an overview of blockchain technology, including its architecture and cybersecurity applications.

This review paper is organized as follows:

- Background
- Evolution of Blockchain
- Research Methodology
- Literature Review
- Conclusion

This survey reviews 57 related studies focusing on the intrusion detection techniques published from the period 1999-2018.

This literature survey provides background, drawbacks, and applications for each technique in intrusion detection research. It likewise discusses different software methodologies and architectures built using blockchain technology for intrusion detection and cybersecurity applications.

This paper also surveys various machine learning and deep learning algorithms used to improve intrusion detection in networks. Finally, this survey endeavors to answer the following research questions:

- What are the different machine learning and deep learning techniques employed to detect threats in the network?
- What are the current applications of blockchain technology to cybersecurity generally and intrusion detection specifically?

II. BACKGROUND

A. Intrusion Detection Systems

This section provides background on key domain knowledge for Intrusion Detection Systems. Intrusion Detection is a way of monitoring the events happening within a network or on local computer to detect any abnormal or malicious behavior which breaches the security or standard policies. Intrusion Detection Systems (IDS) are classified into host-based IDS, network-based (NIDS), and hybrid IDS (HIDS). HIDS monitors an individual computer system, looking for malicious activities, and NIDS examines the network traffic for suspicious payloads. [8]. Fig.1 shows how intrusion detection systems are installed in common network topologies;

978-1-7281-4550-1/19/$31.00 ©2019 IEEE
DOI 10.1109/ICMLA.2019.00187

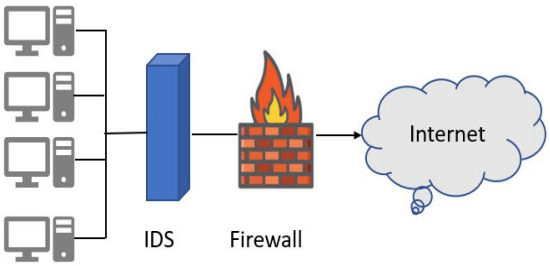

Fig. 1. Intrusion detector in a network

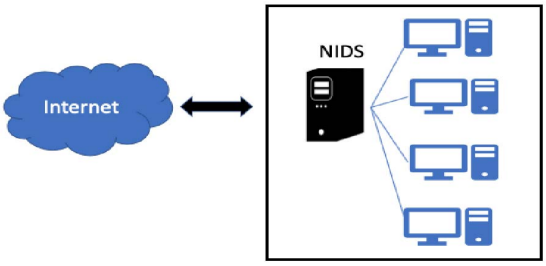

Fig. 2. Deployment of NIDS within a network adapted from [9]

they provide a security layer between network hosts and external networks and monitor for any malicious activity. The remainder of this section discusses the classification of IDS by type along with each type's features and challenges.

a) HIDS and NIDS: Intrusion Detection Systems can be categorized by detection method and deployment type. Based on detection methods, IDS are subdivided into signature-based and anomaly-based categories [9]. For deployment, IDS are mainly categorized into HIDS, NIDS, and Hybrid IDS, which is the integration of HIDS and NIDS to provide additional defense [3].
Fig.2 shows the deployment of a NIDS in a network. Additionally, an IDS can be classified based on detection methods into signature-based, anomaly-based, and specification-based [9]. In the signature-based detection method, a stored signature is compared with network traffic in the system in order to detect attacks. In the anomaly-based detection method, any signs of malicious or abnormal activity are detected, and an alarm is generated for such events. Specification-based detection method identifies any changes in a normal profile and watched events and notifies regarding the change.

b) Collaborative Intrusion Detection System: Collaborative Intrusion Detection Systems increase the detection performance of a single IDS, which can be easily overwhelmed and circumvented in any complex attack like a denial-of-service (DoS) attack. If the attack is not detected promptly, it will cause significant damage to the network and its users. This disastrous occurrence is overcome by collaborative intrusion detection systems (CIDS) [9]. CIDS increase the detection abilities of a single IDS. Each IDS communicates with its peers to collaborate on data sharing and provide trust management [10]. CIDS can be categorized into the following types with examples from the literature:

- Hierarchical Collaboration System like Distributed intrusion detection system (DIDS) [11].
- Subscribe Collaboration System like (Distributed Overlay for Monitoring Internet Outbreaks) DOMINO [12].
- Peer-to-peer query based collaboration system like an Internet-Scale Query Processor (PIER) [13].

