

Article

Blockchain-Based Smart Home Network Security through ML

Anurag Sinha^{1,*}, Pooja Jha, Biresh Kumar, Aditya Mishra, Vaibhav Ujjwal, and Anurag Singh⁵

¹ ICFAI tech school, ICFAI University Ranchi, Jharkhand, India

² Amity Institute of Information Technology, Amity University Jharkhand, Nivaranpur,, India

³ Department of Computer engineering and application, GLA University, Mathura, India

⁴ Galgotias College of Engineering and Technology, Greater Noida, India

⁵ Department of Information Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur, India

*Corresponding author: Anurag Sinha (email: anuragsinha257@gmail.com)

Received 20 August 2022; Accepted 21 October 2022; Issue Published 15 December 2022

Abstract: Due in large part to the Internet of Things' (IoT) anticipated enormous scope and extensive implementation, achieving safe and private communications on the IoT is difficult. Recent initiatives have investigated the use of blockchain technology to enable decentralized protection and privacy. Such methods, however, are prohibitive for the bulk of IoT applications due to their high computational and time requirements. We specifically offer a resource-efficient, blockchain-based IoT security and privacy solution in this study. The approach is made achievable by utilizing Deep Extreme Learning Machine in combination with unique computational resource exploitation in a typical IoT context (such as smart houses) (DELM). In the proposed method, the privacy, integrity, and accessibility of the Blockchain based Architecture of Smart Homes are prudently considered while assessing the reliability of the system. The overheads caused this strategy are negligible with respect to the security and privacy benefits, we further underline by presenting simulated findings.

Keywords: smart home; data; AI; blockchain; smart city; automation

Copyright © 2023 Journal of Smart Internet of Things (JSIoT) published by Future Science for Digital Publishing and Sciendo. This is an open access article license CC BY (<https://creativecommons.org/licenses/by/4.0/>)

1. Introduction

A smart home is an integrated Internet of Things house that provides residents with security, healthy and comfortable standard of life along with several other benefits. Smart home technologies have the potential to simplify and improve independent lives of people. The attention of consumers and device developers has been drawn to them because they offer practical tools like tracking behaviours and safety checks. Although intelligent homes have a lot to offer homeowners and other interested parties, they could be vulnerable to criminal cyberattacks that put users' privacy and safety at risk. Such threats have conventional responses, but they are weak against ferocious attacks

and highly centralised. Therefore, the creative field of autonomous smart home applications and facilities lacks the adaptability and scalability needed for proper utilisation. Numerous sophisticated technologies make life easier for individuals [1]. These programs generate a plethora of data. Safety issues arise from storing this continually changing data in repositories.

However, blockchain has exhibited exceptional results as a pillar of the cyber-security architecture in numerous smart home gadgets, including data transmission and remote connectivity. These issues might be solved via centralised storage networks and blockchain technologies

The three pillars of blockchain technology are rigidity, decentralisation, and openness. While blockchain technology ensures security, the three purposes have become a gateway to a variety of applications, such as the nature of digital currency and the analysis of the viability of intelligent applications. For instance, cyberattacks have recently taken on increasingly complicated forms, such as most attacks managing votes and Sybil attacks for creating false identities and monitoring consensus.

A robust Intrusion Detection System (IDS) is necessary to address the underlying problem because conventional techniques use a signature-based strategy to identify unique arrangements. The Deep Extreme Learning Machine (DELM) [1], one of the newest technologies, may be used to examine data flow to find patterns of attacks and intrusions. In order to process this enormous volume of data, it is crucial to manage smart blockchain-based apps by creating potent and versatile algorithms. Without human assistance, robots can learn, reason, and act in certain ways thanks to machine learning. It is regarded as a framework for artificial intelligence (AI). The fundamental objective of machine learning is to develop an efficient algorithm that can accept information from the input, predict the future, and modify the outputs using statistical analysis. Machine learning has the capacity to analyse a substantial quantity of data and come to informed conclusions.

