Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol.44 No. 6 (2023)

Smart Home Security Using Internet of Things, Deep Learning, and Blockchain Technology

Vivek R.[1], Varshini J.[1], Shubhashree T. K.[1], Ajil A. Varghese[1], Akila L.[1], Rajkumar N.[2*]

[1]*Department of Computer Applications, Krupanidhi Degree College, Bengaluru, Karnataka, India*

[2]*Department of Computer Applications, Krupanidhi College of Management, Bengaluru, Karnataka, India*

Abstract

The number of instances spotted in which the security of various residences has been compromised. These breaches are not just the consequence of theft but also the faults of domestic appliances like gas cylinders and electricity. Some of these appliances have been known to cause these problems. To mitigate the effects of this issue, we must equip our houses with the most cutting-edge technology to be both functional and safe. The main aim of this study is to safeguard homes using IoT, improve home security, and lower the likelihood of adverse effects from security breaches and malfunctions of household appliances. A wide range of technological systems, methods, and fields of study, such as the Internet of Things (IoT), Raspberry PI, Hidden Markov Model, Deep Extreme Learning Machines, and Deep Learning Neural Networks, were investigated. In the past, several technological advancements have assisted in making homes more intelligent by deploying the appropriate technology and monitoring various activities within the home when the user is away from the premises. We will be able to monitor a wide variety of activities taking place within the house. In addition, improved technological efficiency, as well as more developed inventions in the field of smart homes will be proposed because of this research. This research aimed to enhance residential safety and address the rising concerns over security breaches and the malfunctioning of domestic goods. This study investigated novel strategies for securing home properties using cutting-edge technologies such as the Internet of Things (IoT), Raspberry Pi, the Hidden Markov Model, Deep Extreme Learning Machines, Deep Learning Neural Networks, and blockchain technology.

Keywords: *smart home, security breaches, Raspberry Pi, hidden Markov model, deep learning neural network, blockchain*

Introduction

Kevin Ashton first mentioned the Internet of Things (IoT) in his 1999 presentation on the supply chain [1]. Due to the proliferation of IoT, traditional homes are giving way to smart, networked homes. In a "smart home," [2] residents have simple access to and control over numerous high-tech features, such as voice assistants, thermostats, lighting, motion sensors, cameras, doorbells, locks, etc. The smart home is an essential application of the IoT because its components can be remotely monitored and managed. Adding a smart home system may increase the residents' comfort and independence, which is an important objective. Thanks to beneficial features like behavior monitoring and risk assessments, they have gained popularity among users and device manufacturers. Smart homes have numerous advantages but are also susceptible to intrusions that could imperil the owners' safety and privacy [3]. As the prevalence of smart devices increases, many security experts are concerned about their impact on home safety. The potential of edge computation to resolve this issue merits investigation. Focusing on the "things" aspect of computing, "edge computing" [4] refers to a type of technology that facilitates computation at the network's periphery. "edge" facilities are any data processing facilities located between data producers and cloud storage facilities. In contrast to cloud computing, Edge computing can meet

