ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

ARTIFICIAL NEURAL NETWORKS FOR EDGE AND FOG COMPUTING-BASED ENERGY PREDICTION

M.Syamala Sai Sree[1], MP Yeshswini [2], MP Jahnavi [2], K Ruchitha[2], M Jaswitha[2]

[1] *Assistant Professor, Department of Information Technology, Mallareddy Engineering College for Women, (UGC-Autonomous), Hyderabad, India, syamalamallubhotla71@gmail.com.*

[2] *Student, Department of Information Technology, Mallareddy Engineering College for Women, (UGC-Autonomous), Hyderabad, India.*

Abstract

Edge and Fog Computing have become increasingly popular in recent times as innovative distributed computing paradigms that bring computational power closer to the data source. This proximity enables real-time processing and analysis of data, making it particularly advantageous in energy management systems. Accurate prediction of energy consumption is crucial for efficiently utilizing resources and optimizing energy usage. In the realm of energy prediction, the traditional approach involves utilizing statistical methods, time series analysis, and regression models. However, these methods have their limitations. They often require manual feature engineering, overlooking intricate relationships within the data, and leading to limited predictive performance, especially when dealing with complex and non-linear datasets. Furthermore, they may not fully capitalize on the benefits of distributed computing in Edge and Fog environments. On the other hand, accurate energy prediction holds immense significance for sustainable energy management, especially in the context of modern smart grid systems and Internet of Things (IoT) applications.

1. Introduction

Edge and fog computing-based energy prediction is an advanced approach in the field of energy management and forecasting. This method leverages the capabilities of edge and fog computing to enhance the accuracy and efficiency of energy consumption predictions across various applications, such as smart grids, industrial automation, and smart buildings. Edge computing, involving data processing closer to the source of generation or consumption, and fog computing, which extends this concept by distributing computing resources even closer to the data source, play pivotal roles in this context. These paradigms reduce latency, minimize bandwidth usage, and improve real-time decision-making, making them ideal for energy prediction applications. Energy prediction, in this context, refers to estimating future energy consumption patterns, a critical factor for optimizing energy distribution, load balancing, and resource allocation. By deploying edge and fog computing technologies, several advantages are achieved: In the realm of edge and fog computing-based energy prediction, real-time data processing is a pivotal advantage. These computing nodes can process data from sensors and devices in real-time, enabling immediate responses to changing energy consumption patterns. This feature is particularly valuable in applications where timely decision-making is crucial. Reduced latency is another significant benefit. With computing resources positioned closer to the data source, the latency associated with transmitting data to remote servers is minimized, ensuring energy predictions are based on the most up-to-date information available. Data privacy and security are paramount concerns in energy-related applications. Edge and fog computing allow data to be processed locally, reducing the need to transmit sensitive energy consumption data to external servers. This enhances data privacy and security. Scalability is a vital aspect of these architectures. They are highly scalable, allowing for the addition of more computing resources as needed. This flexibility is essential in dynamic environments where energy consumption patterns may change rapidly. Resilience is also a critical feature. Distributed

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

computing architectures are inherently more resilient. If one edge or fog node fails, others can take over, ensuring that energy prediction services remain available. Cost-efficiency is a practical advantage of this approach. By processing data locally and reducing reliance on centralized cloud resources, organizations can potentially lower their operational costs, making it an economically attractive option.

3. Literature Survey

The Internet of Things (IoT) connects the digital and physical worlds. It has shown significant growth over the past decade [1]. The embedded smart heterogeneous devices and related technologies have grown due to the quick development of IoT. For an application to function, a number of heterogeneous and diverse protocols and resource-constrained devices must interact and synchronize with one another under the IoT paradigm [2,3]. IoT applications are usually based on real-time monitoring techniques. These limitations specifically affect interoperability and security, creating hindrances in IoT services. Due to growing problems with environmental pollution and global energy depletion, energy management is required as a result of rising energy prices brought on by a variety of variables, including supply and demand, weather forecasts, global markets, and governmental regulations [4]. The smart home system obtains utility pricing data from smart meters by utilizing the advanced metering infrastructure (AMI). Smart meters can monitor and regulate electrical devices in addition to measuring power usage [5]. Despite the smart home concept becoming more and more popular, such technology is susceptible to numerous security risks. Data transmission using wireless technology greatly decreases the need for physical labor; however, the smart home network community is susceptible to data theft [5]. Technical advancements have been made in creating frameworks for the identification and mitigation of these costly assaults [6]. Smart meters show which appliances are now consuming electricity, how much they cost, and what they are. This knowledge can be abused by many different kinds of people. The unauthorized use of personal data constitutes a privacy infringement and might have very serious repercussions [7].

