IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

Network Security

Likhita K M[1], Mr. Nagesh U B[2], Finny Paul[3], Keerthana G[4], Gary Richards[5]
Faculty, Department of Information Science and Engineering[2]
Students, Department of Information Science and Engineering[1,3,4,5]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *Today, nations all over the world are actively supporting the advancement of intelligent agriculture. They must individually grow unique plants that are matched to the area for farming, and this information is crucial and delicate. This is why information-driven, intelligent agriculture needs network security protection to guarantee data privacy and integrity. This study suggests using dark web technology to protect the privacy of servers and blockchains. In intelligent agriculture, packet transfer frequency will be monitored to guard against distributed denial-of-service (DDOS) assaults. The system's key features are: (1) an identity authentication method; (2) secure information transfer; (3) the creation of private blockchains; (4) a quicker, more effective system for blockchain information authentication; and (5) resilience to DDOS attacks. The proposed system can protect network security for IoT devices as well as servers by utilising dark web technology, which can reduce the risk of DDOS attack damage by preventing the visibility of blockchains and server ID addresses. Results from the experiments show that the suggested scheme's use of lightweight encryption does, in fact, speed up authentication while simultaneously meeting network security criteria.*

Keywords: Network Security

I. INTRODUCTION

A smart house is connected to the internet, enabling users to control a number of smart devices, each of which has a crucial function for the user and their family in the home. An intelligent home network is built on the IoT, which links various intelligent gadgets including wearables, smartphones, and smart computers. Making people's houses more open and secure can make their lives easier and safer. Because the smart home offers practical tools like habit tracking and even safety testing, users and system developers have been forced to do in-depth study. These issues can be resolved via unified "cloud-like" computing networks and blockchain-like platforms. Blockchain was created in 2008 by Satoshi Nakamoto and comprises a network of independent networks that controls a time-stamped collection of damaging proof documents.

Data fusion techniques can be useful due to the vast amount of information transferred in complex networks. Many communications can be transformed into accurate and helpful data for the end user by a data fusion procedure. A data fusion method is presented in this article for networks that naturally expand to include a large number of nodes. Recent academic work has covered a wide range of data fusion concepts and methodologies. The most frequently used categories are "data fusion" and "information fusion." Our investigation is just focused on data provided by sensors; we do not also look at data from other sources. In a data fusion method, sensors are used to increase the accuracy of results. By carefully assessing its reliability with regard to the crucial security goals of secrecy, authenticity, and usability, the suggested approach secures the blockchain-based smart home system. In order to support our claim that the overhead produced by our technique is hardly related to the value of the sensitive information's security and privacy, we also evaluate our method's efficiency in protecting sensitive information while consuming very little power. The following sections make up the rest of this article. The survey papers from related studies are included in Section 2. The fundamental blockchain technologies are described in Section 3 along with an RTS-DELM solution for blockchain-based mobile home and smart home application systems. A solution to the RTS-DELM problem is presented in Section 4, which includes using the DELM method's simulation and results. Section 5 concludes by discussing the study's findings gleaned from the specifics.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