Therefore, utilizing Deep Extreme Learning Machine (DELM) technology and improved performance, this research aims to make intelligent homes safer. A comprehensive analysis of cutting-edge innovations pertinent to blockchain-based smart homes outfitted with the Deep Extreme Learning Machine is provided in this study, along with a fresh perspective on a variety of applications that is supported by the latest stages of technological development. Deep Extreme Learning Machine architecture has been proposed for implementation in blockchain-based smart homes, as presented in Fig. 1. Here, a smart application collects information from many sources, such as sensors, smart devices, and IoT gadgets. Information acquired from these intelligent applications is processed and analysed. A key component of those applications is the blockchain. The Deep Extreme Learning Machine will then be used in these applications to analyse and forecast data. The block-chain network could be used to process the datasets used by the DELM framework, eliminating information errors such repetition, loss of data value, inaccuracies, and disruption. Blockchains are data-dependent. Data-related issues in the DELM framework will therefore be disregarded. Instead of focusing on the complete collection of datasets, the DELM framework can be used to focus on different chain pieces. This will offer an unique foundation for numerous applications, including fraud detection and theft prediction.

This article's sections are organised as follows. The following section provides an overview of the relevant survey articles. We then go over the fundamental structure for blockchain, how the DELM technique is implemented on a blockchain-based smart house, and the architecture for smart home applications. The simulation and tests of the DELM approach are then covered. The final section examines the findings of the research.

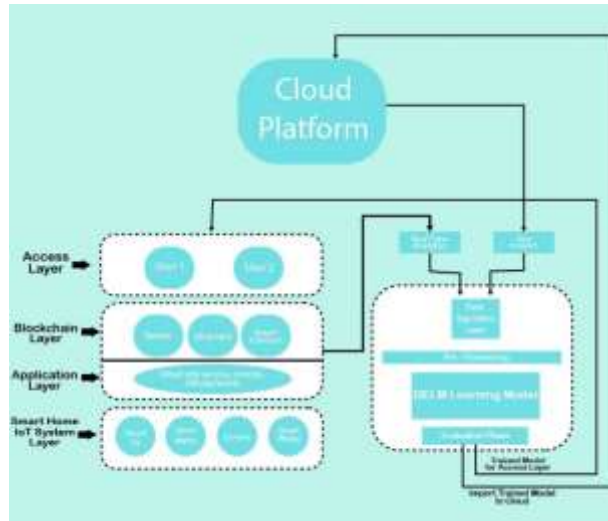


Figure 1: A blockchain-based smart home application framework with 4 layers that uses DELM.

2. PREVIOUS WORK

The ideal of intelligent cities is secure, safe, green, and efficient in all frameworks, including power, water, and transportation [3]. According to [4], a smart city is one that is innovation-focused and better because it links people, data, and urban characteristics through cutting-edge technology, creating a stable, secure city with effective and innovative enterprises and a higher quality of life. The smart city, according to S. Tanwar et al. [5], is a more complex civilization in which numerous elements—including people, the environment, mobility, democracy, and the economy—are installed in a smart system.

A user-centric block-chain approach to secure the IoT's edge data sharing is presented in [6]. Z. Zhou et al's investigation [7] of blockchain technology, contract theory, and edge computing led to the introduction of a reliable and efficient energy sharing system for automobiles to grids. In order to comprehend complex blockchain topologies, [8] proposed a software-defined blockchain platform. They also provided a consensus-function solution to virtual machines using a framework that is application-aware and capable of handling specialised consensus tools. The goal of this project is to help people migrate to the Internet of Things, particularly in the creation of smart cities. According to the Internet of Things European Research Cluster, the Internet of Things (IoT) is a dynamic, worldwide network infrastructure that automatically configures physical and virtual objects and communicates them using a standard, interoperable protocol. The biggest chance for a livable city would be IoT [9]. Numerous computing technologies have been integrated into IoT in order to make it intelligent. The most significant technologies are limited to data mining, AI, cloud computing, and neural networks.

It is assumed that 70 percent the population will reside in towns by the year 2050, [10]. The ease of life is produced by the concept of understanding. A project called "Smart City" makes use of cutting-edge technology to enhance environmental sustainability. Intelligent communities frequently increase environmental efficiency and provide residents with improved facilities. To promote and transform cities into smart cities, connectivity and information technology are essential.

Numerous research papers have been published as a result of the growing popularity of blockchain in smart homes. For instance, [11] explored agreement, access control, home care,

payments incorporation, market sharing, and numerous smart city services in their study on blockchain technology's use in the smart world. However, data analytics with a focus on intelligent home services tend to understudy the usage of blockchain in the technology market. Many see this as a potential use for smart homes using blockchain. The thorough examination of several Peer-to-Peer energy trading network blockchain implementations was identified in [12]. The use of the global agreement process is covered in great detail, as are other aspects of various smart home systems like safety issues, the smart grid, Artificial Intelligence (AI), payment processing, and Big Data analytics. Even though the technical aspects were carefully examined in their research, the sample neglected several typical implications from the standpoint of smart homes, such as financial management for smart cities and smart home care.