According to the report “State of IoT Security” a 22% increase has been observed in cyber attacks on IoT applications. In addition, such attacks being highly graded and sophisticated indicate serious concerns [8,9]. As devices have limited processing and storage capabilities, smart devices are vulnerable to assaults as these devices violate many policies regarding security [10,11]. Most fundamental security aspects such as confidentiality, integrity, and availability must be preserved by every application [12] but, due to real-time monitoring and extensive applications in the IoT paradigm, tens of thousands of devices are embedded and connected, creating trouble for the present server–client model in synchronization and interoperability. Specifically, in smart homes, a variety of IoT-enabled devices are being deployed from various vendors [13]. The immutability of data, system transparency, transactional security, transparency, cryptographic protection, and other distinctive aspects of blockchain enabled it to advance a variety of technologies, including voting processes, IoT applications, supply chain management, finance, healthcare, and insurance, among others. Blockchain development was accelerated by the growing desire for technical advancements. Financial transactions were made possible without relying on middleware due to a peer-to-peer electronic cash system such as Bitcoin [14]. For the elimination of third-party involvement, cryptography is used. For IoT, there are numerous methods for accomplishing confidentiality and security [15].

Various studies are intrigued by the integration of blockchain into IoT biological networks. Only two or three studies, however, have looked into how blockchain supports achieving IoT security requirements. In this area, we describe the projects that describe such partner-level organizations and display the phenomena of projects to satisfy security needs. Since the majority of the work focuses on using blockchain advances to achieve IoT benefits, IoT security analysis is tiresome and the blockchain is constrained. However, with the advancement in Web 3.0, the world is moving toward blockchain-

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

modeled systems for securing data and transactions. In the IoT, a large number of integrated sensors and actuators are in communication with one another and carry out transactions for each action. Most of the time, third parties are required to complete online transactions. This not only imposes restrictions on the transaction's minimum allowable cost but also increases the risk of intrusion and data misuse [16]. Blockchain is one of the ways to strengthen IoT security, especially in distributed systems, and many studies support the use of blockchain-based IoT systems and secure transactions [17]. Blockchain technology is based on the distributed ledger against the centralized database. All the participating entities in the transaction have the ledger copy. In the IoT paradigm where a large amount of transaction data are involved, the disfunction of centralized database results in a loss of data. The blockchain can resolve this issue, in addition to ensuring the transparency of transactions. Due to these promising features, blockchain is gaining attraction for a wide range of applications, including IoT.

Numerous studies have proved the security-enhancing potential of blockchain technology in a variety of fields [18,19,20,21]. Another study [22] proposed a verifiable query layer (VQL) to address blockchain data querying inefficiencies and validity. While blockchain technology has found expanding uses, direct inquiries are time-consuming and indirect queries are compromised, making practical deployment difficult. Another study [23] proposed vChain+ to improve blockchain database search. Blockchain technology, popularized by cryptocurrencies and decentralized applications, is safe and tamper-resistant. The study criticized vChain's worst-case linear-scan search performance and unrealistic public key management. vChain+, an upgraded searchable blockchain system, overcomes these restrictions while providing efficient verified boolean range queries and adding capabilities.

Balogh et al. [4] used the application layer, network layer, and physical layer to make the basic architecture of the IoT systems. Many devices are embedded in the physical layer and interlinked through the gateway. These hardware devices have restricted potential exposure to the assailant. In such a scenario, replacing each affected module is not possible; hence, a mechanism is needed to tackle such problems as network layer attacks and application layer attacks. Many issues and related challenges are linked with IoT interoperability and security [4]. Similarly, the study [24] identified that IoT/CPS systems are not understood completely relative to traditional ones, as these are widely distributed in an uncontrolled manner. The IoT environment is an amalgamation of heterogeneous technologies, various protocols, and processes. Moreover, in IoT systems, there is no standard, stable architecture, nor security mechanism present to integrate different systems. Consequently, varied addressing formats and models introduce complexity in IoT systems, creating the issue of interoperability. Another concern in the IoT environment is the presence of nodal platforms with controlled electrical power, limited memory, and low computational power, which are therefore incapable of incorporating heavy firewalls, ultimately giving rise to security concerns [24].

The study in [25] provided a detailed aspect of the vulnerabilities and thus security weaknesses found in each IoT layer and offered blockchain-enabled solutions. Cybersecurity aims at providing confidentiality, integrity, and authentication as three main aspects of tackling cyber attacks and ensuring the protection of cyber–physical systems. In the context of IoT, confidentiality indicates that data packets are not seized and peeked into, or that the host is not compromised so that an unauthorized person can attain sensitive data, information, or credentials. Integrity ensures that data received or sent are not modified in any unauthorized way. Availability is about all the modules in the system that are working properly and are not prohibited from proper functioning in case the module is infected by some malicious agent or intrusion. It thus ensures disinfecting the device immediately and not operating in a compromised way [25].