II. LITERATURE REVIEW

Blockchain is currently in demand among fans of smart homes, and numerous study publications have been written on the topic. S. Aggarwal et al. [2] examined various facets of healthcare in their study on how blockchain technology would be employed in the smart city, including transaction assimilation, home healthcare, and investment sharing. However, a thorough information analysis of the use of blockchain technology in the smart home has not yet been conducted. The blockchain has several applications in the smart home industry. A thorough analysis of several blockchain implementations for a peer-to-peer resource sharing network was published by M. Andoni et al. [3]. The report provides in-depth details on the implementation and capabilities of various smart home networks, including big data analysis, artificial intelligence (AI), security concerns in the smart grid, and payment systems. They failed to effectively take into account challenges relating to smart homes, such as smart home security and smart city financial planning. A user-based blockchain structure was proposed by Khan et al. [4] to ensure the connectivity of edge information in the Internet of Things. To transfer control and performance of some autos, Z. Zhou et al. [5] investigated distributed computing, contractual analysis, and blockchain technology. In order to recognise dynamic blockchain frameworks, J. Wu et al. [6] proposed a software-specified blockchain interface. They then applied a consent function method to virtual machines with an application-aware system that can extract and manage special consensus resources. Sivaraman et al. [7] addressed security concerns in the networks for smart homes and provided helpful ideas. The smart home equipment must be used in conjunction with an algorithm server to monitor and validate the systems that have been certified. The current standards cannot effectively protect internal user data without eliminating the need to identify users and prohibiting data packets that do not come from the internet. The upgrade handled by Lee et al. [8] offers encryption protocols using a private key, cryptographic certificates that are implemented with shared keys, and software upgrades for embedded systems using a blockchain. For use in smart home applications, this sensor supports secure data collecting, encryption, and queries. As a result, information verification and privacy are promoted. It protects the information that is sent between the user, gateway, network operator, and system. Within the smart home methodology, Hsu et al. [11] suggested a multimodal data fusion mechanism. They created an intelligent smart home environment employing intelligent wearable technology to manage and run the smart home's features. The exponential expansion of Internet of Things (IoT) devices in the modern digital age presents a number of design issues for enterprises in terms of security and privacy. Previous studies suggest that blockchain technology is a critical solution to the IoT's data security issues. Multiple data providers can exchange information securely and reliably using the blockchain technology. IoT data are encrypted and stored in a distributed ledger. [12]. Before suggesting the use of blockchain technology to ensure the security of data kept in sensor networks, Wang et al. [13] examined the security risks associated with data storage in sensor networks. By using a cryptographic accumulator rather than a Merkle hash tree, the approach offers both memberproof and non-memberproof security. Additionally, the present accumulator's limited item capacity cannot accommodate the expanding demands.

2.1 Background

A. Bilinear

Combinations The following are some characteristics of bilinear pairing:

Bilinear: a,b Z q, e = (aP,bP) = e(P,P)ab. • Q G1 is non-degenerate if e(Q,Q) 6 = 1.

Calculable: For all Q G1, there is an effective approach to compute e(Q,Q). This study [22] implements bilinear pairings cryptography, with G1 and data volume being q bits, or 161 bits and 160 bits, respectively. This study uses the bilinear pairings-focused ID-based cryptography (IBC) [23].

Comparatively, multiple data sources can provide more reliable information because the data itself originates from a variety of sources. As a result, results from data fusion methods that combine information from multiple data sources can be more dependable and consistent than those from a single information source. This is how the NSL

The performance of the proposed system was assessed using the KDD [19] and KDD CUP 99 [20] datasets, which were used for data fusion. Every data collection defines a distinct connection that corresponds to a series of packets that move between the provider and target locations in the combined data collection in accordance with a predefined protocol.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

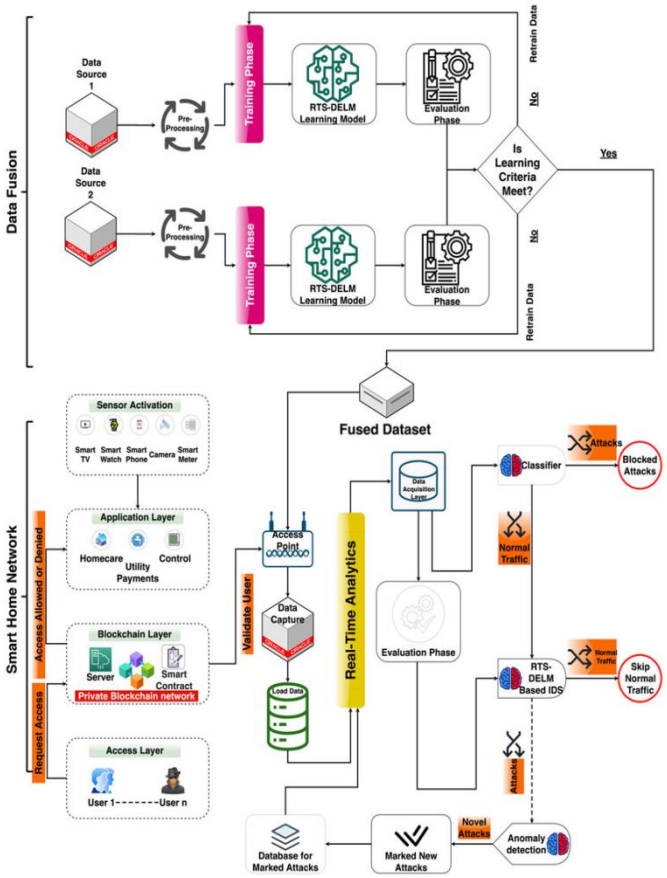


Figure: Proposed blockchain-based smart home network.