3. PROPOSED DEEP EXTREME LEARNING MACHINE (DELM) FRAMEWORK SETTING

Blockchain was developed by Satoshi Nakamoto in 2008 [2]. By leveraging its own blockchain money, a P2P payments network will do away with third parties and double-spending problems (e.g., bitcoins). Every data block in this clustered system is verified with the preceding hash block using the Secure Hash Algorithm (SHA-256). A block's fundamental elements were its block number, the preceding block's hash, the transaction information, the nonce, and the time stamps. In contrast to the timestamp's continuous variable, a nonce's variable is random. The validator and the miner (computer node) continuously hash the static (block) and dynamic (time-stamp and nonce) data in search of a value that starts with a large number of consecutive leading zeros. Commonly referred to as a cryptography problem, this methodology. In the blockchain, the miner who finds the correct hash value will first decide who gets to put the block in. The method used to determine whether or not a block is valid is known as proof of work. Every node connected to an IoT device in a smart home communicates with a memory pool, including blockchain miners. All transactions are stored in the memory pool and are awaiting use in the blockchain to add a new block. The Merkle tree verifies and compiles all transactions.

If a transaction is viable, it is extracted and added to the block so that miners can mine it across the board of the smart home system. Miners alter the nonce and time label to produce a block's hash. The application then tries to compare the generated hash to the target. The hash is connected to the chain whenever mining of a block is completed by a miner. The operation will restart whenever the hash reaches the desired quantity. The performance of the proof of work is evaluated and applied to the chain if the hash value is less than the desired value. This message is therefore broadcast around the network to notify each connected node to erase completed memo pool transactions. Blockchain technology is influencing the smart home communication environment more and more since it is versatile and flexible enough to interface with smart house IoT apps without much difficulty. The blockchain-based smart home network is shown in Figure 1. The architecture consists of four layers: an IoT data sources layer, a DELM-enabled block-chain network layer, a client node, and an intelligent home device layer.

4. Incorporation Of Deep Learning Machine In Blockchain-Based Smart Home

For the evaluation of smart homes, environments, and people, the IoT information layer gathers data from devices that are crucial. These gadgets can be divided into three major categories: sensors, multimedia, and healthcare. A blockchain layer is made up of closed-circuit television, wearables, and other IoT sensor devices. Information from these nodes is gathered and kept on a centrally constructed repository or database, such a blockchain, which creates the base layer of the stack.

DELM computing technology can be used to enhance blockchain-based applications. Using DELM for the distributed ledger can enhance security. By providing better channels for information exchange, DELM can also be used to lengthen the time it takes to understand something. It also

creates the opportunity to develop better frameworks employing the centralised design of blockchain technology. We introduced the DELM implementation architecture in blockchain-enabled intelligent technology, as shown in Figure 1. Here, a smart application collects data from a variety of sources, including cameras, smart devices, and IoT systems. These approaches' information was assessed as a part of smart applications. The blockchain plays a crucial role in these intelligent applications. Nevertheless, the DELM framework can be applied to such application data for interpretation (data analysis and real-time analysis) and prediction. Data sets utilised by DELM models are processed over a blockchain network.

Repetition, incorrect data values, flaws, and noise-related errors are all minimised. Information-related issues can be reduced with the DELM system because information is dispersed on a blockchain. The DELM frame might be based on specific chain segments rather than the entire data set. This can include special frameworks for certain applications, including fraud detection or identity theft prevention. The blockchain model is based on the edge of the IoT architecture and is made up of three essential components: the Deep Extreme Learning Machine layer, the smart contract, and the blockchain information architecture. The proposed method is composed of three layers: data gathering, preparation, and evaluation. The evaluation layer consists of two sublayers: prediction and performance evaluation. For experimental study, reliable actuators and sensor data are obtained.

