electronics

MDPI

Article

Blockchain-Assisted Cybersecurity for the Internet of Medical Things in the Healthcare Industry

Mohammed Saeed Alkatheiri * and Ahmed S. Alghamdi

Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia

* Correspondence: msalkatheri@uj.edu.sa

Abstract: The Internet of Medical Things (IoMT) plays an important role in strengthening sustainable healthcare systems. IoMT significantly influences our healthcare because it facilitates monitoring and checking patient medical information before transferring the data to a cloud network for future use. The IoMT is a big-data platform which is growing rapidly, so it is critical to maintain all data safely and securely. In this study, Blockchain-Assisted Cybersecurity (BCCS) for the IoMT in the healthcare industry is proposed. Blockchain is a decentralized digital ledger that allows end-to-end communication and provides interaction between untrustworthy persons. BCCS uses a conventional in-depth approach and blockchain to create a procedure for collecting medical information from the IoMT and integrated devices. The proposed system utilizes blockchain to record and extract the accumulated information in a secure and distributed manner within a closed environment suitable for healthcare professionals, such as nursing homes, hospitals, and the healthcare industry where data exchange is needed. The experimental outcomes show that the proposed system has a high security rate of 99.8% and the lowest latency rate of 4.3% compared to traditional approaches. In all, the reliability of the proposed system gives the highest rate of 99.4%.

Keywords: blockchain; IoMT; cybersecurity; healthcare; big data

Citation: Alkatheiri, M.S.; Alghamdi, A.S. Blockchain-Assisted Cybersecurity for the Internet of Medical Things in the Healthcare Industry. *Electronics* **2023**, *12*, 1801. https://doi.org/10.3390/electronics12081801

Academic Editors: Wenquan Jin, Meilan Jiang and Shabir Ahmad

Received: 8 February 2023
Revised: 25 March 2023
Accepted: 3 April 2023
Published: 11 April 2023

1. Introduction

The Internet of Medical Things (IoMT) is a group of Internet-connected devices that provide healthcare solutions. Primarily, the IoMT is a networked architecture of healthcare equipment [1], healthcare applications [2], and healthcare activities [3]. More specifically, connected systems and sensors empower healthcare industries to improve the efficiency of their medical activities and workflow administration and monitor patient wellness from remote places [4]. The IoMT connects the virtual and physical environments to enhance patient wellness by speeding up diagnosis and therapies and modifying patient lifestyle and health conditions in real time [5,6]. The interconnection of medically relevant technologies will have a significant influence on patients and healthcare professionals [7]. Along with the rapid growth and diversified nature of the IoMT, safeguarding it has become a significant challenge as advanced security issues develop and previous security issues become more acute [8]. The definition of data protection is the ability to store and transport data without allowing unauthorized access to ensure data consistency [9], legitimacy [10], legality, and confidentiality [11]. Only authorized users have access to the protected information. Because of unauthenticated users and their unauthorized access, cybercrime evolves and frequently impacts healthcare systems and sensors [12]. A large quantity of IoMT data is gathered, transmitted, and distributed among many healthcare industries [13,14]. The data transmission should be carried out in a protected manner [15]. Because of this tremendous data transformation process, the number of cyberattacks has increased dramatically [16]. It indicates the need for a reliable system to protect IoMT healthcare data [17]. This study proposes the using blockchain technologies to create a more

secure and trustworthy IoMT framework [18]. Blockchain is a decentralized digital ledger that allows end-to-end communication and provides interaction between untrustworthy persons [19]. Blockchain technology executes various transactions between unfamiliar parties in a cloud network even though they do not believe each other [20]. Blockchain is a sort of database system that can monitor and process data from a huge number of sources without utilizing a centralized server [21,22]. The decentralized digital ledger comprises a sequence of blocks that are cryptographically linked to one another [23]. It is not feasible to modify or erase information blocks that have been stored on the blockchain decentralized digital ledger [24,25]. In this study, Blockchain-Assisted Cybersecurity (BCCS) for the IoMT in the healthcare industry is proposed. The significant research objectives of the study are given as follows.