The authors in [26] worked on factors improving security to ensure CIA goals. To strengthen security, it is recommended to divide IoT devices into those that need direct Internet connectivity into network

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

segments and those that should be forbidden network access. The network segment should be kept under monitoring for any potential unexpected traffic and be subjected to the necessary response [26]. The study in [8] focused on efficient message filtering for privacy-preserving authentication and secure packet forwarding for aggregated transmission evidence generation. Privacy of identification, location, input, output privacy, and function privacy is required for IoT security. Secure IoT cloud systems are dependent on trustworthiness, resiliency, language, coding method, data validation and handling, and dependability. Another study [27] presents an approach where digital identity management is enabled by blockchain. Consequently, there is no need for a central authority and blockchain can be enabled to hide or share IDs. Blockchain implements distributed authority and creates secure layers to avoid record tampering. In the Metaverse, the digital world is relying on blockchain technology to solve confidentiality, integrity, and authentication-related problems [25]. The authors in [9] discussed different modules and their functionality present in smart homes [28,29] and outlined the transactional methods associated with the smart home. They also proposed the metrics for efficiency in terms of processing time traffic and energy consumption. Integrity, confidentiality, and availability are ensured as security goals. The study in [15] proposed an Ethereum-based distributed smart contract in replace of the orthodox centralized system to tackle DDoS attacks. This was achieved by giving resources to each device and enabling the proposed system to distinguish between untrusted and trusted devices.

The study in [30] investigated the vulnerability aspects of IoT networks regarding DDoS attacks. Furthermore, how they affect the services, blockchain methods for tackles DDoS attacks, and the challenges in integrating IoT and blockchain were also analyzed. In [31], the authors developed an algorithm that mines consumer behavior data exclusively and applied machine learning models to advise activities for optimal energy consumption at homes. The algorithm may be utilized for energy optimization in smart homes without reducing the comfort of the occupants. The digital-STROM home automation system's event data are analyzed by the system for recurring and periodic patterns. These patterns are transformed into association rules, given a priority order, and compared to the inhabitants' recent behavior. The system makes a recommendation to the occupants if it finds ways to conserve energy without reducing comfort. An assortment of test homes were placed under the system's deployment. The test subjects had the option of rating how the advice affected their level of comfort. During a second test phase, the system's parameters were modified based on this feedback to increase accuracy [31]. For resource-constrained IoT devices, a high computing power is needed. Cryptographic techniques in blockchain consume higher power, which is a big challenge for blockchain technology. For blockchain to offer the appropriate level of security and anonymity, asymmetric encryption methods are crucial [32]. PoS has been regarded as more secure and energy-efficient than PoW. The Ethereum platform, which is a well-known blockchain application, uses PoS. Ethereum is the first platform to make the use of smart contracts possible. The Ethash function is used by Ethereum-based coins to implement the Keccak hash function [32].

3. Proposed System Design

Activity diagrams are graphical representations of Workflows of stepwise activities and actions with support for choice, iteration, and concurrency.

In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control as shown in Figure 1.