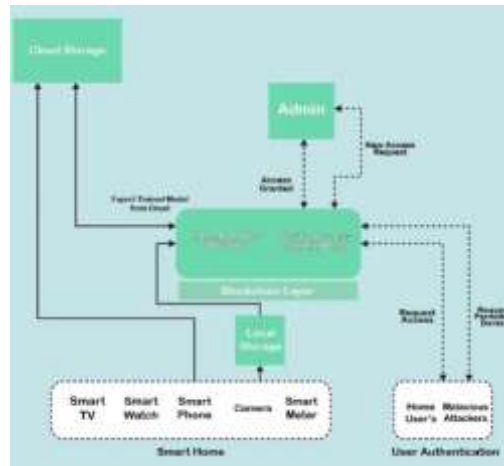


Figure 2: Blockchain-based smart home management system empowered with DELM.

The information gathered is given to the acquisition layer as input. Specific data cleaning and planning strategies have been implemented to eliminate knowledge disparities at the preprocessing layer. The DELM was employed to safeguard the smart home network from any nefarious or intrusive application layer behaviour.

Through cryptography, hash values link blocks together. While intelligent contracts adhere to existing standards to make decentralised transactions easier and more straightforward, a home server computer may be thought of as a miner for verifying upcoming transactions and adding more blocks.

The application layer is designed to encourage the integration of specialised smart home applications with the present blockchain networks. A few of the smart home technologies addressed by this framework are the digital market, access management, interoperability in the home and healthcare, automatic infrastructure payment, and intelligent community services. Other parties can profit from blockchain-based smart home technologies like microgrids, retail stores, utility suppliers, careers, and so forth thanks to the access layer, which tops the hierarchy.

The development of smart devices has opened the door for innovative IoT solutions to run smart residential systems efficiently and intelligently. Cameras, CCTV, smart TVs, exercise equipment,

smartphones, and actuators are the primary elements of a more advanced smart home environment. The key services of an IoT-enabled smart home include remote controls, alarm generation, safety surveillance, and other similar functions. A customised access control system that enables the home user to be enabled upon request must be utilised to increase the effectiveness of the smart home and spot any harmful hacker activity. A description of this access authorisation may be found in a user's collection of IoT system access records. To survive hostile attacks, such information should be kept in an unforgeable distributed information network. To demonstrate how blockchain creates secure access, we utilise the scenario below.

the resident (Admin), who could use the applications in the smart home and have access to them. Figure 2 demonstrates how using a block-chain produces safe access. The user must first decide on the amount of access before applying it to the home service computer. Youths, children, visiting families, and the home's administrator (Admin) are all authorised at the highest level, although they require mid-level clearance. Neighbors and outsiders have little (or no) control rights. When a user submits a request, the home server first verifies the access control directory. Once this directive has been sent by the home server to the blockchain layer, the individual user's legal authentication is completed. For several consumers and devices, the access control list is stored in a blockchain policy header. One part of the block data needed to run control tools and policies is the policy header. The administrator receives the request from the new user and has the authority to accept or reject it. Blockchain miners enter the header policy details and perform operations after the administrator grants or rejects authorization. It is possible to get rid of malicious attackers using this technique.

5. Deep Extreme Learning Machine

This paper has developed an automated ITC-BWODHL technique for congestion detection to improve traffic congestion control in smart cities. The ITC-BWOHDL technique intends to utilize feature subset selection with parameter-tuning strategies for effective traffic congestion management. It comprises a three-step procedure such as EPO-FS-based feature selection, HDL-based congestion detection, and BWO-based hyperparameter tuning. The ITC-BWOHDL technique primarily designed the EPO-FS approach to reduce computation complexity and improve classification results. The BWO-based hyperparameter tuning process gets executed to enhance the classification outcomes of the HDL algorithm. For exhibiting the greater classification outcome of the ITC-BWOHDL system, a comprehensive range of experiments was executed. The achieved outcomes stated the betterment of the ITC-BWOHDL algorithm over other models. In future, real-time traffic data can be collected to examine the congestion control results of the ITC-BWOHDL technique.