1. The functional architecture of blockchain technology in ensuring cybersecurity aspects of the healthcare industry.
2. An overview of the Internet of Medical Things and its functional features.
3. Details on Blockchain-Assisted Cybersecurity for the Internet of Medical Things in the healthcare industry with the proposed model.

The rest of this study is structured as follows. A literature survey is provided in Section 2. The functional architecture of blockchain technology is discussed in Section 3. Section 4 provides an overview of the Internet of Medical Things. Discussions on the proposed model with numerical computation are given in Section 5. Section 6 discusses the experimentation results, and Section 7 concludes the study.

2. Literature Study

The term "privacy data" relates to a patient's characteristics, such as sickness and economic status [26]. When reviewing the transmission features of this original information, it is critical to check that the personal qualities of the new database are appropriately handled and that the database secures the patient's privacy during the information distribution phase [27,28]. The IoMT significantly influences our healthcare because it facilitates monitoring and checking medical information from patients before it is transferred to a cloud network for future use [29,30]. The IoMT is a big-data platform that is rapidly growing, so it is critical to safely and securely maintain all the data [31,32]. This study significantly elaborates on the previous research contributions on providing cybersecurity for the IoMT in the healthcare industry. Ray PP et al. [33] introduced data encryption and decryption (DED) to protect IoMT data from cyberattack. Encryption techniques were employed to convert the original message or the actual information into cipher-data. The ciphered data were subsequently sent to the destination through the public network. The encrypted data were then decrypted at the destination. Due to restricted resources and security considerations, a lightweight peer-to-peer code management method was described in which codes were communicated with low resource consumption. Egala BS et al. [34] developed a secured cloud network (SCN) utilizing IoMT sensors; it was associated with the digital sign timestamp technique and contradictory techniques to monitor an individualâ€™s confidential information. This method is extremely effective in terms of delivering healthcare services while consuming minimal healthcare resources. According to a safety and operational study, the secured cloud network can handle the difficulties in the healthcare system. Li X et al. [35] proposed an access control algorithm (ACA) to protect IoMT healthcare data. The access control monitoring algorithm develops some policies and a user's identification to prohibit unauthorized users from accessing data. Access control employs various cryptography approaches, including homogeneous passcode cryptography, heterogenous passcode cryptography, and feature-based cryptography. Its complexity and passcode generation process determine cryptography's protection. As a result, the life cycle of the surveillance mechanism is directly dependent on the passcodes. Wazid M et al. [36] developed an architecture for healthcare security networks (HSN) based on cloud computing techniques. They developed an access control system that enables adaptive and sophisticated security rules and focuses on cipher data and

feature-based cryptography. Cloud platforms are not completely trusted. Healthcare records require reliability and accuracy, which might be affected if data are removed or modified without authorization [37,38]. The criteria for data protection are generally established by the consumer for security purposes so that the network operator cannot easily access the information [39,40]. Furthermore, a reliable third party with a good reputation that delivers unbiased audit findings may be implemented appropriately to enable cloud network operators' responsibility and preserve the legal advantages of cloud users [41]. Confidential data should be encoded before transmission to ensure data security, which excludes conventional data usage [42–44]. In [45], the authors secure an IoMT system using metaheuristic-based encryption and an authentication scheme.

The BCCS system we propose in this study uses a conventional in-depth approach and blockchain to create a procedure for collecting medical information from the IoMT and integrated devices. The proposed system utilizes blockchain to record and extract the accumulated information in a secure and distributed manner within a closed environment, suitable for healthcare professionals, such as nursing homes, hospitals, and healthcare industry where data exchange is needed. Blockchain technology is also utilized successfully for securing systems that concern data other than health-related applications. For example, the authors in [46] apply blockchain and a deep learning framework to secure a cooperative adaptive cruise control system. In addition, the authors in [47], proposed a blockchain-based secure system for online examinations that uses a combination of time-lock and multi-signature techniques to achieve transparency and fairness.

3. Functional Architecture of Blockchain

Blockchain is a decentralized digital ledger that allows end-to-end communication and provides interaction between untrustworthy persons. Blockchain comprises n number of blocks, as illustrated in Figure 1.

