SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I5P103

Volume 11 Issue 5, 20-26, May 2024
© 2024 Seventh Sense Research Group®

Original Article

Adaptive Service Dependent Secure Blockchain Model for Improved Security in IoT Networks

R. Premkumar[1], S. Sathyalakshmi[2]

[1,2]Hindustan Institute of Technology and Science, Tamilnadu, India.

[1]Corresponding Author : premkumar.raju@gmail.com

Received: 02 March 2024 Revised: 03 April 2024 Accepted: 02 May 2024 Published: 29 May 2024

Abstract - *The problem of secure routing and data security in Internet of Things (IoT) networks is analyzed, and the nature of IoT nodes in terms of behavior introduces a higher threat towards data transmission and data security. The existence of malformed malicious devices introduces different threats which degrade the performance of entire IoT networks, and the services provided. To handle this, there are a number of secure routing algorithms prescribed in literature that have great deflection in the performance in secure routing and data security. To improve security, an Adaptive Service Dependent Secure Blockchain Model (ASSBM) is presented in this article. The model focused on two constraints: (1) maximizing the service throughput by incorporating a secure routing algorithm with Transmission Behavior Analysis, which analyzes the behavior of different IoT nodes in different data transmissions to measure the Transmission Leverage Trust (TLT) and used towards route selection, and (2) improving the data security by adapting service-centric blockchain algorithm which applies data encryption with different encryption schemes and keys being selected according to the nature of service. By classifying the services under different categories, the selection of encryption schemes and keys are differentiated between various classes of services. Both stages support the improvement of data security and secure transmission. The ASSBM model hikes the secure routing and data security performance.*

Keywords - *IoT Networks, Blockchain Security, Secure Routing, ASSBM, TLT.*

1. Introduction

The development of Internet technology has been used in different areas and various sectors. In this way, the communication sectors have used the development at the device level, which works independently. The Internet of Things (IoT) networks are the one which comprises a number of IoT devices which can perform independent transmission and comes with radio devices. They can perform transmission and perform specific activities being designed to perform.

The IoT devices would perform both data reception and transmission which support the service access to be performed by various other nodes independent of their location. In general, the growth of service orient architecture enables the access of services by their users independent of their location. For example, when a device or user looks to ping a service provided by any service provider, they can access the service from their location with the support of IoT networks.

The devices of the IoT networks come with a limited transmission range, which stops them from directly communicating with the far-away server. However, they perform cooperative transmission to complete the task and support the other nodes in accessing the service.

The presence of cooperative transmission in IoT networks provides various supports as well as issues. The data transmission phase in the network is performed by discovering a set of routes through the IoT nodes, and an optimal route is selected to transmit the service data. Such data transmitted through intermediate nodes faces different threats like modification attacks, routing attacks, and so on.

This really degrades the performance of the service throughput as well QoS performance of the entire network. This must be handled with care towards maximizing the QoS of the environment. In general, the routing in IoT networks is performed according to different factors like hop count, energy, traffic and so on. However, the route selection should be performed by considering the trust of the nodes.

In measuring the trust of the nodes, the method considers their previous involvement and the frequency of the nodes being used. But it fails to consider their behaviour in proper transmission and their involvement in stealing data and so on. This must be considered towards maximizing the secure routing performance. On the other side, the biggest challenge is the data security of data being transmitted. When the intermediate malicious device performs a modification attack and learns the data towards the service nature, then it would perform different threats like DDOS attack. In order to improve data security, there are a number of data encryption algorithms in the literature.

Some of the methods use Attribute Based Encryption (ABE), and some of them would use profile-dependent encryption to improve the data security. However, those methods are not capable of restricting the threat considered. To solve this issue, the modern blockchain-based technique has been used in various problems.

The blockchain is the modern secure paradigm, which has different blocks to maintain the data, hash code and reference part. The data part is the part in the block which is used to store the encrypted data. The hash code part contains the code for the concerned block, which contains the secret code being used to decode the data present in the block.

Finally, the reference block shows which block in the chain should be referred to pick the next data. Also, the user who is allowed to read the data can only properly use the hash code in finding the encryption scheme and key towards data decryption. The other users cannot read the original data. Also, the blockchain models would share the encryption schemes and keys set with the registered and trusted users. The sets and values can be changed and shuffled in different time stamps, and they can be maintained in different criteria which would support the improvement of data security.