Each of these techniques aims to detect any abnormal activity within the network.

c) Challenges: IDS solutions confront many challenges such as security and trust; some of these are listed below:

- Wireless Adhoc networks are dynamic, and hence, it's difficult to depend on a centralized server for analysis and correlation tasks [14].
- Physical security of mobile hosts poses a challenge because a trusted mobile device could be used to infiltrate the network and would not necessarily be detected by an IDS.

B. Blockchain Technology

A blockchain is a chain of blocks where each block holds the record of transactions. The blockhead contains the metadata, and the block body does the recording of transactions [15]. In contrast to physical currency, advanced money and digital forms of payment are accompanied by an undeniable issue called double-spending. This is one of the significant challenges addressed by blockchain technology.

The fundamental utility provided by a blockchain is a sequentially secure method for accessing a block and data records. Ordinarily shared and synchronized over a distributed system, blockchains are accordingly regularly utilized as a public ledger of transactions. Furthermore, each member in the blockchain system can see the record information, dismiss or check it, depending on the protocol. Once acknowledged, transaction records are annexed to the blockchain in a sequential request of their check [9].

a) Blockchain Architecture: A blockchain is an arranged chain of blocks. Blocks hold related data and the information for transactions. The structure of a blockchain consists of three main parts;

- A hash value: This provides the information for the previous block.
- Hash function and a timestamp: The hash function stores the blockchain data, and the timestamp holds the time when the blocks are created [16].
- A Merkel root: This condenses all transactions in the block in order to check the presence and integrity of the transaction information rapidly.
- Block body: The block body stores every single reviewed transaction during the generation of the block. These

individual blocks are linked with hash values to create a blockchain [15].

C. Machine Learning

Machine learning algorithms are extensively used in cyber-security to detect anomalies in networks, and they have been proven to provide high detection rates [17]. In a process called supervised learning [18], these algorithms are applied to the training data to build the prediction model [19]. This prediction model is then used to evaluate given data for any malicious activities [20].

Supervised machine learning methods include support vector machine (SVM), naive Bayes classifier, decision table, and decision tree [21]. Supervised learning algorithms require the data to be class labeled, whereas the unsupervised learning algorithm does not require class labeled data [22]. Unsupervised algorithms include clustering, k-means, deep neural network etc [23]. Semi-supervised algorithms lie between the above mentioned two algorithms they do not require all data to be class labelled [24]. Graph-based, self training, and generative models are some of these examples of semi-supervised machine learning algorithms [25]. Fig.3 shows the classification of machine learning techniques [26].

D. Deep Learning

Deep Learning originated from the Neural Network (NN) algorithm [26]. Different techniques are employed to tackle the drawback of one hidden layer in NN [27].

Deep learning has an immense number of techniques and learning strategies. The authors [28] [29] subdivide deep learning into three categories: generative, discriminative, and hybrid [26] [30].

Machine Learning Methods			
	Supervised Learning	Unsupervised Learning	Semi-supervised Learning
Definition	Requires labelled dataset with pre-defined classes	Requires labelled dataset with out pre-defined classes	Lie in between they do not require all data to be class labelled
Method	Classification	Clustering	Graph Models
Example	SVM, Naive bayes classifier, descision table & trees	k-means,deep nueral network	Graph based,self training.

Deep Learning Methods			
	Generative (Unsupervised learning)	Discriminative (Supervised learning)	Hybrid
Definition	Also named generative architectures uses unlabeled data.	Helps to distinguish the data parts for pattern classification	Combines both generative & discriminative architectures
Aim	Pattern recognition in supervised learning	Mostly used for image recognition	To distinguish data as a discriminative approach
Example	Auto Encoder, SPN, RNN, Boltzmann Machine (BM)	Convolutional Neural Network (CNN)	Deep Neural Network

Fig. 3. Classification of machine and deep learning methods

III. Evolution of Blockchain

a) Types of Blockchains: Actors interacting with a blockchain are either readers or writers. Readers read, analyze, or verify the blockchain. Writers have the ability to extend the blockchain using a consensus protocol. Blockchains are classified into three categories [31] [32] as follows:

- Public/Permissionless blockchains: Public blockchains are open and are not centralized. The Bitcoin and Ethereum cryptocurrencies exemplify such blockchains. The public can view all the records and can participate in the consensus process. There is no central authority to grant access to readers and writers on the network. Any peer can leave or join the network.