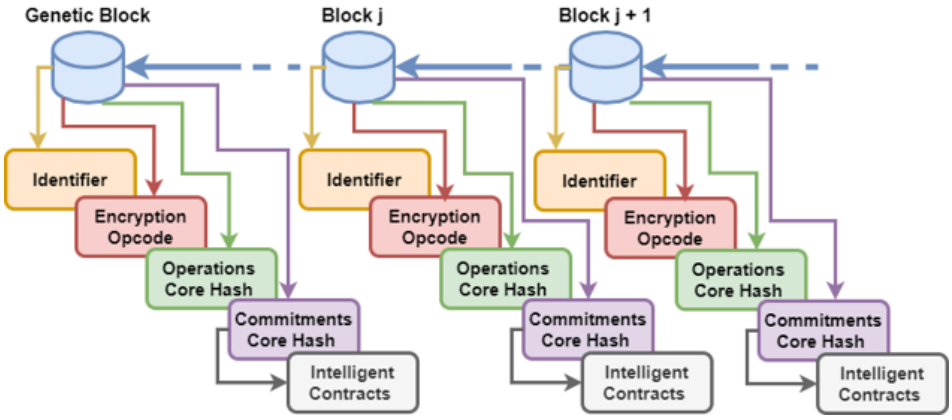

Figure 1. Functional architecture of blockchain.

In this functional architecture, apart from the initial block (genetic), each block is integrated into its preceding block through a reverse connection, the hash code of its earlier block. For example, block $j+1$ has the hash code of its earlier block j. Every block also includes additional data fields, such as an identifier, an encryption opcode, a core hash of all operations, and a core hash of all commitments. Because even a single bit change might result in a unique hash code, the fixed-size core hash values of both operations and commitments are essentially irreversible.

Intelligent contracts are another disruptive invention in blockchain technology that the development of blockchain has propelled. When specific criteria are met, intelligent contracts operating on the upper end of the blockchain can streamline the implementation of contractual agreements and restrictions. Intelligent contracts are irreversible after being synthesized into executable code and recorded in blockchains related to the irreversibility of blockchain and the core hash of all intelligent contracts. Intelligent contracts can

help streamline administration, increase the efficiency of business operations, and reduce potential threats. The following are the essential characteristics of blockchain architectures:

1. Immutability indicates that falsifications of data kept in blockchain are exceedingly difficult since even little changes might result in incorrect data.
2. Transactional non-repudiation can be enabled by digital signatures, non-symmetric encryption/decryption methods, and decentralized consensus procedures.
3. Traceability denotes the ability to track data sources by examining currently accessible blockchain data with accompanying metadata.
4. Diversity of blockchain enables transactions to be authenticated by the number of users spread across the network without the need for a central authority. In this manner, administrative costs may be reduced, while system dependability is improved.

Blockchain technologies are generally classified into three categories:

1. Open blockchains;
2. Personal blockchains;
3. Collaborative blockchains.

Open blockchains, such as cryptocurrency, Bitcoin, and EOSIO, may be accessed by any user in the blockchain community, but personal blockchains feature intensive access control to restrict user functionality. Collaborative blockchains reside between private and open blockchains. Open blockchains often have less sustainability than personal blockchains due to the poorer capacity of cryptographic techniques, where capacity represents the number of operations confirmed per second. Collaboration blockchains yield less efficiency than personal blockchains but greater efficiency than open blockchains.

4. Overview of Internet of Medical Things (IoMT)

Recent advancements in sensing devices, healthcare instruments, and wireless communications have resulted in the emergence of the IoMT. It is employed in various healthcare situations, including e-medicine, remote rehabilitative services, and pandemic isolation. The IoMT, which connects various healthcare instruments and infrastructures with the healthcare industry, has resulted in huge amounts of diversified healthcare records. Healthcare providers can easily identify and diagnose a healthcare issue and treat patients using huge quantities of IoMT information. Figure 2 illustrates the overview of the IoMT architecture. In the IoMT architecture, numerous IoMT sensors generate enormous amounts of IoMT information, captured, interpreted, and evaluated by healthcare providers.