The DELM can be applied in a variety of industries to foresee issues such as health issues, energy usage, transportation, traffic management, and more. [1]. The learning mechanism can be overridden in the conventional Artificial Neural Networks (ANN) algorithms, which require several changes and lengthy learning cycles. According to [13], an extreme machine is a machine with knowledge. Because DELM learns quickly and performs well in the rate of procedural convolution, it may be employed widely in a variety of fields for classification and regression tasks. To achieve high accuracy and a low error rate in the learning phase of the proposed system, we employed the backpropagation strategy, in which data travels backward through the network and the neural network modifies the weights. The extreme learning machine is a feed-forward neural network with several layers that indicates data only moves in one direction. As we extract the training model and forecast the actual data throughout the validation stages, the network's weights remain constant. The proposed DELM approach has three layers, including an input layer, hidden layers, and an output layer. There are several hidden layers, an output layer, and input layers in the DELM structure. In contrast to an extreme learning machine, which uses numerous neurons and one hidden layer to train a dataset, a deep extreme learning machine uses several buried layers and a fixed

number of neurons to maximise network efficiency. Therefore, as demonstrated in Table 1, we have improved results compared to other machine learning techniques by expanding the network's hidden layers and its fixed population of neurons. We have included a feed-forward technique with the backpropagation technique to modify the network weights and lower the error rate. In terms of accuracy, the DELM framework performs better than the other machine learning methods.

Numerous statistical indicators, including accuracy, miss rate, sensitivity, specificity, false positive value, and positive prediction value, are included in the assessment layer, are evaluated to optimise smart home security.

The backpropagation method's components include weight setup, feedforward propagation, reverse error propagation, and distinguishability updating. The hidden layer of each neuron uses a sigmoid activation function. By reducing the square sum from the desired output by 2, this aids in the design of the DELM hidden layer and the sigmoid input function. It is necessary to modify the weight in order to mitigate the typical mistake.

Method	Accuracy of NSL- KDD dataset [14]	Accuracy of KDD- CUP- 99 dataset [15]
ANN	81.3%	90.41%
SVM	69.49%	89.96%
Decision Tree	81.49%	91.11%
Proposed DELM	93.93%	94.61%

Table 1: Contrasting the proposed DELM method with existing machine learning techniques using various datasets.

6. RESULT

With input data from [14], the Deep Extreme Learning Machine (DELM) in the suggested framework was developed. 15% of the data are utilised for validation, while 85% of the data are used for training. DELM looked for any malice or infiltration in a variety of secret layers, hidden connections, and activation functions. Additionally assessed were the amount of neurons in buried layers and several active activities. To accurately forecast the effectiveness of this system, we analysed the DELM in this analysis. We employed many statistical measures to calculate the output with the DELM algorithm's counterpart algorithms.

Table 2 shows the proposed blockchain-based smart home empowered with the DELM system model prediction of intrusion detection during the training periods. 124,845 samples in total are used for training. These are further separated into 57502 samples of attack and 67,343 samples of normal behaviour. A normal class of samples is discovered to have 65,366 samples accurately predicted, whereas 1,977 samples are wrongly projected as attacks when none actually exist. In the event that an assault is found, 57502 samples are gathered, of which 55,082 are accurately classified as such and 2,420 are mistakenly classified as such when an attack is present.

The suggested smart home built on a blockchain, displayed in table 3, that is equipped with intrusion detection predicted by the DELM system model during validation. 22,544 samples in total are used for validation. These are further separated into 9,709 samples of normal and 12,834 samples of attack, respectively. 9 237 samples of a typical class are observed to be successfully predicted, whereas 473 records are wrongly projected as attacks when none actually exist. Similar

to the assault example, 12,834 samples are collected, of which 11,936 are accurately predicted as detected attacks and 898 are incorrectly predicted as normal when an attack actually was there.

The performance of the proposed blockchain-based smart house outfitted with the DELM system model employing a variety of statistical measures during the training and validation stages. It is amply demonstrated that the accuracy and miss rates produced by the suggested model while training is 96.34% and 3.71%, respectively. During validation, the suggested system's accuracy and miss rates were 92.45 percent and 7.21 percent, accordingly. Additionally, it displays how well the system model performed during the training and testing phases in terms of sensitivity and specificity. It clearly shows that the proposed system during training gives 96.43 percent and 95.8 percent sensitivity and specificity, respectively, while it gives 92.87 percent and 96.19 percent sensitivity and specificity during validation. In order to forecast the outcomes, additional statistical metrics including false positive and false negative rates, probability ratios for both positive and negative outcomes, as well as positive and negative prediction values, are included.

85% of sample data in training of the proposed DELM based model			
Total samples (N = 124,845)		Output (O ₀ , O ₁)	
Input	Expected output (T ₀ , T ₁)	O ₀ (normal)	O ₁ (attack)
	T ₀ = 67,343 normal	65,366	1,977
	T ₁ = 57,502 attack	2,420	55,082

Table 2: Training of the deep, extreme learning machine system model for the blockchain-based smart home amid the anticipation of hostile activities or assaults.