- Private/Permissioned blockchains: These blockchains are centralized in nature and requires permission by central authority for the authorization of the records. Hyperledger fabric and R3 Corda are some of the examples [33].

- Consortium blockchain: They are somewhat centralized. Also known as multi-centralized, these use small segments of hubs to decide agreement. Read permissions could be public or restricted within this type. One of the typical applications is called clearing.

b) Key Characteristics of Blockchain: Blockchain empowers another plan approach for distributed database utilizing peer-to-peer (P2P) communications. It is intended to fulfill key administration requirements [32] [7]. Some of them are as follows;

- Authenticity: Ensures authenticity of each transaction and prevents duplication (e.g, does not allow duplicate payments) [34].

- Transparency: Empowers transparency of data and guarantees data trace-ability (i.e., makes misrepresentation difficult).

- Attack Prevention: Ensures the integrity of the network environment from malicious user attacks.

- Decentralization: In a centralized communication framework, each transaction has to be approved through a central server, which increases expense of transaction processing and execution bottlenecks at the central server; in blockchain technology, a consensus algorithm is used to preserve the information consistency in the distributed network [7].

- Persistence: It is almost impossible to erase or rollback

transactions once they are incorporated into the blockchain. Transactions are approved rapidly, and invalid exchange is not conceded by the miners. Blocks that contain invalid transactions are identified right away.

- Anonymity: The identity of the user interacting with the blockchain is not uncovered. Note that blockchain cannot ensure the ideal protection safeguards because of the characteristic requirement [7].

- Open verification: This enables anyone to check the accuracy of the condition of the system. Miners can easily confirm the state of the transition in a distributed ledger, which can be restricted for some participants. Any participant can verify the state of the records that was changed, and the public will have the same view of the record up to some extent [32].

- Data Redundancy: This requirement is imperative for certain users; blockchains provide this by replication across peers.

- Privacy & Trust: Two essential aspects of blockchain technology, these provides read, write, grant and revoke permissions on the ledgers. Data is thus protected from unauthorized attacks.

c) Applications of Blockchain: In this section we discuss the applications and drawbacks of blockchain within Cybersecurity [7] [9], Supplychain [31] [35], Smart Contract and Sidechain [32] [36], Cryptocurrency [37] [38] [39] etc. They are listed and explained as follows:

- Cybersecurity: Blockchain is combined with domain name service so that it gives domain owners protection from attacks through decentralization of the DNS service [40].
- Supply Chain and Logistics: Blockchain bridges the transparency gap in supply-chains between customers and buyers through features such as public availability in order to track the path of products from factories, to suppliers, and finally to customers. Decentralization enables participation of all entities in the supply chain [41].Companies such as SmartLog have used it successfully to obtain transparency across their supply chain network.

- Smart Contract & Side chain Technology: Smart contracts are electronic contracts that enforce the agreements & transactions in a blockchain; for example, Ethereum supports the execution of code on the blockchain, and Bitcoin has been supporting smart contracts for a while. Sidechain technology is a software program in blockchain ledgers similar to a smart contract that allows the important information from one block to the other.

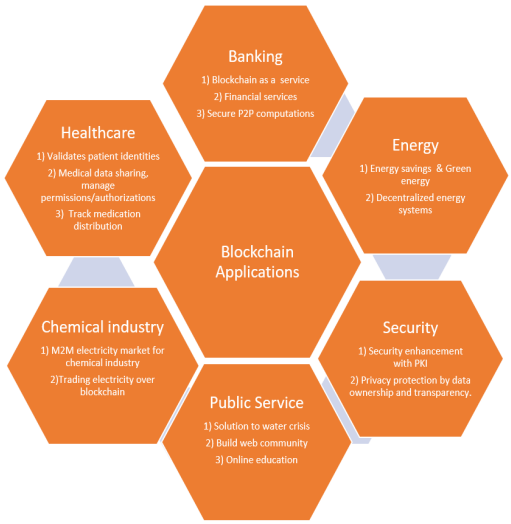

Fig. 4. Other applications of blockchain technology

- Cryptocurrency in digital economy: Utilizes cryptography to control the financial issuance and verifies the transactions. The principal digital currency, Bitcoin, created in 2009, remains the most broadly utilized cryptocurrency. Bitcoin provides for the inclusion of 40 bytes of subjective information to an exchange, which becomes a permanent part of the blockchain record. Bitcoin's blockchain has thus been utilized to enlist resource and proprietorship beyond money-related transactions.