The IoMT can provide dependable and effective healthcare services to both patients and healthcare providers. The emergence of the IoMT also brings with it the associated difficulties:

1. A lack of compatibility across various IoMT domains;
2. Confidentiality and cybersecurity flaws in the IoMT instruments and networks.

IoMT systems are heterogeneous because they are made up of various biosensors, healthcare systems, IoT interfaces, and wireless networks. Furthermore, the heterogeneity of the IoMT is evidenced in the variety of wireless systems, such as near-field transmission, Bluetooth technology, and wireless local area networks. The diversity of distributed IoMT systems leads to poor compatibility between systems, resulting in a variety of data barriers. As a result, it is difficult to transmit healthcare information between healthcare facilities and organizations. On the other hand, healthcare data transmission is critical for healthcare practitioners, particularly in preventing and managing pandemics. Furthermore, the IoMT is concerned with significant cybersecurity and confidentiality issues. Healthcare sensors and medical equipment, which are frequently resource-constrained, have inherent weaknesses to malicious assaults, such as eavesdropping, interference, malware, and worm threats. Secondarily, when compared to other forms of IoT information, IoMT information is highly confidential. The data confidentiality of patients may be purposefully or unintentionally leaked during the gathering, processing, and analysis of IoMT data.

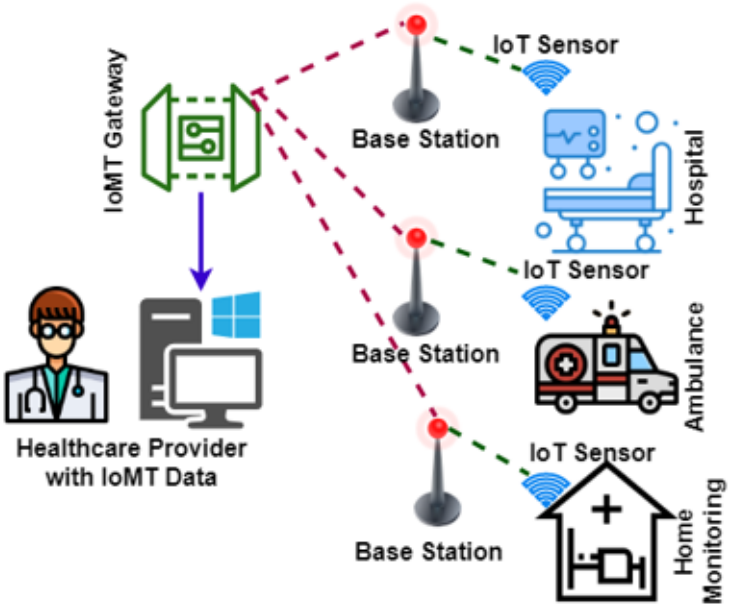

Figure 2. Overview of IoMT architecture. The figure shows the overall concept of the IoMT-based data acquisition, storage, processing, and distribution system. Base stations accumulate data from disparate sensors deployed in diverse situations. Data from the base station are received by the healthcare providers through the gateway.

5. Blockchain-Assisted Cybersecurity for the Internet of Medical Things

Blockchain interconnection with the IoMT can overcome cybersecurity and privacy problems. Figure 3 illustrates the architecture of Blockchain-Assisted Cybersecurity for the IoMT. The proposed architecture comprises four states:

1. Healthcare instrument state;
2. Blockchain state;
3. Edge network state;
4. Data synthesis state.

The healthcare instrument state is equipped with numerous IoMT healthcare instruments, such as thermal imaging cameras, laser designators, wrist sensor systems, wearable devices, and biosensors. The edge network state is simply a combination of communications infrastructure and edge computational resources. IoMT data can be collected and pre-processed by edge computing nodes embedded with wireless networks, WiFi routers, and the IoMT gateway. Furthermore, the blockchain state serves as a critical gateway to provide reliable analysis of multiple resources across the preceding levels. The data synthesis state comprises cloud computation capabilities, digital storage platforms, machine learning, artificial intelligence, and neural networks algorithms. Edge computing capabilities in the edge network state or objects in the data synthesis state are connected to nodes in the blockchain state. As a result, blockchain-assisted IoMT can also provide excellent authenticity and authentication protocols at both the edge network state and the blockchain. The edge network state and the blockchain state minimize the complication of IoMT devices and the diversity of IoMT interactions. However, the blockchain state can deliver blockchain-assisted functions to other programs to ease the development process. The blockchain state uses the built-in augmented reality network of blockchain to interconnect various IoMT sub-networks across the complete IoMT network. The heterogeneous IoMT modules are therefore merged as a whole to provide complete satisfaction to other programs. As a consequence, IoMT system compatibility can be enhanced.