The rigidity of blockchain depends on how dynamic the sets and values are shuffled and maintained. By considering all these, an efficient Adaptive Service Dependent Secure Blockchain Model (ASSBM) is presented in this article. The method enforces security in two ways: one is secure routing by choosing a secure transmission route according to the TLT measure. Second by enforcing blockchain security model by using service-dependent blockchain security.

The article is organized to present a detailed introduction to blockchain and IoT networks in section 1. Section 2 briefs the literature review and explores the related works of the problem considered. Section 3, details the working of the proposed ASSBM model, and section 4 presents the experimental results and discussion. Section 5 presents the conclusion of the article in detail.

1.1. Related Works

A number of secure routing and data security schemes are prescribed in the literature. This section details some of the methods around the problem. A Privacy-Preserving Blockchain-Assisted Security Protocol is presented in [1], which performs informal security analysis using Burrows-Abadi-Needham (BAN) logic and the Real-or-Random (ROR) model. Towards emergency handling in fog assisted healthcare IoT, a low-latency, secure and reliable decision making with emergency handling (LSRDM-EH) is given in [2]. Blockchain security with service architecture is presented in [3] to support cloud manufacturing equipment authentication with blockchain. Linear Elliptical Curve Digital Signature (LECDS) with blockchain is presented in [4] to improve the security of cloud servers.

A Public Blockchain-Envisioned Secure Communication Framework for ITS (PBSCF-ITS) is presented in [5] to support smart transportation. The model provides access control and key management within vehicle-to-vehicle communication. The security challenges in medical systems are analyzed and how the blockchain can be used in the problem is discussed in [6].

A blockchain-based privacy-ensured IoMT is presented in [7] to support decentralized EHT and uses smart contract-based service automation with security. Blockchain security with Merkle Hash Zero Correlation Distinguisher (BSMH-ZCD) is presented in [8] to support smart city applications. A Deep Learning (DL) and blockchain security framework is sketched in [9] to support IoT communication.

A Software Defined Security by Contract for Blockchain-Enabled MUD-Aware Industrial IoT Edge Networks is presented in [10]. An agile blockchain-based relational data security model is presented in [11] to improve security against RDB in the cloud.

A block chain based environment model is presented in [12], which uses distributed blockchain storage mode towards sharing of monitoring data and handles data forgery. A survey on the application of blockchain security in forensics management in IoT networks is presented in [13].

The performance of blockchain based security and privacy models in IoT is presented in [14], which analyzes various techniques of data security under different metrics. A Blockchain-based Special Key security Model (BSKM) is presented in [15], which integrates confidentiality, integrity and availability factors in enforcing security in big data.

A Network Sharding Scheme with an Access Frequency set (N2SAF) is presented in [16] to improve scalability in transaction sharding to reduce the pressure in storage. The method uses a bloom filter for privacy protection.

An Adaptive Bi-Recommendation and Self-Improving network (ABRSI) is presented in [17], which uses knowledge of intrusion detection to perform intrusion detection. A Flow Topology-Based Graph Convolutional Network (FT-GCN) is presented in [18] to detect intrusion attacks in IoT networks.

A fuzzy rough set scheme is given in [19] to detect intrusion attacks in IoT networks. The method uses a fuzzy rough set for feature selection and uses a deep convolutional generative adversarial network for detecting intrusion attacks. A Mac protocol-based intrusion detection scheme is presented in [20]. All the methods explored introduce poor performance in data security and secure routing in IoT networks.

2. Adaptive Service Dependent Secure Blockchain Model (ASSBM)

The proposed Adaptive Service-Dependent Secure Blockchain Model (ASSBM) maintains the traces of various transmissions performed in the network. Using those traces, lots of routes are identified with the help of topology in the presence of any packet to be transmitted.

For the routes identified, Transmission Behavior Analysis is performed to identify the most effective secure route for the data transmission. The detection of a secure route is performed by measuring the Transmission Leverage Trust (TLT), which is being measured based on various factors of data transmission like total transmission, total retransmission, number of drops, and number of modifications that appeared.