- IoT & Blockchain integration: Auto-pay feature in vehicles enables users to pay for fuel using smart contract on blockchain [39]. Other Internet of Things applications include Iotcoin, Community currency, Enigma, International travel, etc.

- Voting: E-Voting is an issue with numerous security challenges. Public verfiability and security are addressed by blockchain [42].

- Others: Various other applications of blockchain include securing data for personal use to Business, Enterprises and Shared Economy. Blockchain are also being extensively used in predictive analysis, digital identity, copyright protection and many others. Fig. 4 summarizes blockchain applications .

d) Challenges and Limitations of Blockchain technology in intrusion detection systems and cybersecurity: In this section we discuss some of the challenges in current blockchain technology in network intrusion detection and cybersecurity applications [7] [9].

- Scalability & Speed: With the increase in number of transactions, the blockchain gets cumbersome. It

is necessary that every node stores the transactions and check their validity, and the speed depends on the protocol utilized. Speed acts as a constraint to the scalabilty of blockchain. As the blockchains can currently process only 7 transactions per second, it can not satisfy the necessity of handling millions of transactions due to small size of the block [7]. The scalabililty issue of blockchain is addressed by various ways such as:

a) Capacity Optimization of Blockchain: It is difficult for a node to work on the duplicate ledger; [43] proposed removing old transactions from a network, and all the addresses will be held by a database named account tree. Another to way to to address this issue was proposed by Versum . Versum enabled lightweight customers to redistribute costly calculations over huge inputs . It guarantees the calculation result is right through looking at results from various servers [44].

b) Redesigning Blockchain: New generation bitcoin called Bitcoin-NG was proposed in [45], whose primary thought was to decouple the traditional block into two sections called key block and micro block which was used for leader election and storing the transactions respectively. When the key block is created, the node turns into the pioneer who is in charge of producing micro blocks. Bitcoin-NG likewise broadened the heaviest (longest) chain technique in which micro blocks convey no weight. Along these lines, blockchain is overhauled, and the reciprocation between block size and system security is provided.

- Privacy Leakage: Blockchain provides a degree of security through the open and private keys. Clients execute with their private key and open key without presenting their identity. However, it appears that blockchain can't ensure the security in transactions since all the transactions are open for the public to view. Furthermore, ongoing examination has demonstrated that a client's Bitcoin exchanges can be connected to uncover the client's data. Additionally, a strategy has been exhibited to interface the client's pseudonyms to IP addresses, notwithstanding when clients are behind firewalls [7] [46]. Blockchain users can be uniquely recognized by the nodes with which they interact. This set can be learned and used to discover the source of an transaction. Different techniques have been proposed to improve obscurity of blockchain, which could be generally classified into two sorts, mixing and anonymous.

- Selfish Mining: Blockchain is prone to attacks by selfish miners. Selfish miners do not broadcast the mined blocks and get more revenue. In order to fix this issue, Heilman [47] displayed a novel methodology for legitimate mine workers to pick which branch to pursue. With arbitrary signals and timestamps, genuine excavators would choose all the newer squares. Due to this, the solution in [47] mitigates against timestamp forgery.

- Cost and Energy: Computation and transaction verification in any bitcoin mining for a single miner requires extensive energy. And, the cost and energy increase as the network evolves [9].

- Privacy & Security: Attacks like DOS are very common on blockchain platform. There is a major demand of privacy & security as the applications related to blockchain involves smart contracts and transactions on the the shared ledger.

- Complexity & delay: Blockchains are distributed; it takes of time for transactions to complete, and users to update their ledgers. This delay can invite attackers.

- Adoption & Awareness: The public lacks basic understanding of how the blockchain technology works and how it can be adopted. This is causing major hindrance in its establishment.

- Size & Organization: Many firms and organizations prefer to develop their own blockchain systems; given the significant size of distributed ledgers, this deteriorates the performance of existing blockchains and makes them less proficient.