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

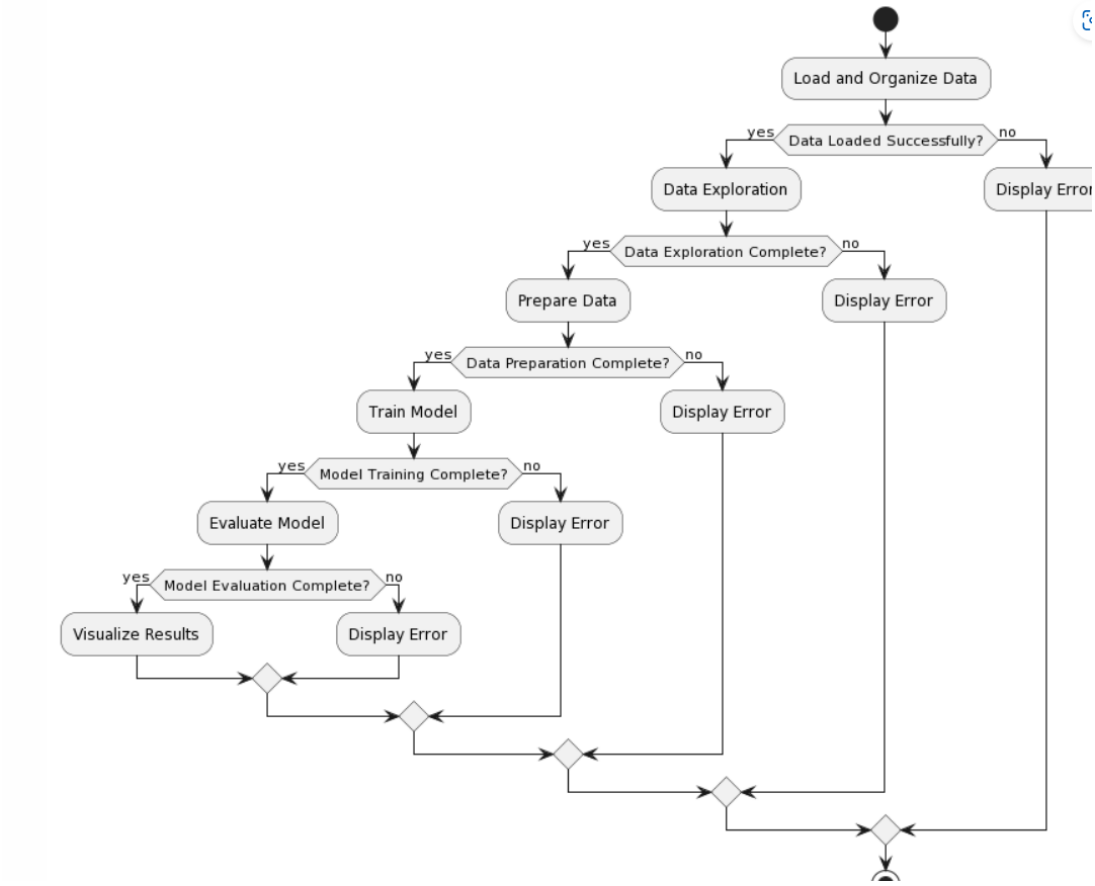

Figure 1. Proposed system design.

3.1 ANN model

ANNs are a network with automatic adjustment of network parameters, which can iteratively calculate data according to the set coordinates and models. The training process of deep learning model is actually a process of constantly tuning the ownership values of nodes which are all used as tools to describe data features. The key to whether the model can describe the features of things lies on the final training results of each weight. The ANN takes the neural network as the carrier and focuses on the depth. It can be said to be a general term, including the recurrent neural network with multiple hidden layers, the all-connected network and the convolutional neural network. Recurrent neural networks are mainly used for sequence data processing and have a certain memory effect. The long-term and short-term memory networks derived from them are better at processing long-term dependencies. Convolutional neural networks focus on spatial mapping. And image data is particularly suitable for feature extraction of various networks. When the input data is dependent and sequential, the results of CNN are generally not good. There is no correlation between the previous input of CNN and the next input. The RNN network appeared in the 1980s. It is designed a different number of hidden layers. Each hidden layer stores information and selectively forgets some information. In this way, the data characteristics of the sequence changes of the data can be extracted. RNN has not only achieved many results in the fields of text processing and speech processing, but also been widely used in the fields of speech recognition, machine translation, text generation, sentiment analysis, and video behavior recognition. Therefore, this paper will use RNN modelling to predict the risk of abnormal blood lipids in steel workers. The RNN is good at processing time series data and can describe the context of the data on the time axis.

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

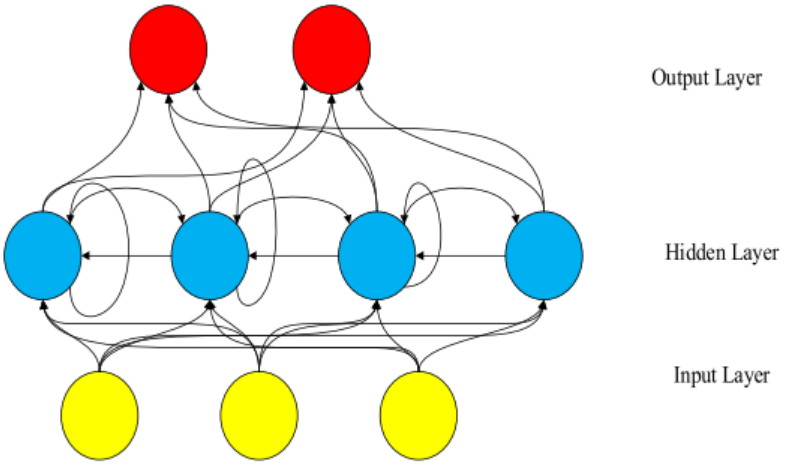

Figure 2: RNN using ANN

As can be seen from the figure above, the RNN structure is relatively simple. It mainly consists of an Input Layer, a Hidden Layer, an Output Layer, and an arrow in the Hidden Layer represents the cyclic update of data, which is the method to realize the time memory function. The input levels of this paper were: age, BMI, marital status, education level, family income, alcohol consumption, smoking, exposure to high temperature, noise, shift work. The 10-dimensional data were normalized and input into the RNN model. After the extraction of hidden layer depth features, the output layer output the sequence of lipid health status, in which 1 represented normal lipid status and 0 represented abnormal lipid status.