Further, the method adopts a service-dependent blockchain algorithm which applies data encryption with different encryption schemes and keys being selected according to the nature of the service. By classifying the services under different categories, the selection of encryption schemes and keys are differentiated between various classes of services.

The blockchain generated has been transmitted to the user from which the user can obtain the result in the reverse manner. The working model of the ASSBM system is pictured in Figure 1, where the functions are defined in this section.

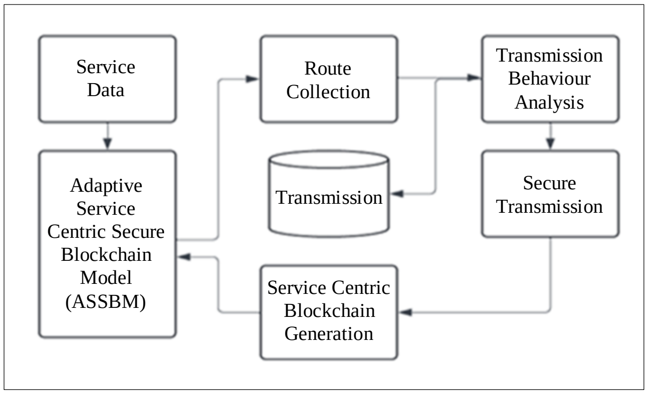
Service Data
Route Collection
Transmission Behaviour Analysis
Adaptive Service Centric Secure Blockchain Model (ASSBM)
Transmission
Secure Transmission
Service Centric Blockchain Generation

Fig. 1 Block diagram of ASSBM model

3. Materials and Methods

3.1. Route Collection

The data packet belonging to any service has been transmitted through a specific route being identified. To identify the set of routes in the network, the method performs route collection initially. To collect the transmission routes available, the method uses the network topology.

With the topology, the method identifies a set of devices present in the topology. Using the location details and the transmission range of various IoT devices, a set of possible routes is detected to perform secure transmission.

```
Algorithm:
Given: Network Topology NTop
Obtain: Route Set Rs
Start
  Read NTop
  Device Set Ds = $\sum IoT \in NTop$
  Find neighbor set Nes= $\sum_{i=1}^{size(Ds)} Ds(i).location \leftrightarrow User.location$
  For each neighbor n
  Find set of routes to reach service point .
  Route set Rns = $\sum_{i=1}^{size(Ds)} Ds(i).location \rightarrow n.location$
  Add Rns to route set Rs = $(\sum Routes \in Rs) \cup Rns.$
  End
Stop
```

The route collection algorithm fetches the routes possible to perform route selection according to the TLT measure.

3.2. Transmission Behaviour Analysis

The transmission behaviour analysis is the process of analysing the behaviour of IoT nodes contained in any route. It has been performed to evaluate the security of the route towards secure transmission.

To analyse the performance of the devices, the method considers the count of transmission the nodes have been involved. Among them, how much number of transmissions went well and complete.

Also, the number of transmissions received with malformed data and the number of transmissions retransmitted are counted. With these values, the value of Transmission Leverage Trust (TLT) is measured. Estimated TLT value has been used in route selection towards secure transmission.

```
Algorithm:
Given: Transmission Trace TT, Route RObtain: Route Obtain: TLT
Start
  Read TT and R.
  Device set Ds = $\sum IoT \in R$
  For each device d
  Collect Device Trace DT = $\sum_{i=1}^{size(TT)} TT(i).Route \in D$
  Compute number of Transmission NT = size(DT)
  Compute number of complete transmissions NcT= size(DT)
```

```
   $\underset{i=1}{Count(DT(i).State == Complete)}$
   Compute number of retransmission NRT = $\overset{size(DT)}{\underset{i=1}{Count(DT(i).State == Retransmit)}}$
   Compute number of malicious transmissions Nmt = $\overset{size(DT)}{\underset{i=1}{Count(DT(i).State == Malicious)}}$
   Compute TLT(D) = $\frac{NcT}{NT} \times \frac{Nmt}{NRT}$
  End
  Compute TLT$_R$ = $\sum_{i=1}^{size(Ds)} Ds(i).TLT \Big/ size(Ds)$
Stop
```

The working of transmission behaviour analysis is presented in the above algorithm, which measures the TLT value for the route to support secure transmission.