There are 41 characteristics per record in this data collection. These features consist of six unique fields and 35 continuous fields. C. Using a Real-Time Sequential Deep Extreme Learning Machine in a Blockchain-Based Smart Home The benefits of implementing RTS-DELM are listed below;

Blockchain provides a high level of trust and protection;

User authentication, a way to lawfully access and conduct transactions on the blockchain network. Blockchain is a reliable way to incorporate an incentive-based mechanism to allow users and consumers to contribute data. Blockchain applications incorporate real-time transaction mechanisms into smart contracts to ensure that the contractual commitments, which were already negotiated, are fulfilled. Furthermore, the RTS-DELM model would be improved with the aid of this huge data. RTSDELM computational technology can be used to make the use of blockchain-based systems smarter. When using the distributed blockchain technology RTS-DELM, data confidentiality can be improved. By exchanging new information and enhancing understanding, RTS-DELM can be utilised to speed up the process of comprehension. It provides the network architecture and foundation needed to create a decentralised blockchain application. In this article, we examine the sophisticated RTS-DELM deployment architecture. Collecting intelligence from many information sources, including sensors, mobile devices, and IoT systems, will be the right use of this technology. Smart apps exploit the knowledge gained by applying these strategies. The fundamental structural component of smart apps is the blockchain. Nevertheless, real-time data can be evaluated and predicted using the RTS-DELM approach for analysis. Additionally, the RTS-DELM model's data may be processed by the blockchain. When creating data for study, mistakes including duplication, missing data parameters, glitches, and noise are minimised. The blockchain is used to communicate knowledge, and the RTS-DELM architecture can be used to minimise data-related problems. When only a small piece of a data collection is required, the RTS-DELM approach can work well. In many different domains, including fraud detection and prevention, the architecture offers a wide range of solutions. The RTS-DELM framework, knowledge architecture, smart contracts, and blockchain layer are the three primary components of the blockchain infrastructure, which focuses on the edge of the Internet of Things (IoT). Large amounts of hidden

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

layers, hidden neurons, and several activating mechanisms have been used in the proposed RTS-DELM system to maximise the security and privacy of smart homes. The proposed method divides the analysis of the data into three stages: data collecting, preparation, and assessment. The prediction layer and the performance layer were the two sub-layers that made up the evaluation layer. Accurate data are gathered from sensors and actuators for analysis. The collection layer uses the data after receiving it as raw data. To eliminate discrepancies in the preprocessing layer, a thorough technique for data cleaning and preparation has been put into place. The RTS-DELM was used to stop disruptive or intrusive programmes, hence maximising the home network's protection. Hash functions used in cryptography link blocks together. One could think of a home server PC as a miner that creates new blocks and verifies new transactions. Contrarily, intelligent contracts adhere to predefined rules to facilitate and speed up decentralised transactions. Blockchains can use a variety of consensus models, including proprietary, public, and federated ones, although private blockchains work better in smart homes.

We provide the following justification for how blockchains will contribute to safe access. • Prior to adding the access level to the home service computer, the consumer must choose it. For instance, the homeowner (Admin) has the greatest degree of authority, but minors, young people, and visitors to close family members require mid-level authorization. • Figure 2 illustrates how blockchain enables secure entrance for a user who has access to the smart home and is utilising applications inside. • Visitors and family members have comparatively limited access rights. The home server verifies repository security access before executing a client request. The home server sends the encrypted login and password to the blockchain layer after getting a customer order. • A blockchain regulation header contains a list of permission requirements for different users and implementations. The policy header is a component of the block data that is used to implement control policies and services. The request for access is examined by the administrator before being approved or denied. Miners respond in accordance with the policy specifics supplied to the header when the data is incorporated into the blockchain. When used against hostile attackers, this approach is effective.