FORWARD PROPAGATION OF RNN: Figure 4.3 shows the hierarchical expansion of the Hidden Layer. T −1, t, t +1 represent the time series. X represents the input sample. St represents the memory of the sample at time t. W represents the weight of the input. U indicates the weight of the input sample at this moment, and V indicates the weight of the output sample.

$$s_t = f\,(W * s_{t-1} + U * x_t)$$

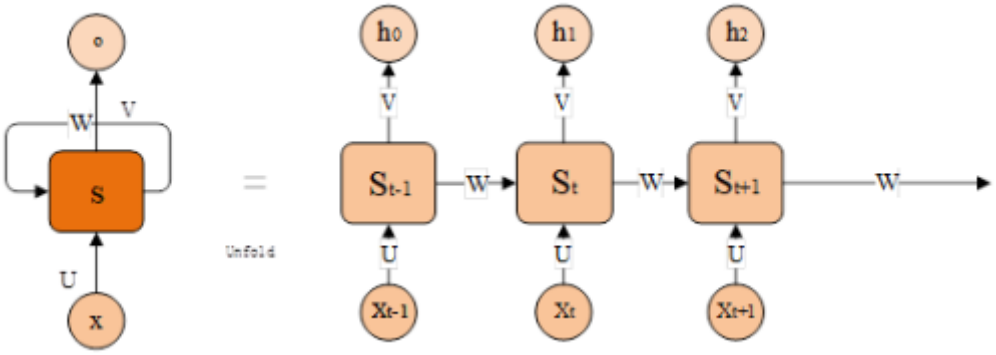

Figure 3: Forward Propagation in RNN

At time t = 1, generally initialize the input, randomly initialize W, U, V, and perform the following formula calculation:

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

$$h_1 = Ux_1 + Ws_0$$
$$s_1 = f(h_1)$$
$$o_1 = g(Vs_1)$$

Among them, f and g are activation functions, where f can be activation functions such as tanh, ReLU, sigmoid. G is usually a SoftMax function. Time advancing, the state s1 as the memory state of time 1 will participate in the prediction activity of the next time, that is:

$$h_2 = Ux_2 + Ws_1$$
$$s_2 = f(h_2)$$
$$o_2 = g(Vs_2)$$

And so on, the final output value can be obtained as:

$$h_1 = Ux_t + Ws_{t-1}$$
$$s_t = f(h_t)$$
$$o_t = g(Vs_t)$$

Here, W, U, and V are equal at every moment which is weight sharing.

BACK PROPAGATION OF RNN: The back propagation process of RNN is the updating process of weight parameters W, U, and V. Each output value o_t will produce an error value E_t, tanh the total error value can be expressed as: Since the output of each step depends on not only the network of the current step but also the state of the previous steps, the Backpropagation Through Time (BPTT) algorithm is used to pass the error value at the output back, and the gradient descent method is used to perform the weight update.

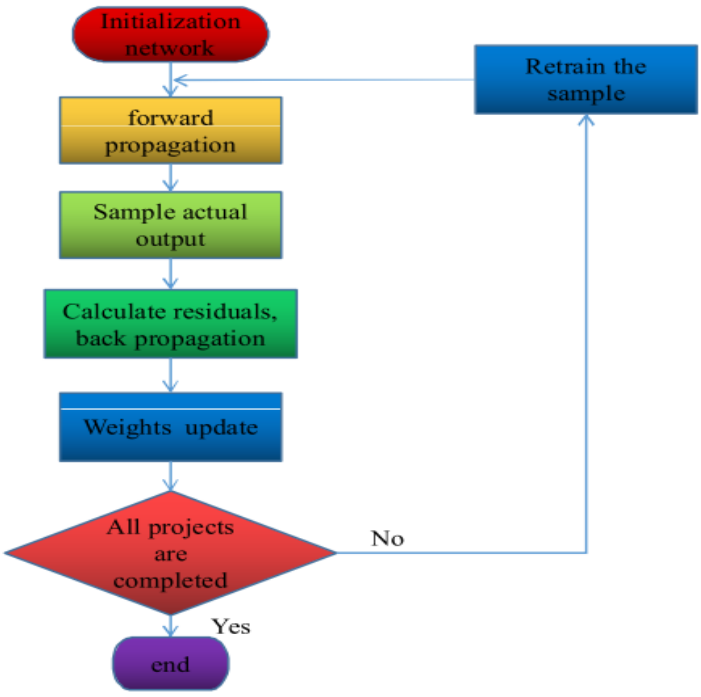

Figure 4: RNN training process.

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

4. Results and Description

The figure below displays a subset of the original dataset that is being used for fog and energy prediction. It shows a few rows or samples of the data.