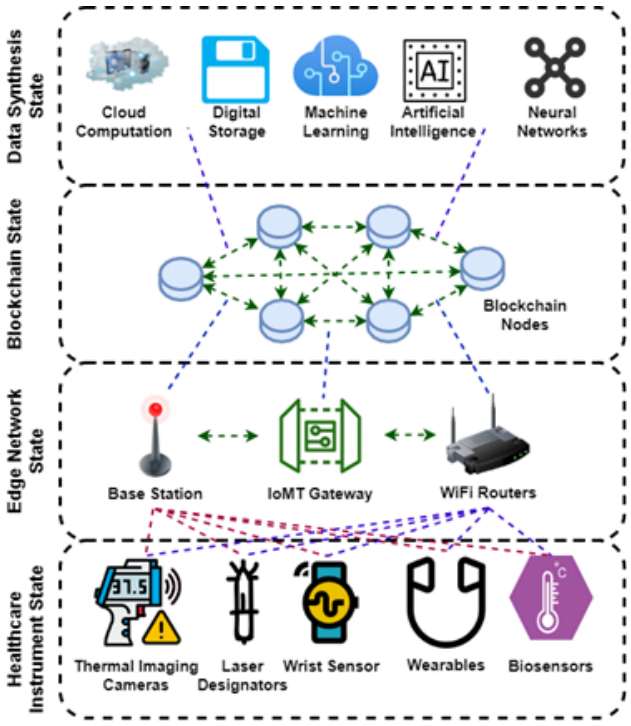

Figure 3. Architecture of Blockchain-Assisted Cybersecurity for IoMT systems. The overall architecture is organized into four states, i.e., healthcare instrument state, edge network state, blockchain state, and data synthesis state.

The BCCS Model

The classified elements include O data combination series, $G = \{a_{p,q}, b_p\}_{p=1}^{O}$, while $a_{p,q} = (x_{p,q}, y_{p,q})$ is a multistate sequence of mined healthcare data $\left(x_{p,q} \in F^{o_f * U}\right)$ and combined data $\left(y_{p,q} \in F^{c_f * U}\right)$ of length U with $q = 1, 2, \cdots, U$. $a_{p,q}$ represents the q state of the p combined healthcare data sequence, while b_p indicates the state label pointer in a denoted state dataset β. It is significant to remember that the developed BCCS model transmits to the possibility matrix and that the probability of the state dataset is given in Equation (1):

$$x(b|a;c) = \sum_{i} exp(F(b,i|a;c) - D(c)), \tag{1}$$

where $c = [\phi, \mu]$ is a domain vector, $i \in \{i_1, i_2, \ldots, i_U\}$, and $i_p \in I$ represents the latent features. The quantity of latent features, in general, varies from the state passcode because i_q can communicate to an organizational feature in a state. However, identical notation is used for computation convenience. $F(b,i|a;c)$ is known as the constancy vector, and $D(c)$ indicates the log divider to prompt the normalization task as given in Equation (2)

$$D(c) \log \sum_{b} \sum_{i} exp\left(F(b',i|a;c)\right). \tag{2}$$

In general, the possibility is tolerable for each probable formation of discrete and couple states as given in Equation (3)

$$F(b,i|a;c) = \sum_{m \in \epsilon} \sum_{p} \vartheta_p(b, i_m, a; \varphi_p) + \sum_{m,a \in \rho} \sum_{p} \delta_p(b, i_m, i_a; \omega_p), \tag{3}$$

where the parameters φ and ω indicate scalar and vector features needed to be equated in potential creation, and $\vartheta_p(b, i_m, a; \varphi_p)$, $\delta_p(b, i_m, i_a; \omega_p)$ indicate scalar and vector nodes. The scaler node is given in Equation (4)

$$\vartheta_p(b, i_m, a; \varphi_p) = \sum_m \theta_{1,p}(b, i_m; \varphi_{1,p}) + \sum_l \theta_{2,p}(b, i_m; \varphi_{2,p}). \quad (4)$$