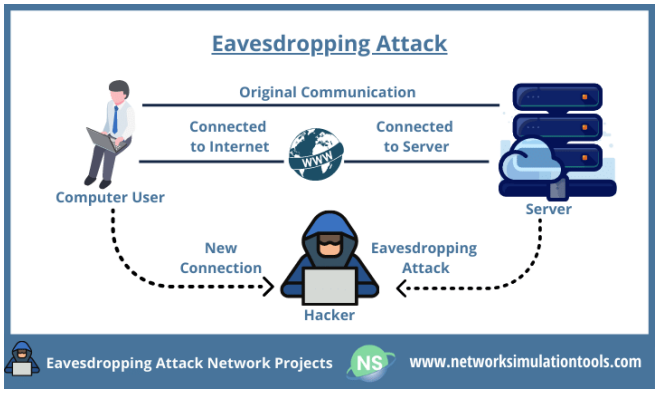


Figure: Eavesdropping by attacking or transmitting information

Through the use of telephone lines, instant messaging via the Internet, video conferencing, and faxing with a listening and change attack, information can be transmitted and, without the user's awareness, heard, changed, and prevented. There are various network analysis protocols that can be used to carry out this assault. CODEC (convert video or audio analogue signal to digital signal and vice versa) quickly converts digital audio to high quality but large volume audio files with the aid of attack software (WAV). The user typically has no idea that this assault is being carried out. The system completes the required tasks quietly and without undue strain. The information was stolen without a shadow of a doubt. Only those who are cognizant of this danger.

III. REAL-TIME SEQUENTIAL DEEP EXTREME LEARNING MACHINE

The optimum method for enhancing smart home networks is RTS-DELM, which includes a range of hidden layers, numerous hidden neurons, and a variety of various activation functions. The three phases of the proposed technique are data collection, review, and presentation. The application layer has two sub-layers: one is for estimating, and the other is for assessment. There are also more levels between these two. Data were gathered via sensors during experiments for observational research. The information gathered by the data gathering system was then made accessible as input to the data gathering system. Numerous data processing methods were employed up until final processing to remove

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

abnormalities from the results. In order to enhance smart home networks and stop disruptive or intrusive activity, the RTS-DELM algorithm was used.

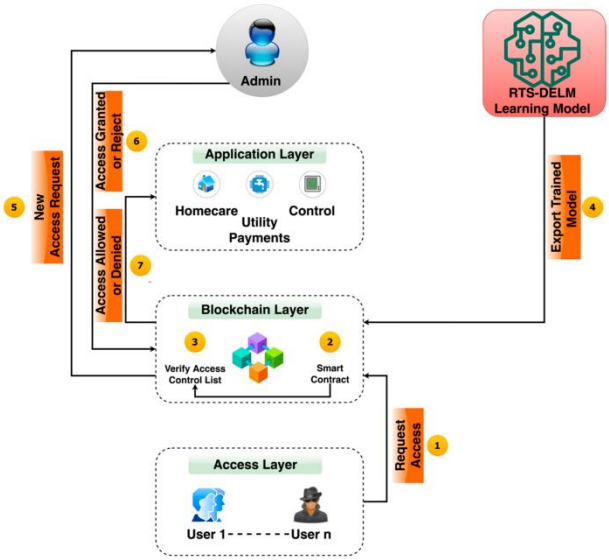


Figure: Proposed blockchain-based smart home management system.

Deep Extreme Learning Machine in tialThe optimum method for enhancing smart home networks is RTS-DELM, which includes a range of hidden layers, numerous hidden neurons, and a variety of various activation functions. The three phases of the proposed technique are data collection, review, and presentation. The application layer has two sub-layers: one is for estimating, and the other is for assessment. There are also more levels between these two. Data were gathered via sensors during experiments for observational research. The information gathered by the data gathering system was then made accessible as input to the data gathering system. Numerous data processing methods were employed up until final processing to remove abnormalities from the results. In order to enhance smart home networks and stop disruptive or intrusive activity, the RTS-DELM algorithm was used. There are many different applications for smart homes that can use the RTS-DELM approach. A sizeable portion of sensor readings is typically needed to maintain the necessary detection accuracy. RTS-DELM uses integrated routing and security techniques to address a number of network access issues. However, taking into consideration that 80% of a proposed blockchain-based smart home management system in Figure 2.

The RTS-DELM method applies to a wide variety of smart home applications. A considerable portion of sensor readings is typically ignored in order to maintain the necessary detection accuracy.