low bandwidth costs, low latency, and data security requirements. IoT aims to enhance individuals' quality of life by streamlining business processes across multiple industries. The Raspberry Pi is used to build a home monitoring system with real-time reporting capabilities. The low cost, minimal power consumption, and availability of open-source software make Raspberry Pi an attractive option for application development [5]. In the 21st century, the Internet of Things will revolutionize many industries. Thanks to embedded cyber-physical systems, physical objects can be remotely monitored, managed, and accessed. Although the objects are not computers, they contain computers. Satoshi Nakamoto, an enigmatic programmer, devised the blockchain in 2008 [7]. The blockchain is a distributed database that permanently documents transactions without the risk of forgery. More universities are studying blockchain than any other topic [8]. It is a distributed, immutable digital ledger secured by cryptography [9]. It is a reliable central hub for TXs that do not require third parties. A cryptographic signature may be used to validate the blockchain of each request. Since all system participants create and maintain the ledger equally, blockchain stores tamper-proof and immutable data securely and encrypted [10]. Due to the peer-to-peer nature of blockchain, any user can join the network. Any node/user that connects to the blockchain will obtain a copy of the blockchain immediately. Each newly created block is added to the growing list at the end of the chain following verification that it has not been tampered with. The network nodes concur on the block's legitimacy to ensure its integrity. Other network nodes compare the requested block to their copy of the blockchain and reject any blocks that have been altered. Proof-of-Work (PoW) is the consensus among validating nodes that a block has been verified successfully [9]. This algorithm aims to validate transactions (TXs) and add new entries to the blockchain. PoW relies on random computations, necessitating much computer power and quick hardware to solve the complex cryptographic problem (required number of preceding zeros in hash configurations). If an adversary has a supercomputer capable of solving cryptographic puzzles in record time, they can manufacture new blocks and seize network control. "Machine learning" refers to instructing computers to learn, reason, and act autonomously [3]. It is a framework for artificial intelligence. The primary objective of machine learning is to develop efficient algorithms for evaluating and altering outputs considering predictions generated from input data. Machine learning can determine and derive conclusions from vast amounts of data. Deep Extreme Machine Learning (DEML) technique to enhance the efficacy and safety of IoT-enabled sensors in smart residences. This study makes a significant contribution by evaluating the state-of-the-art technologies related to blockchain-based smart homes enabled by the DEML and by providing a fresh perspective on various applications (such as smart home data sharing).

Internet of Things for Smart Home

Internet of Things (IoT) has become the driving force behind the inter-networking of physical objects, devices, and objects with communication capabilities (collectively known as "connected devices" or "smart devices"), such as automobiles, buildings, and other items equipped with electronics, actuators, sensors, software, and network connectivity that can collect, exchange, store, and analyze data. The IoT and the technologies that support it make connecting many different categories of devices possible without interrupting data transmission. In addition, the IoT offers unrestricted access to specialized data sets that can influence the development of exhaustive analytic tools. The wide variety of devices, sensors, network connectivity protocols, actuators, data transfer protocols, and associated services integral to designing and implementing IoT-based innovative systems makes designing and developing a general architecture for these systems challenging. "Smart Home" is an example of how IoT technology can enhance people's daily lives by integrating information technology and services over a private network in their residences. The smart home system can be monitored and controlled more precisely using various technologies embedded in multiple devices. This means that routine domestic tasks can be automated without human intervention or a remote control, resulting in increased productivity, security, comfort, and cost savings. A "Smart Home" [11] is a domicile equipped with several cutting-edge technologies, including but not limited to automated lighting and temperature control, a high-definition television, a computer, a mobile phone, an audio and video system, and a security camera or systems. All components in a smart home are networked together and can be remotely controlled using a smartphone or the internet. A "Smart Home" is a residence that uses sensors and Internet of Things-enabled technology to ensure the residents' health, safety, comfort, and cost-efficiency. A smart home's highly developed and advanced technology, such as automated door openers and a smart light management system, substantially improves the fundamental functionality of home appliances and offers

numerous practical advantages. IP-enabled smart cameras, object motion sensors, smart door locks, and security alarms can significantly improve the security of a residence. Regarding automated homes, cutting-edge, one-of-a-kind technology is necessary to provide a constant, everywhere connection between sensors, actuators, and home appliances in a secure setting. To overcome this issue, we can utilize the Internet of Things [12].