DateTime	TotalUsage	Month	TemperatureF	Humidity	Hour_y	Minute_y	Day_y	Holiday
2016-01-01 00:00:00	19.843233	1	50.0	63.0	0	0	6	0
2016-01-01 01:00:00	18.462483	1	49.8	63.0	1	60	6	0
2016-01-01 02:00:00	17.414167	1	48.9	61.0	2	120	6	0
2016-01-01 03:00:00	15.914683	1	48.6	61.0	3	180	6	0
2016-01-01 04:00:00	19.195933	1	47.7	63.0	4	240	6	0
...	...	...	...	...	...	...	...	...
2017-12-31 13:00:00	23.331300	12	38.5	90.0	13	780	1	0
2017-12-31 14:00:00	25.814400	12	37.2	84.0	14	840	1	0
2017-12-31 15:00:00	29.153450	12	36.1	84.0	15	900	1	0
2017-12-31 16:00:00	30.285350	12	35.4	84.0	16	960	1	0
2017-12-31 17:00:00	33.841383	12	34.2	84.0	17	1020	1	0

17429 rows × 8 columns

Figure 5: sampled dataset used for Fog and energy prediction

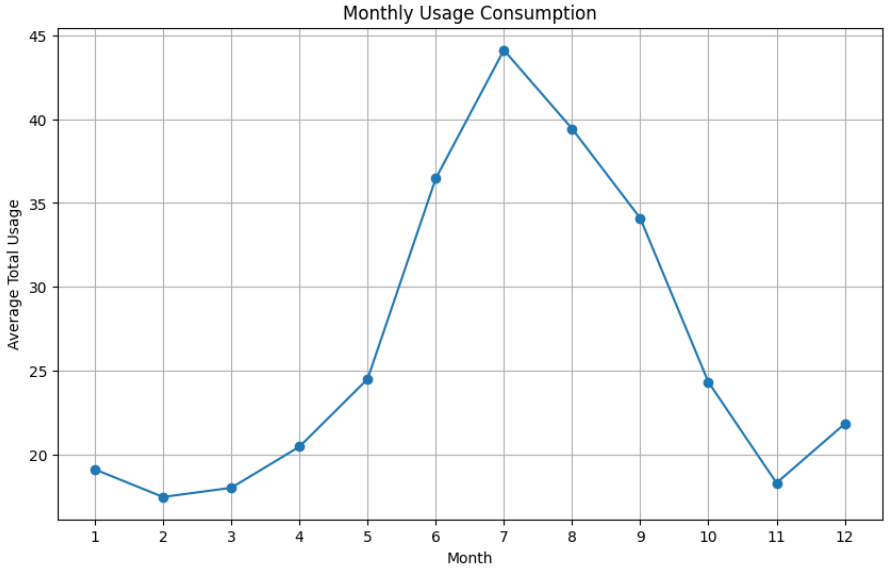

Figure 6: line plot for visualising monthly energy consumption

```
Model: "sequential_1"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
lstm_1 (LSTM)                (None, 20)                2320
_________________________________________________________________
dense_1 (Dense)              (None, 1)                 21
=================================================================
Total params: 2,341
Trainable params: 2,341
Non-trainable params: 0
_________________________________________________________________
None
ERROR! Session/line number was not unique in database. History logging moved to new session 4366
```