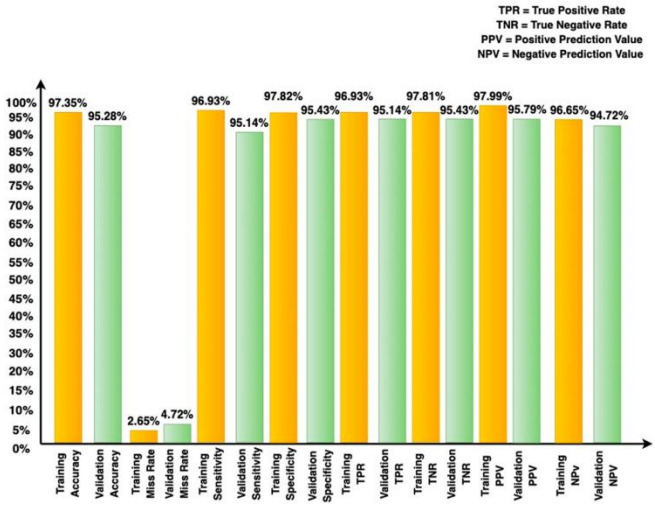


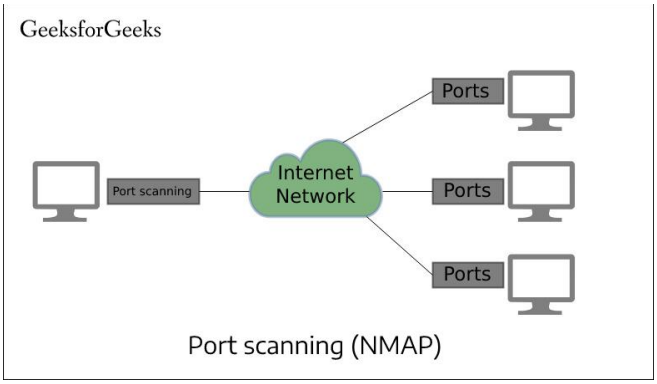
Figure: Statistical measures for the proposed blockchain-based smart home network architecture for the estimation of intrusion with fused dataset during validation and training

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

Evaluates the system model's performance during the training and validation stages in terms of sensitivity, specificity, true positive rate (TPR), true negative rate (TNR), positive predicted value (PPV), and negative predicted value (NPV). As demonstrated in Table 3, the proposed framework provides significantly improved accuracy by reducing the error rate, and we evaluated the dependability of our technique based on the dependability of other published algorithms in the literature. The Generative Adversarial Networks (GANs), Deep Extreme Learning Machine (DELM), and Artificial Neural Network-based Intrusion Detection System all perform worse than the suggested RTS-DELM framework in terms of accuracy.

3.1 Port Scanning

Computers that provide network services are less frequently employed than the attack type of port scan. To ensure network security, we need to focus more on virtual ports. mainly because ports provide a route for data transmission. There are 65,536 standard ports on the machine. Computer ports can be compared to a home's door or window. The raid on the port checkpoints appears to show that the burglars were aware of whether the windows and doors were open or closed before breaking in. It will be simpler for a robber to enter the home if they see the window is open. During an attack, the hacker employs the Ports Check technique to determine whether a port is open or closed.



IV. CONCLUSION

The blockchain technology concept of a smart contract is used in this study to verify the user's identity for access to centralised smart home services. This study's most important contribution is its illustration of how simple it is to obtain facilities and how safe the resources are. Even if another user tries to access a resource that is already in use, no other third-party users can access smart home devices, so redundant authentication is not necessary. A major challenge with smart homes is intrusion detection, particularly in the context of assessment and prediction. Meanwhile, recent developments in the blockchain and machine intelligence fields have shown great promise in achieving these goals. This paper discussed the need for an effective strategy and offered an effective and compact system for intrusion prevention. To optimise multi-sensor networks, an RTS-DELM strategy was created, and data fusion methods were also given. A variety of metrics were employed to evaluate the proposal's viability. The reliability of RTS-DELM results demonstrated that the suggested method is superior to others. The suggested RTS-DELM approach demonstrated 95.28% accuracy, which is an unusually high success rate. The results received are encouraging, and we will keep looking into other uses for the device by deploying more datasets and different frameworks.