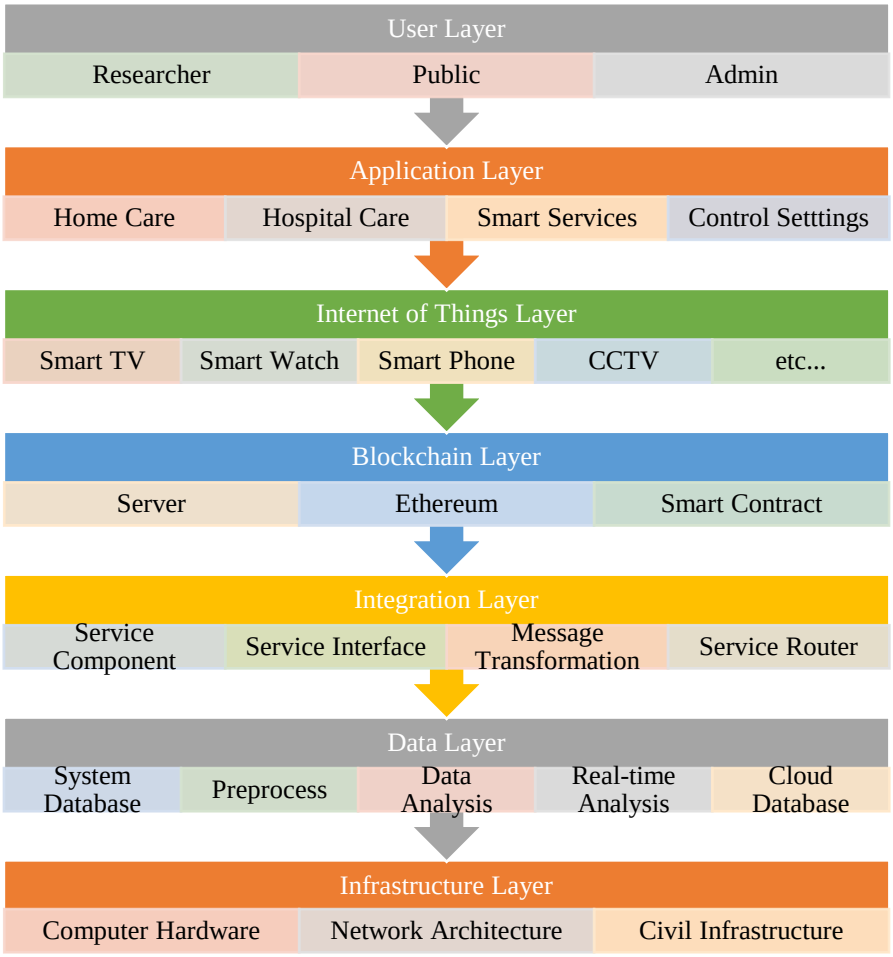

Fig. 1. Proposed Deep Extreme Machine Learning Architecture Diagram

Machine Learning for Smart Home

Deep Extreme Machine Learning (DEML) could be utilized for many purposes, including predicting health issues, predicting energy consumption, planning, and managing transportation networks. [13]. Existing techniques for Artificial Neural Networks (ANN) can be reconstructed, have protracted learning cycles, and require substantial modifications. Huang et al. [14] define "extreme machine knowledge." Due to its rapid learning and high success rate during procedural convolution, DEML has the potential to be applied to a variety of classification and regression tasks. Even though the extreme machine learning is a feedforward neural network, which implies that data travels only in one direction along a series of layers, we used the backpropagation approach to learning in this proposed system, in which data flows backward through the network the neural network adjusts the weights to achieve high accuracy with minimal error rate. The network weights are held constant while the trained model is extracted, and predictions are made using the actual data. Three layers comprise the proposed DEML strategy: the input, concealed, and output layers. The input, concealed, and output layers form the DEML structure. DEML uses many hidden layers and a constant number of neurons to train the dataset. In contrast, the other type, an "extreme learning machine," uses a single hidden layer and many neurons, increasing the network's hidden layers while maintaining the total number of neurons. DEML's backpropagation and feed-forward algorithms were integrated to reduce the error rate, and the network's weights were fine-tuned. In terms of precision, the DEML framework outperforms other machine learning approaches. To improve the security of smart homes, the

evaluation layer monitors several parameters, such as accuracy, failure rate, specificity, sensitivity, positive prediction value, and false positive value. The backpropagation technique involves establishing initial weights, disseminating them forward, propagating errors backward, and revising the model's ability to distinguish itself. In the buried layer, each neuron is activated using a sigmoid function. To construct the sigmoid input function and the DEML hidden layer, it is beneficial to calculate the square root of the difference between the desired output and the actual output. The weights must be rebalanced to rectify this prevalent error.