3.3. Secure Transmission

The proposed ASSBM model performs secure transmission in two ways. One by choosing an efficient, secure route selection and another in the way of adapting the Service Dependent Blockchain Generation algorithm. To start with, the method uses the routes collected in the first phase. For the routes identified, each route transmission behaviour is analysed which yields the TLT value for the route. According to the value of TLT, the method chooses the most secure route to transmit the data.

Further, towards data security, the method uses the service dependent blockchain generation. The generated blockchain has been given to the receiver. The receiver, in turn, would decrypt the data from the blockchain given.

```
Algorithm:
Given: Route Set Rs, Transmission Trace TT, Service Data Sd
Obtain: Null
Start
  Read Rs, Sd and TT.
  For each route R
  TLT = Perform Transmission Behavior Analysis (TT, R)
End
   Route R = $\overset{size(Rs)}{\underset{i=1}{Max(Rs(i).TLT)}}$
   Blockchain B = Service Dependent Blockchain Generation (Sd)
   Transmit b through route R.
   Stop
```

The secure transmission algorithm analyzes the transmission behavior of routes given and identifies the most secure route. A selected route has been used to transmit the blockchain generated.

3.4. Service-Dependent Blockchain Generation

The service-dependent blockchain generation algorithm maintains a set of service taxonomy, which contains a set of service classes and the scheme set for each class with the key sets to be used. From the service request, the service class is identified, and the service has been executed. With the service result, the method generates a blockchain with k number of blocks which is being identified randomly.

For each block in the chain, the method selects a random scheme and key according to the sets available. With the selected scheme and key for any block, the data has been encrypted and added to the concerned block. Similarly, for the block identified, the method generates the hash code with the random numbers generated. To generate the hash code, the cubic functions and square functions are used. The cubic function generates the cubic value of the random number provided, and the square function generates the square value of the random numbers given. Such values are used to produce the hash code.

```
Algorithm:
Given: Service Request Sreq, Service Taxonomy ST
Obtain: Blockchain B
Start
  Read Sreq and ST.
  Identify service requested S = $service \in Sreq$
  Service class Sc = $\overset{size(ST)}{\underset{i=1}{ST(i).class == S.Class}}$
  Encryption scheme set Ess = $\overset{size(ST)}{\underset{i=1}{\sum ST(i).class == SC \&\& ST(i).EncryptionScheme}}$
  Encryption Key set EKs = $\overset{size(ST)}{\underset{i=1}{\sum ST(i).class == SC \&\& ST(i).EncryptionKey}}$
  Service Data Sd = Execute service and obtain data.
  Generate blockchain B = Blockchain(Random(1,10))
  Number of blocks Nb = size(B)
  Block data Bd = Split(Sd,Nb)
  For each block b
  Random number Rn = $\overset{Size(10)}{\underset{i=1}{Random(i,10)}}$
  Encryption scheme Es = Ess(Rn)
  Random Number Rn1 = $\overset{Size(10)}{\underset{i=1}{Random(i,10)}}$
  Encryption key Ek = Eks(Rn1)
  Cipher data Cd = Encryption(Es,Ek,Bd(b))
  If Rn is odd then
```

```
      Hash code Hc = Square(Rn)+#Square(Rn1)
      Else
      Hash code Hc = Cube(Rn)+$+Cube(Rn1)
      End
   B(data)=Cd
   B(hashcode) = Hc
   End
Stop
```

The service dependent blockchain generation algorithm generates the blockchain and performs data encryption according to the service nature. The generated blockchain has been given to the user from which the user can obtain the original data.

3.5. Service-Dependent Blockchain Data Decryption

The end users receive the blockchain from the service and extract the original data from the chain. To perform this, the method identifies the number of blocks in the chain initially. Using this, the method reads the blocks of the chain and identifies the hash code.