Figure 7: Summary of a proposed model

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

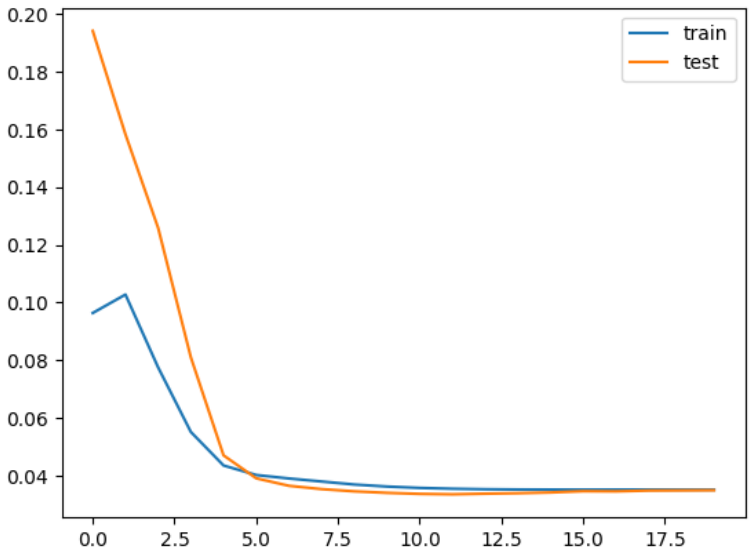

Figure 8: Line plot of the training and testing loss of a machine learning model

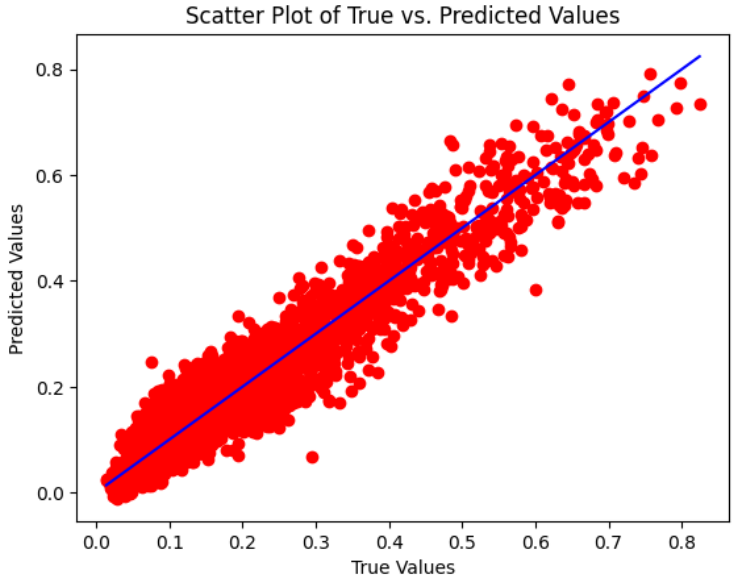

Figure 9: Prediction results of proposed model

5. Conclusion

In conclusion, the integration of Artificial Neural Networks (ANNs) with Edge and Fog Computing for energy prediction represents a promising and innovative approach to address the pressing challenges in sustainable energy management. This project has demonstrated that ANNs, with their ability to automatically learn and extract patterns from data, can overcome the limitations of traditional methods for energy prediction. By leveraging the computational power and real-time processing capabilities of Edge and Fog environments, this approach offers more accurate and reliable energy consumption forecasts. It is particularly crucial in the context of modern smart grid systems and Internet of Things (IoT) applications, were rapidly changing energy consumption patterns and large-scale data processing demand sophisticated solutions. The successful implementation of this method has the potential to revolutionize energy management systems, leading to optimized resource allocation, improved energy efficiency, and cost reduction, ultimately contributing to sustainability efforts and a greener future.

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

References

[1]. Akbari-Dibavar, A.; Nojavan, S.; Mohammadi-Ivatloo, B.; Zare, K. Smart home energy management using hybrid robust-stochastic optimization. Comput. Ind. Eng. 2020, 143, 106425.

[2]. Al-Qerem, A.; Alauthman, M.; Almomani, A.; Gupta, B. IoT transaction processing through cooperative concurrency control on fog–cloud computing environment. Soft Comput. 2020, 24, 5695–5711.

[3]. Ammi, M.; Alarabi, S.; Benkhelifa, E. Customized blockchain-based architecture for secure smart home for lightweight IoT. Inf. Process. Manag. 2021, 58, 102482.

[4]. Balogh, S.; Gallo, O.; Ploszek, R.; Špaček, P.; Zajac, P. IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques. Electronics 2021, 10, 2647.

[5]. Bansal, S.; Kumar, D. IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. Int. J. Wirel. Inf. Netw. 2020, 27, 1–25.

[6]. Smart Home Dataset | Kaggle. Available online: https://www.kaggle.com/code/offmann/smart-home-dataset (accessed on 26 October 2022).

[7]. Chen, S.W.; Chiang, D.L.; Liu, C.H.; Chen, T.S.; Lai, F.; Wang, H.; Wei, W. Confidentiality protection of digital health records in cloud computing. J. Med. Syst. 2016, 40, 124.

[8]. Deshpande, V.M.; Nair, M.K.; Bihani, A. Optimization of security as an enabler for cloud services and applications. In Cloud Computing for Optimization: Foundations, Applications, and Challenges; Springer: Cham, Switzerland, 2018; pp. 235–270.

[9]. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.

[10]. Fakhri, D.; Mutijarsa, K. Secure IoT communication using blockchain technology. In Proceedings of the 2018 International Symposium on Electronics and Smart Devices (ISESD), Bandung, Indonesia, 23–24 October 2018; pp. 1–6.

[11]. Gillis, A.S. What Is IoT (Internet of Things) and How Does It Work? 2021. Available online: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (accessed on 4 March 2021).

[12]. Hosseinian, H.; Shahinzadeh, H.; Gharehpetian, G.B.; Azani, Z.; Shaneh, M. Blockchain outlook for deployment of IoT in distribution networks and smart homes. Int. J. Electr. Comput. Eng. 2020, 10, 2787–2796.

[13]. Autonomic interoperability manager: A service-oriented architecture for full-stack interoperability in the Internet-of-Things. ICT Express 2021, 8, 507–512. [CrossRef]

[14]. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.H. Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals. Sensors 2020, 20, 2195.