It can also be represented as a constancy function combined with dual utilities. Part of the domain state is to design the intercommunication of the state label b with the hidden network i_m, and it is expressed in Equation (5)

$$\theta_{1,p}(b, i_m; \varphi_{1,p}) = \sum_{\alpha \in \beta} \sum_{\gamma = I)} \varphi_{1,p} \partial(b = \alpha) \partial(i_m = \gamma), \quad (5)$$

whereas ∂ is a representation variable; if its argument is legal, it is equated to one, otherwise zero. The representation feature designing is the intercommunication between the hidden network i_m and interaction a, given in Equation (6):

$$\theta_{2,p}(b, i_m; \varphi_{2,p}) = \sum_{\gamma = I} \varphi_{2,p} \partial(i_m = \gamma) a. \quad (6)$$

The vector elements are a transitional feature and represent the intercommunication between a couple of concealed related hidden networks i_m and i_a as given in Equation (7) below:

$$\delta_p(b, i_m, i_a; \omega_p) = \sum_{\alpha \in \beta \wedge \mu, \gamma = I} \omega_p \partial(b = \alpha) \partial(i_m = \mu) \partial(i_a = \gamma). \quad (7)$$

Based on the results obtained from the above computational iterations, Blockchain-Assisted Cybersecurity can be used by healthcare professionals, such as nursing homes, hospitals, and the healthcare industry where data exchange is needed. The use of blockchain with the IoMT has the potential to enhance IoMT cybersecurity significantly. Initially, the constructed security features of blockchain, such as heterogeneous encrypted communications methods and digital signatures, can provide significant protection for IoMT healthcare information. Second, integrating blockchain with existing safety techniques, such as authorization and access control, can improve cybersecurity. Finally, intelligent contracts incorporated in IoT sensors can automatically activate auto-upgrading programs to upgrade IoT instrument software continuously, improving cybersecurity. Furthermore, blockchain decentralization can reduce the chances of system failures caused by single-point malfunctions or other hostile assaults, thereby enhancing cybersecurity and dependability. Blockchain can accomplish considerable privacy protection by concealing blockchain identity addresses and authenticating blockchain transactions. The combination of blockchain with other privacy-protection schemes, such as encryption prevarications and other cryptographic methods, can empower users with greater privacy protection. In this way, confidential IoMT information can be kept and analyzed locally before being transferred to remote cloud networks. As a result, the deployment of the edge network state helps to protect healthcare data privacy.

6. Experimental Results and Discussion

This section provides detailed discussion on the operational performance of the proposed Blockchain-Assisted Cybersecurity (BCCS) for the IoMT in the healthcare industry compared with conventional IoMT healthcare data security approaches, such as data encryption and decryption (DED), secured cloud network (SCN), access control algorithm (ACA), and healthcare security networks (HSN). In this research, the cybersecurity of IoMT healthcare data was gathered from 24 user nodes. As illustrated in Figure 3, the proposed model (BCCS) ensures privacy and data security. This developed model integrates with blockchain technology for security enhancement in the cybersecurity of the IoMT health-

care data. This proposed model combines deep learning with an artificial intelligence algorithm to enable efficient resource consumption in the IoMT of the healthcare industry. Furthermore, BCCS utilizes computational algorithms to obtain the cybersecurity data for 16 monitoring intervals. The cloud server is utilized for data recording, analysis, and evaluation purposes, and it can maintain 2 TB of healthcare data with an analyzing speed of 2.4 GHz. Blockchain is a sort of database system that can monitor and process data from a huge number of sources without utilizing a centralized server. The decentralized digital ledger comprises a sequence of blocks that are cryptographically linked to one another. It is not feasible to modify or erase information blocks that have been stored on the blockchain. The experimental results of the proposed model were investigated using performance metrics, such as precision, reliability, security rate, and latency rate. For evaluating the privacy and data security in the IoMT in the healthcare industry using the proposed model (BCCS), a relative investigation was performed on conventional IoMT healthcare data security approaches, such as DED, SCN, ACA, and HSN.