From the hash code, the method identifies the index of the scheme and the key to be used to decrypt the data. Each block has been decrypted accordingly and merged to produce the final result.

```
Algorithm:
Given: Scheme set Ss, Key set Ks, Blockchain B
Obtain: Original data Odat.
Start
  Read Ss, Ks, B.
  Compute number of blocks Nb = Size(B)
  Original data Odat.
    For each block b
    If Nb is odd then
      Index set Is = Split(B.hashcode,"#")
      Key index ki = SquareRoot((Is(2))
      Scheme index Si = Square Root (Is(1))
      Odat = Odat.append(Decrypt(Ss(si),Ks(Ki),b.data)
      Else
        Index set Is = Split(B.hashcode,"#")
        Key index ki = Cube Root((Is(2))
        Scheme index Si = Cube Root (Is(1))
        Odat = Odat.append(Decrypt(Ss(si),Ks(Ki),b.data)
      End
   End
Stop
```

4. Results and Discussion

The Adaptive Service dependent Secure Blockchain Model (ASSBM) is implemented and the performance is evaluated with varying numbers of users and nodes. The performance of the methods is recorded and compared with the results of others.

Table 1. Experimental setup

Factors	Values
Programming Tool	Advanced Java
Total Users	100
Total IoT Nodes	200
Service Classes	10

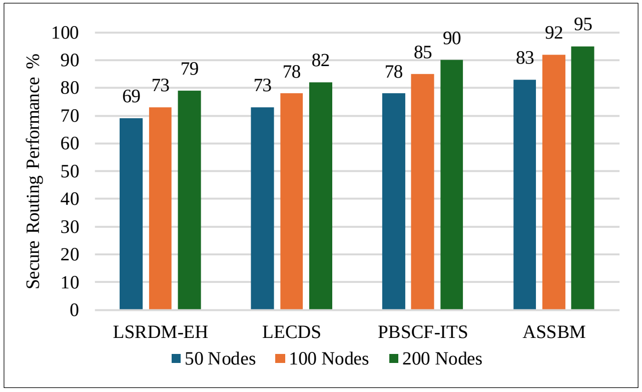

Fig. 2 Secure routing performance

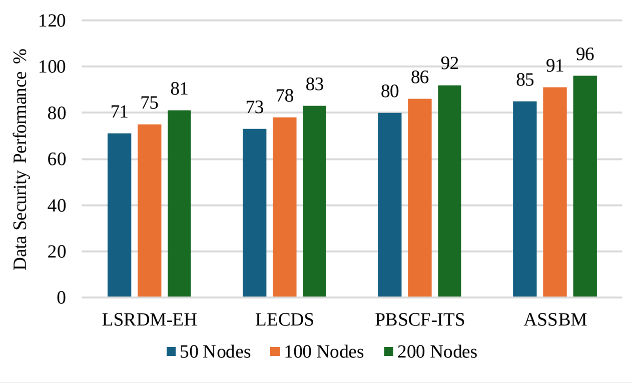

Fig. 3 Data security performance

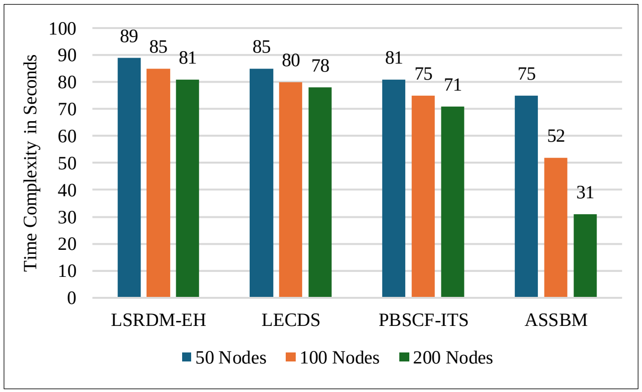

Fig. 4 Time complexity

The experimental setup used to evaluate the performance of ASSBM has been presented in Table 1. The efficacy in secure routing and secure transmission is evaluated and pictured in Figure 2. The ASSBM model hikes security performance in all constraints. The efficacy in providing data security is evaluated and pictured in Figure 3, and the ASSBM model achieves higher performance. The time complexity in data transmission is measured for different methods and pictured in Figure 4. The ASSBM model produces less time complexity than others.

5. Conclusion

This paper presented a novel Adaptive Service Dependent Secure Blockchain Model (ASSBM) to support IoT networks. The model maintains the transmission history, and based on that, the method applies Transmission behavior analysis over the routes identified to find the most secure route to enforce secure transmission. On the other side, data security is enforced by using service service-dependent blockchain generation algorithm. The ASSBM model has achieved higher data security and reduces the time complexity.