15% of sample data in validation of the proposed DELM based model			
Total samples (N = 22,544)		Output (O ₀ , O ₁)	
Input	Expected output (T ₀ , T ₁)	O ₀ (normal)	O ₁ (attack)
	T ₀ = 9,709 normal	9,235	473
	T ₁ = 12,834 attack	898	11,936

Table 3: Validation of the deep, extreme learning machine system model for the blockchain-based smart home during the detection of harmful behavior or assaults.

7. Conclusion

Additionally, other statistical measurements are incorporated in order to forecast the results. In terms of evaluation and prediction, intrusion identification in smart homes continues to be a significant difficulty. Meanwhile, recent advancements in the fields of machine intelligence and

blockchain have demonstrated considerable promise in reaching such goals. Such solutions are not easily applicable due to the limited processing and power in the most of the smart home arrangements. This work filled this gap by offering a simple yet powerful approach for intrusion identification and prediction. It was suggested to use a Deep Extreme Learning Machine (DELM) blockchain-based architecture. A variety of statistical methods were used to evaluate the effectiveness of the suggested solution. These estimation results demonstrate that the DELM method is far more reliable than other techniques. With a score of 92.45%, the suggested DELM technique showed astonishing accuracy. The reported results are promising, and we are currently looking at expansions using new datasets and alternative architectural designs.

References

- [1] S. Abbas *et al.*, “Modeling, Simulation and Optimization of Power Plant Energy Sustainability for IoT Enabled Smart Cities Empowered with Deep Extreme Learning Machine,” *IEEE Access*, vol. 8, 2020, pp. 39982–97.
- [2] S. Nakamoto *et al.*, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Manubot, 2019.
- [3] C. Badiet *et al.*, “Smart City IoT Platform Respecting GDPR Privacy and Security Aspects,” *IEEE Access*, vol. 8, 2020, pp. 23601–23.
- [4] G. S. Aujla *et al.*, “BlockSDN: Blockchain-as-a-Service for Software Defined Networking in Smart City Applications,” *IEEE Network*, vol. 34, no. 2, 2020, pp. 83–91.
- [5] S. Tanwar *et al.*, “Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward,” *IEEE Access*, vol. 8, 2020, pp. 474–88.
- [6] G. Li *et al.*, “Preserving Edge Knowledge Sharing Among IoT Services: A Blockchain-Based Approach,” *IEEE Trans. Emerging Topics in Computational Intelligence*, 2020, pp. 1–13.
- [7] Z. Zhou *et al.*, “Secure and Efficient Vehicle-to-Grid Energy Trading in Cyber Physical Systems: Integration of Blockchain and Edge Computing,” *IEEE Trans. Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, 2020, pp. 43–57.
- [8] J. Wu *et al.*, “Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT,” *IEEE Network*, vol. 34, no. 1, 2020, pp. 69–75.
- [9] Y. H. Park *et al.*, “Blockchain-Based Model for Trustworthy Shared Internet of Things Device Management,” *Proc. 2020 Int’l. Conf. Electronics, Information, and Commun. (ICEIC)*, IEEE, 2020, pp. 1–2.
- [10] M. Moore, P. Gould, and B. S. Keary, “Global Urbanization and Impact on Health,” *Int’l. J. Hygiene and Environmental Health*, vol. 206, no. 4-5, 2003, pp. 269–78.
- [11] S. Aggarwal *et al.*, “Blockchain for Smart Communities: Applications, Challenges and Opportunities,” *J. Network and Computer Applications*, vol. 144, 2019, pp. 13–48.
- [12] M. Andoni *et al.*, “Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities,” *Renewable and Sustainable Energy Reviews*, vol. 100, 2019, pp. 143–74.
- [13] G. B. Huang, D. H. Wang, and Y. Lan, “Extreme Learning Machines: A Survey,” *Int’l. J. Machine Learning and Cybernetics*, vol. 2, no. 2, 2011, pp. 107–22.
- [14] “NSL-KDD,” Kaggle.com, 2020, available: <https://www.kaggle.com/hassan06/nslkdd>; accessed: 15 Jan 2020.
- [15] “Network Intrusion Detection,” Kaggle.com, 2020, available: <https://www.kaggle.com/sampadab17/network-intrusion-detection>; accessed: 26 Aug. 2020.