- Management & Guidelines: Rules and regulations are frequently lag behind cutting edge innovation. Because of the absence of normal principles for finishing transactions on a blockchain, Bitcoin blockchain has avoided existing guidelines for better proficiency. Nevertheless, as Blockchain applications become more integrated into financial and cybersecurity environments, it will be necessary for them to conform to standard guidelines.

IV. Research Methodology

The purpose of this study is to review different techniques employed in intrusion detection. This papers conducts a thorough review of intrusion detection using various blockchain, machine learning and deep learning techniques. We started by researching on "Intrusion Detection Systems" and techniques for attack prevention. From the 200+ papers published in this domain matching our initial search criteria, we have reviewed 57 papers, book chapters, and journal articles, concentrating on blockchain, machine learning, and deep learning technologies. We restricted the chronological scope to the past 19 years (1999-2018).

We used the following databases in our search:

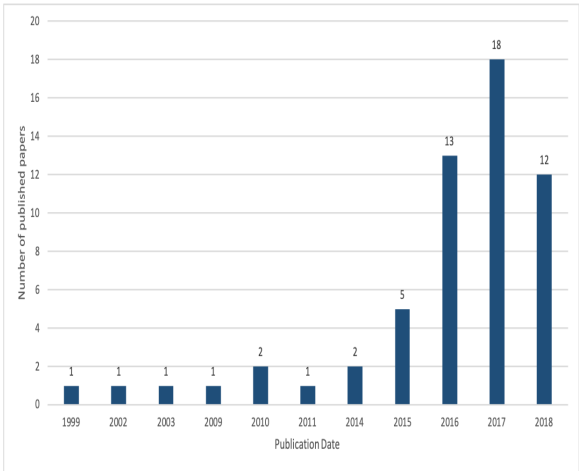

Fig. 5. Papers published in blockchain, machine learning and deep learning for intrusion detection

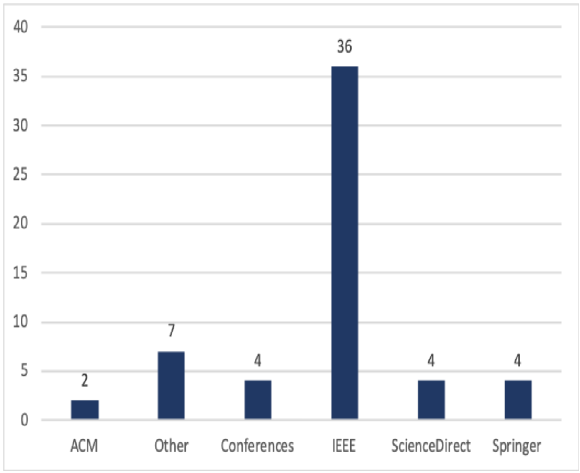

Fig. 6. Papers published in various databases.

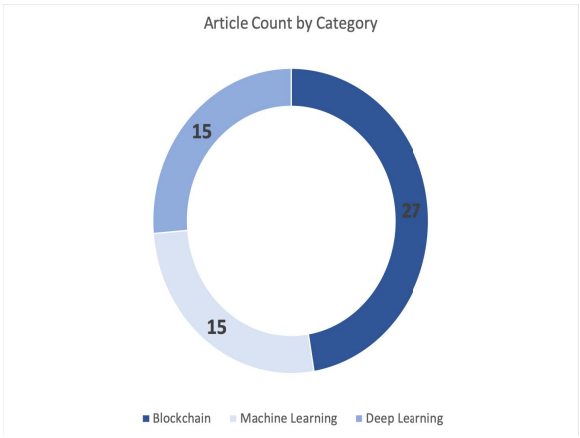

Fig. 7. Publications by topical category.

- ACM Digital Library
- Applied Science and Technology Full Text
- Computing (ProQuest)
- Gartner
- IEEE Xplore
- ProQuest Science
- SpringerLink.

We used the search text "Intrusion detection blockchain, machine and deep learning". There were numerous machine learning approaches used along with hybrid algorithms combining deep learning technology. Since our focus was blockchain technology, we omitted other hybrid technologies.

A. *Classification of papers by publication date*

There have been numerous publications on intrusion detection. We have selected over 57 papers from 200+ papers for our review. Publication counts have risen in this domain area, especially since 2016. Fig. 5 shows the publication counts per year .