Acknowledgments

The first author would like to acknowledge Dr. M. Arivukarsi, Associate Professor working at Kondunadu College of Engineering and Technology, and Dr. S. Sathyalaksmi from Hindustan Institute of Technology and Science for providing me with guidance throughout the project.

References

[1] Garima Thakur et al., “An Effective Privacy-Preserving Blockchain-Assisted Security Protocol for Cloud-Based Digital Twin Environment,” *IEEE Access*, vol. 11, pp. 26877-26892, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Junyu Ren et al., “Task Offloading Strategy with Emergency handling and Blockchain Security in SDN-Empowered and Fog-Assisted Healthcare IoT,” *Tsinghua Science and Technology*, vol. 27, no. 4, pp. 760-776, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Tharaka Hewa et al., “Fog Computing and Blockchain-Based Security Service Architecture for 5G Industrial IoT-Enabled Cloud Manufacturing,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7174-7185, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] B. Sowmiya et al., “Linear Elliptical Curve Digital Signature (LECDS) with Blockchain Approach for Enhanced Security on Cloud Server,” *IEEE Access*, vol. 9, pp. 138245-138253, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mohammad Wazid et al., “Fortifying Smart Transportation Security through Public Blockchain,” *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 16532-16545, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Qin Liu et al., “The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities,” *IEEE Systems Journal*, vol. 16, no. 4, pp. 5741-5752, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Bhaskara S. Egala et al., “Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control,” *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11717-11731, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Rizwan Patan et al., “Blockchain Security Using Merkle Hash Zero Correlation Distinguisher for the IoT in Smart Cities,” *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 19296-19306, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Shailendra Rathore, Jong Hyuk Park, and Hangbae Chang, “Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT,” *IEEE Access*, vol. 9, pp. 90075-90083, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Prabhakar Krishnan et al., “Software-Defined Security-by-Contract for Blockchain-Enabled MUD-Aware Industrial IoT Edge Networks,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7068-7076, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ruba Awadallah, and Azman Samsudin, “Using Blockchain in Cloud Computing to Enhance Relational Database Security,” *IEEE Access*, vol. 9, pp. 137353-137366, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Manyu Zhao, Wei Liu, and Kai He, “Research on Data Security Model of Environmental Monitoring Based on Blockchain,” *IEEE Access*, vol. 10, pp. 120168-120180, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Zhuofan Liao et al., “Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey,” *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 1159-1175, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Mohamed Amine Ferrag, and Lei Shu, “The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial,” *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17236-17260, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Cigdem Bakir, “New Blockchain-Based Special Keys Security Model with Path Compression Algorithm for Big Data,” *IEEE Access*, vol. 10, pp. 94738-94753, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ruonan Li et al., “A Blockchain-Enabled Framework for Enhancing Scalability and Security in IIoT,” *IEEE Transactions on Industrial Informatics*, vol. 19, no. 6, pp. 7389-7400, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Jiashu Wu et al., “Adaptive Bi-Recommendation and Self-Improving Network for Heterogeneous Domain Adaptation-Assisted IoT Intrusion Detection,” *IEEE Internet of Things Journal*, vol. 10, no. 15, pp. 13205-13220, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Xiaoheng Deng et al., “Flow Topology-Based Graph Convolutional Network for Intrusion Detection in Label-Limited IoT Networks,” *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 684-696, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Yixuan Wu et al., “Intelligent Intrusion Detection for Internet of Things Security: A Deep Convolutional Generative Adversarial Network-Enabled Approach,” *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3094-3106, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nanavath Kiran Singh Nayak, and Budhaditya Bhattacharyya, “MAC Protocol Based IoT Network Intrusion Detection Using Improved Efficient Shuffle Bidirectional COOT Channel Attention Network,” *IEEE Access*, vol. 11, pp. 77385-77402, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Xiaokang Zhou et al., “Hierarchical Adversarial Attacks Against Graph-Neural-Network-Based IoT Network Intrusion Detection System,” *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9310-9319, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Ayodeji Oseni et al., “An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 1000-1014, 2023. [CrossRef] [Google Scholar] [Publisher Link]