Blockchain for Smart Home

The Internet of Things (IoT) information layer collects data from connected devices to evaluate smart homes, environments, and individuals. This technology is predominantly employed in sensors, multimedia, and medical devices. The atmospheric condition is measured using sensors. Using the thermostat, you can monitor and adjust the temperature in your residence, for instance. The IoT sensor network's blockchain layer comprises surveillance cameras, wearable electronics, and other sensors. The foundation of any structure is a repository or database, such as a blockchain, that holds aggregated data from multiple nodes. The Deep Extreme Machine Learning (DEML) computation technology is helpful for blockchain-based applications. DEML can be used to increase the security of the distributed ledger. By providing more communication channels, DEML may also prolong the negotiation process. Moreover, the decentralized nature of blockchain technology presents an opportunity to improve framework development. We introduced the DEML implementation architecture depicted in Figure 1 for use in blockchain-enabled smart technologies. The application collects data from various sensors and sources, including cameras, smart devices, and IoT infrastructure. Tests of "smart" software incorporated implementations of these findings. With blockchain technology, these cutting-edge software applications can be developed. Using the DEML framework, such application data can be understood (via data analysis and real-time analysis) and predicted. Data sets generated on a blockchain are processed using DEML models. Data errors such as repetition, absent values, inconsistencies, and noise are reduced as much as possible. By distributing data across a blockchain, the DEML system mitigates information-related issues. The DEML framework requires only a limited subset of the data to function effectively. This may necessitate the development of specialized frameworks for purposes such as detecting fraud and preventing identity theft. The blockchain concept has three primary components that augment the fundamental infrastructure of the IoT. The three primary components of this system are the blockchain infrastructure, the smart contract, and the DEML. The proposed DEML system relies heavily on concealed layers, neurons, and triggering mechanisms to ensure the utmost level of smart home security. The proposed methodology comprises data collection, processing, and analysis. The evaluation layer includes both the prediction and performance evaluation layers. To conduct experiments, precise sensor data and actuatable actuators are required - the collected information functions as input for the acquisition layer. The initiation of specialized data cleansing and planning tools has eliminated preprocessing layer knowledge inconsistencies. The DEML was implemented to protect the smart home network from application-layer attacks. Hash values serve as the cryptographic adhesive between blocks. A home server system may be considered a miner for validating new transactions and creating new partnerships, whereas smart contracts adhere to predetermined laws to facilitate decentralized transactions. Public, proprietary, and federated blockchains all have their place, but for a highly developed home network, the most cost-effective option is a private blockchain controlled by a single business.

Discussion

The Internet of Things (IoT) information layer collects data from connected devices to evaluate smart homes, environments, and individuals. In a sensor network for the IoT, devices like CCTV cameras and wearable electronics comprise the blockchain layer. The foundation of any structure is a repository or database, such as a blockchain, that holds aggregated data from multiple nodes. The DEML computation technology is helpful for blockchain-based applications. DEML can be used to increase the security of the distributed ledger. By providing more communication channels, DEML may also prolong the negotiation process [3]. Proactive processing enhances data quality and reliability by anticipating and eliminating potential sources of error. DEML examined the system's numerous hidden partitions, networks, and activations for indicators of malicious intent [15, 16]. In addition, the number of neurons performing each active function and the number of neurons present in each hidden

layer were evaluated. We evaluated the DEML to predict the efficacy of this method accurately. We utilized analogs of the DEML method to calculate the outcome based on various statistical metrics.