B. *Classification of papers by publication source*

The papers considered for this literature survey were drawn from a variety of databases shown in Fig.6 . This figure indicates that most of the papers were published in IEEE publications.

Fig. 7 shows the distribution of publications by topical category. Of the papers we reviewed, blockchain had the highest count, followed by machine learning and deep learning. While machine learning and deep learning research still exceeds that for blockchain overall, we emphasized the blockchain research for our review due to its relevance and potential for cybersecurity .

V. Literature Review

In this section, different challenges of intrusion detection system are listed. We also discuss various techniques to overcome these challenges. First, blockchain based solutions will be described. Next, we will discuss the contribution of different machine learning [48] and deep learning algorithms in protecting the network from malicious attacks.

A. *Blockchain Based Intrusion Detection*

Blockchain-based CIDS: The author in [49] proposed an architecture of CIDS, which is based on blockchain and its distributed nature. In this model the nodes communicate with each other on two layers called Alert exchange layer and Consensus layer. The peers in the CIDS network can collaborate with each other without disclosing confidential data. This model provides data privacy and integrity.

Provchain: The author in [50] designed and implemented a decentralized data provenance using blockchain to gather and confirm cloud information provenance, by inserting the provenance information into blockchain transactions. The Provchain provides reliability, user privacy, and security to

the applications stored on the cloud.

Blockchain to protect Personal Data: The author [46] proposed an architecture which uses blockchain to secure the personal data by saving the file access permissions in blockchain on a centralized cloud.

Block secure P2P cloud storage: Another author proposed a block chain based solution for securing cloud-based storage in peer to peer contexts. This paper [51] demonstrates new cloud storage architecture to provide more reliable and secure cloud storage. They customized the genetic algorithm and reduced the file loss rate.

B. Machine Learning Techniques for Intrusion Detection

Two-tier Machine Learning Approach: In this paper, the author [52] proposed a 2 tier architecture for network intrusion detection using deep learning and machine learning algorithms. They performed simulations on KDD data set using Weka data mining tool and have demonstrated that the passage of data through two classifiers increases system security.

Hybrid machine learning techniques: In this paper, the author [22] presented a design and implementation to detect the attacks which are known by supervised learning and unsupervised learning to detect the unknown attacks. The design consisted of 7 hybrid models. The first layer consisted of supervised learning algorithm, and the second layer consisted of unsupervised algorithm. The goal of this approach is to enhance the intrusion detection in networked environments.

C. Deep Learning Techniques for Intrusion Detection Techniques

Deep Learning approach: The author [6] proposed a deep learning approach for creating a network intrusion detection system (NIDS) [53] [54]. They used sparse auto-encoder and soft-max regression on NSL-KDD dataset [55]. Anomaly detection accuracy is evaluated. Their results show that they performed better than the previous anomaly detection [56].

Deep belief network(DBN): The author [57] proposed a deep learning approach and built an intrusion detection system that uses DBN. This approach showed higher accuracy than the existing system using other training approaches like SVM, DBN and SVM-DBN [58]. In this approach DBN was used for data classification on NSL-KDD dataset.

VI. CONCLUSION

In this paper we have reviewed 57 papers from ACM Digital Library, IEEE Xplore, Sciencedirect and SpringerLink databases. Following a brief introduction to IDS, collaborative IDS, machine learning, deep learning and blockchain technology, we have presented a description of blockchain evolution, its applications, and limitations. We surveyed machine learning and deep learning technologies used for detecting malicious user attacks in networks. As part of our review, we classified the publications by year, database source, and topical category. Within the cybersecurity domain, blockchain technology promises novel solutions to issues of data provenance, data sharing, and trust [9]. Especially for CIDS, as blockchain technology evolves, it will supplement traditional intrusion detection systems and enhance cybersecurity defenses within networked environments.

REFERENCES

[1] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35 365–35 381, 2018.

[2] Z. Wang, "Deep learning-based intrusion detection with adversaries," *IEEE Access*, vol. 6, pp. 38 367–38 384, 2018.

[3] U. Bashir and M. Chachoo, "Intrusion detection and prevention system: Challenges & opportunities," in *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on*. IEEE, 2014, pp. 806–809.

[4] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," *Expert Systems with Applications*, vol. 36, no. 10, pp. 11 994–12 000, 2009.