Contributions of Authors: M.S.F. and S.K. gathered information from various sources. M.S.F., S.K., and A.R. carried out formal analysis and simulation; M.S.F., S.K., A.R., and S.A. contributed to writing by preparing the initial draught; writing—review and editing; M.A.K. and S.O.H. carried out supervision; M.S.F., S.A. and A.R. carried out revision; and M.A.K. and S.A. carried The manuscript's published form was approved by all authors after they had read it.

Funding: This work was partially funded by the National Research Foundation of Korea (NRF) under Grant 2020R1A2B5B01002145 (50%), and partially by the Institute of Information and Communications Technology Planning and Evaluation (IITP) under the High-Potential Individuals Global Training Program under Grant 2021-0-01532 (50%). (MSIT). Statement from the Institutional Review Board: Not relevant for research involving neither humans nor animals. Not applicable for investigations not involving humans, according to the informed consent

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

statement. Data Availability Statement: Upon request, the corresponding author will provide access to the simulation files/data that were utilised to support the study's conclusions. Conflicts of Interest: The authors say they have none.
The authors appreciate the anonymous reviewers' insightful comments and recommendations on the manuscript. Under Contracts MOST107-2221-E005-029 and 108-2221-E-005-021-MY3, the Ministry of Science and Technology of Taiwan, R.O.C., provided some funding for this work. This research was funded supported by the Information Security Research Center at National Sun Yat-sen University in Taiwan, as well as by the Taiwan Information Security Center (TWISC@NSYSU).

REFERENCES

[1]. Kaufman, Perlman and Speciner, Network Security: Private Communications in a Public World, second edition (Prentice Hall, 2003).
[2]. BS 7799-2 (2002) Information Security Management Systems – Specification with Guidance for Use , British Standards Institution.
[3]. Ellis, J. and Speed, T. (2001) The Internet Security Guidebook, Academic Press. 4. Cheswick and Bellovin, Firewalls and Internet Security, 1/e (Addison-Wesley, 1994; free online for personal use). Second edition with Rubin (Feb.2003).
[4]. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus.Rev. 2008, 10, 21260.
[5]. Aggarwal,S.;Chaudhary,R.;Aujla,G.S.;Kumar,N.;Choo,K.K.R.;Zomaya,A.Y.Blockchainforsmartcommunities: Applications, challenges and opportunities. J. Netw. Comput. Appl. 2019, 144, 13–48. [CrossRef]
[6]. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 2019, 100, 143–174. [CrossRef]
[7]. Khan, M.A.; Abbas, S.; Rehman, A.; Saeed, Y.; Zeb, A.; Uddin, M.I.; Nasser, N.; Ali, A. A machine learning approach for blockchain-based smart home networks security. IEEE Netw. 2020, 35, 223–229. [CrossRef]
[8]. Zhou, Z.; Wang, B.; Dong, M.; Ota, K. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. IEEE Trans. Syst. Man Cybern. Syst. 2019, 50, 43–57. [CrossRef]
[9]. Wu, J.; Dong, M.; Ota, K.; Li, J.; Yang, W. Application-aware consensus management for software-defined intelligent blockchain in IoT. IEEE Netw. 2020, 34, 69–75. [CrossRef]
[10]. A. Almeida, D. Doneda, and M. Monteiro, "Governance challenges for the internet of things," IEEE Internet Comput., vol. 19, no. 4, pp. 56–59, 2015.
[11]. K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet of things: Research challenges and opportunities, "IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3567–3569, 2018.
[12]. T. Qiu, R. Qiao, and D. O. Wu, "Eabs: An event-aware backpressure scheduling scheme for emergency internet of things," IEEE Trans. Mobile Comput., vol. 17, no. 1, pp. 72–84, 2018.
[13]. Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," IEEE Access, vol. 25, no. 6, pp. 12–18, 2018.
[14]. J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2526–2536, 2018.
[15]. J.Granjal,E.Monteiro,andJ.S.Silva,"Securityfortheinternetofthings: A survey of existing protocols and open research issues," IEEE Commun. Surveys Tut., vol. 17, no. 3, pp. 1294–1312, 2015.
[16]. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacyissuesininternet-of-things,"IEEEInternetThingsJ.,vol.4,no.5, pp. 1250–1258, 2017.