Conclusion

Integrating IoT, Machine Learning, and Blockchain technologies might improve smart homes and other areas. The three pillars of innovation include improving security, comfort, and efficiency in our living spaces. It is essential to recognize that these advances present new problems. Many common devices have been connected through the Internet of Things, resulting in enormous data collection and robust automation systems. IoT technology has made home automation, energy efficiency, and security possible. IoT-enabled devices improve domestic comfort and security, including temperature adjustment and safety. Smart home IoT applications need DEML. In intelligent systems, DEML helps identify health concerns, optimize energy management, and improve mobility. Machine learning algorithms improve smart home living by analyzing large amounts of data and making accurate predictions. Smart homes are safe and reliable thanks to machine learning algorithms that monitor and secure the IoT environment. Blockchain technology's decentralized, unchangeable ledger improves smart home IoT data security. Blockchain security improves data integrity and privacy. Blockchain technology, including smart contracts and decentralized transactions, automates smart home functions and reduces intermediaries. These technologies give a complete smart home solution for the changing environment. The Internet of Things (IoT) collects and distributes data while machine learning algorithms analyze it. Blockchain technology also verifies transactions. Smart houses with several technologies improve efficiency, convenience, security, and privacy. IoT, ML, and Blockchain technologies are changing intelligent home settings and other areas. This technology lets inhabitants live in optimum, safe, and flexible spaces. Smart homes must balance innovation with privacy and security to maximize their potential.

Reference

[1] Ashton, K., 2009. That 'Internet of things' thing. *RFID journal*, *22*(7), pp.97-114.

[2] The statistics portal, statistics and studies from more than 22,500 sources, 2017. Last accessed 27 February 2019.

[3] Khan, M.A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M.I., Nasser, N. and Ali, A., 2020. A machine learning approach for blockchain-based smart home networks security. *IEEE Network*, *35*(3), pp.223-229.

[4] Shi, W., Cao, J., Zhang, Q., Li, Y. and Xu, L., 2016. Edge computing: Vision and challenges. *IEEE internet of things journal*, *3*(5), pp.637-646.

[5] Lee, Y.C. and Lee, C.M., 2020, October. Real-time smart home surveillance system of based on raspberry Pi. In *2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)* (pp. 72-74). IEEE.

[6] Saxena, U., Sodhi, J.S. and Tanwar, R., 2020. Augmenting smart home network security using blockchain technology. *International Journal of Electronic Security and Digital Forensics*, *12*(1), pp.99-117.

[7] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*.

[8] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B., 2019. A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, *7*, pp.82721-82743.

[9] Yaga, D., Mell, P., Roby, N. and Scarfone, K., 2019. Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

[10] Yu, Y., Li, Y., Tian, J. and Liu, J., 2018. Blockchain-based solutions to security and privacy issues in the internet of things. *IEEE Wireless Communications*, *25*(6), pp.12-18.

[11] Razzaque, M.A., Milojevic-Jevric, M., Palade, A. and Clarke, S., 2015. Middleware for internet of things: a survey. *IEEE Internet of things journal*, *3*(1), pp.70-95.

[12] Ray, A.K. and Bagwari, A., 2017, November. Study of smart home communication protocol's and security & privacy aspects. In *2017 7th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 240-245). IEEE.

[13] Abbas, S., Khan, M.A., Falcon-Morales, L.E., Rehman, A., Saeed, Y., Zareei, M., Zeb, A. and Mohamed, E.M., 2020. Modeling, simulation and optimization of power plant energy sustainability for IoT enabled smart cities empowered with deep extreme learning machine. *IEEE Access*, *8*, pp.39982-39997.

[14] Huang, G.B., Wang, D.H. and Lan, Y., 2011. Extreme learning machines: a survey. *International journal of machine learning and cybernetics*, *2*, pp.107-122.

[15] Ray, A.K. and Bagwari, A., 2020, April. IoT based Smart home: Security Aspects and security architecture. In *2020 IEEE 9th international conference on communication systems and network technologies (CSNT)* (pp. 218-222). IEEE.

[16] Rajkumar, N., Rajendra, SV., and Jayavardhan, GV. 2021, Role of IoT and Blockchain in Pharmacy Industry, *International Journal of Biology, Pharmacy and Allied Sciences*, 10(12): 278-286