[5] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in *2016 8th IEEE International Conference on Communication Software and Networks (ICCSN)*. IEEE, 2016, pp. 581–585.

[6] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (Formerly BIONETICS)*, ser. BICT'15. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016, pp. 21–26. [Online]. Available: http://dx.doi.org/10.4108/eai.3-12-2015.2262516

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Big Data (BigData Congress), 2017 IEEE International Congress on*. IEEE, 2017, pp. 557–564.

[8] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (idps)," *NIST special publication*, vol. 800, no. 2007, p. 94, 2007.

[9] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: a review," *Ieee Access*, vol. 6, pp. 10 179–10 188, 2018.

[10] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivanko, and M. Muhlhauser, "Towards blockchain-based collaborative intrusion detection systems," in *Critical Information Infrastructures Security*, G. D'Agostino and A. Scala, Eds. Cham: Springer International Publishing, 2018, pp. 107–118.

[11] S. R. Snapp, J. Brentano, G. V. Dias, T. L. Goan, L. T. Heberlein, C.-L. Ho, K. N. Levitt, B. Mukherjee, S. E. Smaha, T. Grance *et al.*, "Dids (distributed intrusion detection system)-motivation, architecture, and an early prototype," in *Proceedings of the 14th national computer security conference*, vol. 1. Washington, DC, 1991, pp. 167–176.

[12] V. Yegneswaran, P. Barford, and S. Jha, "Global intrusion detection in the domino overlay system." in *NDSS*, 2004.

[13] R. Huebsch, B. Chun, J. M. Hellerstein, B. T. Loo, P. Maniatis, T. Roscoe, S. Shenker, I. Stoica, and A. R. Yumerefendi, "The architecture of pier: an internet-scale query processor," 2005.

[14] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," in *null*. IEEE, 2003, p. 368.

[15] S. Yin, J. Bao, Y. Zhang, and X. Huang, "M2m security technology of cps based on blockchains," *Symmetry*, vol. 9, no. 9, p. 193, 2017.

[16] M. Vukolić, "Rethinking permissioned blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. ACM, 2017, pp. 3–7.

[17] H. Sarvari and M. M. Keikha, "Improving the accuracy of intrusion detection systems by using the combination of machine learning approaches," in *2010 international conference of soft computing and pattern recognition*. IEEE, 2010, pp. 334–337.

[18] D. Endler, "Intrusion detection. applying machine learning to solaris audit data," in *Proceedings 14th Annual Computer Security Applications Conference (Cat. No. 98EX217)*. IEEE, 1998, pp. 268–279.

[19] P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches," *Computer Communications*, vol. 34, no. 18, pp. 2227–2235, 2011.

[20] T. Poongothai and K. Duraiswamy, "Intrusion detection in mobile adhoc networks using machine learning approach," in *International Conference on Information Communication and Embedded Systems (ICICES2014)*. IEEE, 2014, pp. 1–5.

[21] A. Warzyński and G. Kołaczek, "Intrusion detection systems vulnerability on adversarial examples," in *2018 Innovations in Intelligent Systems and Applications (INISTA)*. IEEE, 2018, pp. 1–4.

[22] D. Perez, M. A. Astor, D. P. Abreu, and E. Scalise, "Intrusion detection in computer networks using hybrid machine learning techniques," in *2017 XLIII Latin American Computer Conference (CLEI)*. IEEE, 2017, pp. 1–10.

[23] B. Wahyudi, K. Ramli, and H. Murfi, "Implementation and analysis of combined machine learning method for intrusion detection system," *International Journal of Communication Networks and Information Security*, vol. 10, no. 2, pp. 295–304, 2018.

[24] M. Jabbar, R. Aluvalu, and S. S. S. Reddy, "Intrusion detection system using bayesian network and feature subset selection," in *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*. IEEE, 2017, pp. 1–5.

[25] T. Mehmood and H. B. M. Rais, "Machine learning algorithms in context of intrusion detection," in *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)*. IEEE, 2016, pp. 369–373.

[26] K. Kim and M. E. Aminanto, "Deep learning in intrusion detection perspective: Overview and further challenges," in *2017 International Workshop on Big Data and Information Security (IWBIS)*. IEEE, 2017, pp. 5–10.