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

[15]. Javaid, U.; Siang, A.K.; Aman, M.N.; Sikdar, B. Mitigating loT device based DDoS attacks using blockchain. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 15 June 2018; pp. 71–76.

[16]. Khan, Z.A.; Zafar, A.; Javaid, S.; Aslam, S.; Rahim, M.H.; Javaid, N. Hybrid meta-heuristic optimization based home energy management system in smart grid. J. Ambient. Intell. Humaniz. Comput. 2019, 10, 4837–4853.

[17]. Saraf, C.; Sabadra, S. Blockchain platforms: A compendium. In Proceedings of the 2018 IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, Thailand, 11–12 May 2018; pp. 1–6.

[18]. Ghosh, B.C.; Bhartia, T.; Addya, S.K.; Chakraborty, S. Leveraging Public-Private Blockchain Interoperability for Closed Consortium Interfacing. In Proceedings of the IEEE INFOCOM 2021—IEEE Conference on Computer Communications, Vancouver, BC, Canada, 10–13 May 2021; pp. 1–10.

[19]. Peng, Z.; Xu, J.; Chu, X.; Gao, S.; Yao, Y.; Gu, R.; Tang, Y. VFChain: Enabling Verifiable and Auditable Federated Learning via Blockchain Systems. IEEE Trans. Netw. Sci. Eng. 2022, 9, 173–186.

[20]. Gao, S.; Peng, Z.; Tan, F.; Zheng, Y.; Xiao, B. SymmeProof: Compact Zero-Knowledge Argument for Blockchain Confidential Transactions. IEEE Trans. Dependable Secur. Comput. 2023, 20, 2289–2301.

[21]. Li, Z.; Gao, S.; Peng, Z.; Guo, S.; Yang, Y.; Xiao, B. B-DNS: A Secure and Efficient DNS Based on the Blockchain Technology. IEEE Trans. Netw. Sci. Eng. 2021, 8, 1674–1686.

[22]. Wu, H.; Peng, Z.; Guo, S.; Yang, Y.; Xiao, B. VQL: Efficient and Verifiable Cloud Query Services for Blockchain Systems. IEEE Trans. Parallel Distrib. Syst. 2022, 33, 1393–1406.

[23]. Wang, H.; Xu, C.; Zhang, C.; Xu, J.; Peng, Z.; Pei, J. vChain+: Optimizing Verifiable Blockchain Boolean Range Queries. In Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE), Kuala Lumpur, Malaysia, 9–12 May 2022; pp. 1927–1940.

[24]. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. Internet Things 2018, 1, 1–13.

[25]. Mohanta, B.K.; Jena, D.; Ramasubbareddy, S.; Daneshmand, M.; Gandomi, A.H. Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet Things J. 2020, 8, 881–888.

[26]. Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Security and privacy for cloud-based IoT: Challenges. IEEE Commun. Mag. 2017, 55, 26–33.

[27]. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet Things 2020, 11, 100227.

[28]. Altaf, A.; Abbas, H.; Iqbal, F.; Khan, M.M.Z.M.; Daneshmand, M. Robust, Secure, and Adaptive Trust-Oriented Service Selection in IoT-Based Smart Buildings. IEEE Internet Things J. 2021, 8, 7497–7509.

ISSN: 0975-3583,0976-2833 VOL14, ISSUE 10, 2023

[29]. Altaf, A.; Abbas, H.; Iqbal, F.; Derhab, A. Trust models of internet of smart things: A survey, open issues, and future directions. J. Netw. Comput. Appl. 2019, 137, 93–111.

[30]. Shah, Z.; Ullah, I.; Li, H.; Levula, A.; Khurshid, K. Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. Sensors 2022, 22, 1094.

[31]. Zehnder, M.; Wache, H.; Witschel, H.F.; Zanatta, D.; Rodriguez, M. Energy saving in smart homes based on consumer behavior: A case study. In Proceedings of the 2015 IEEE First International Smart Cities Conference (ISC2), Guadalajara, Mexico, 25–28 October 2015; pp. 1–6.

[32]. Abed, S.; Jaffal, R.; Mohd, B.J.; Al-Shayeji, M. An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. Clust. Comput. 2021, 24, 3065–3084.

[33]. Seok, B.; Park, J.; Park, J.H. A lightweight hash-based blockchain architecture for industrial IoT. Appl. Sci. 2019, 9, 3740.

[34]. Raj, A.; Maji, K.; Shetty, S.D. Ethereum for Internet of Things security. Multimed. Tools Appl. 2021, 80, 18901–18915.

[35]. Moniruzzaman, M.; Khezr, S.; Yassine, A.; Benlamri, R. Blockchain for smart homes: Review of current trends and research challenges. Comput. Electr. Eng. 2020, 83, 106585.