[27] S. Behera, A. Pradhan, and R. Dash, "Deep neural network architecture for anomaly based intrusion detection system," in *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)*. IEEE, 2018, pp. 270–274.

[28] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *Ieee Access*, vol. 5, pp. 21 954–21 961, 2017.

[29] L. Deng, "A tutorial survey of architectures, algorithms, and applications for deep learning," *APSIPA Transactions on Signal and Information Processing*, vol. 3, 2014.

[30] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, 2016, pp. 258–263.

[31] N. Bozic, G. Pujolle, and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," in *Smart Cloud Networks & Systems (SCNS)*. IEEE, 2016, pp. 1–8.

[32] K. Wust and A. Gervais, "Do you need a blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018, pp. 45–54.

[33] J. J. Xu, "Are blockchains immune to all malicious attacks?" *Financial Innovation*, vol. 2, no. 1, p. 25, 2016.

[34] Y. Cai and D. Zhu, "Fraud detections for online businesses: a perspective from blockchain technology," *Financial Innovation*, vol. 2, no. 1, p. 20, 2016.

[35] M. Pilkington, "11 blockchain technology: principles and applications," *Research handbook on digital transformations*, vol. 225, 2016.

[36] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Work Pap.–2016*, 2016.

[37] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain technology: applications in health care," *Circulation: Cardiovascular Quality and Outcomes*, vol. 10, no. 9, p. e003800, 2017.

[38] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, 2017.

[39] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia computer science*, vol. 98, pp. 461–466, 2016.

[40] F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From bitcoin to cybersecurity: A comparative study of blockchain application and security issues," in *2017 4th International Conference on Systems and Informatics (ICSAI)*. IEEE, 2017, pp. 975–979.

[41] K. Sadouskaya *et al.*, "Adoption of blockchain technologyin supply chain and logistics," 2017.

[42] M. Pawlak, A. Poniszewska-Marańda, and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," *Procedia Computer Science*, vol. 141, pp. 239 – 246, 2018, the 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2018) / The 8th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2018) / Affiliated Workshops. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050918318271

[43] B. Franca, "Homomorphic mini-blockchain scheme," 2015.

[44] J. van den Hooff, M. F. Kaashoek, and N. Zeldovich, "Versum: Verifiable computations over large public logs," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 1304–1316.

[45] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th Symposium on Networked Systems Design and Implementation (16)*, 2016, pp. 45–59.

[46] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[47] E. Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 161–162.

[48] C. Sinclair, L. Pierce, and S. Matzner, "An application of machine learning to network intrusion detection," in *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)*. IEEE, 1999, pp. 371–377.

[49] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivanko, and M. Muhlhauser, "Towards blockchain-based collaborative intrusion detection systems," in *International Conference on Critical Information Infrastructures Security*. Springer, 2017, pp. 107–118.

[50] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, ser. CCGrid '17. Piscataway, NJ, USA: IEEE Press, 2017, pp. 468–477. [Online]. Available: https://doi.org/10.1109/CCGRID.2017.8

[51] J. Li, J. Wu, and L. Chen, "Block-secure: Blockchain based scheme for secure p2p cloud storage," *Information Sciences*, vol. 465, pp. 219–231, 2018.

[52] M. Sreekesh *et al.*, "A two-tier network based intrusion detection system architecture using machine learning approach," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. IEEE, 2016, pp. 42–47.

[53] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with svm for network intrusion detection," *IEEE Access*, vol. 6, pp. 52 843–52 856, 2018.

[54] K. Yang, J. Liu, C. Zhang, and Y. Fang, "Adversarial examples against the deep learning based network intrusion detection systems," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 559–564.

[55] M. Z. Alom and T. M. Taha, "Network intrusion detection for cyber security using unsupervised deep learning approaches," in *2017 IEEE National Aerospace and Electronics Conference (NAECON)*. IEEE, 2017, pp. 63–69.

[56] R. Mitchell and R. Chen, "A survey of intrusion detection in wireless network applications," *Computer Communications*, vol. 42, pp. 1–23, 2014.

[57] M. Z. Alom, V. Bontupalli, and T. M. Taha, "Intrusion detection using deep belief networks," in *2015 National Aerospace and Electronics Conference (NAECON)*. IEEE, 2015, pp. 339–344.

[58] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 2016, pp. 195–200.