6.1. Precision Analysis

The proposed model's precision is considerably enhanced for user nodes and monitoring intervals, as shown in Figures 4 and 5. Here, the primary state obtains the healthcare data from the IoMT sensor and the literature to identify whether the state is secure or insecure. Based on this examination, the precision range is improved, and these healthcare data are integrated with the IoMT sensor. If any insecure action is recognized, a warning is sent to the healthcare industry, and it is denoted as $G = \{a_{p,q}, b_p\}_{p=1}^{O}$. This warning is directed as per schedule, and the healthcare data relates to the domain state of the matching literature data. This match state focuses on the Blockchain-Assisted Cybersecurity model, differentiating patients' activities. The quantity of data generated from IoMT sensors is integrated with classifying an activity as secure or insecure. In this assessment, the precision range and the exact identification of the patient's activity are improved. If the patient's behavior is secure, the warning is not sent; otherwise, it is sent.

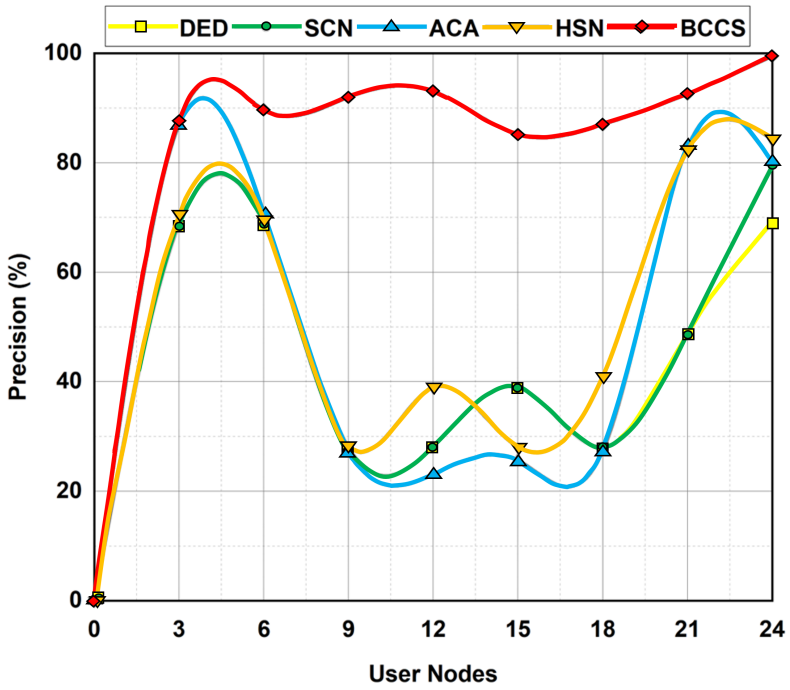

Figure 4. Precision (user nodes).

6.2. Reliability Aspects

The system reliability can be improved for user nodes and monitoring intervals, as shown in Figures 6 and 7, respectively. If the patient's IoMT healthcare data are insecure,

the data collected from IoMT sensors are mapped with the error values in the cloud server. At the same time, the data are matched with the error value to help improve the system reliability. It is denoted as $\vartheta_p(b, i_m, a; \varphi_p)$, and it is executed through the edge network state. The deviation between secure and insecure data is detected at a quick dispensation range, and the outcomes are calculated realistically. The outcome is therefore specific to the patient's state and uncertainty. Healthcare data are tracked alternatingly, and steadiness and variability are measured during data synthesis. The capability is assessed realistically in the data synthesis state, and it is communicated to the user nodes. Literature mapping and information analysis are utilized in the monitoring structure, and system reliability is interconnected with the matching technique. The user nodes are utilized to transmit healthcare data and develop real-time outcomes on the IoMT network. Thus, user nodes grasp patients' activities and develop stronger warning indicators.

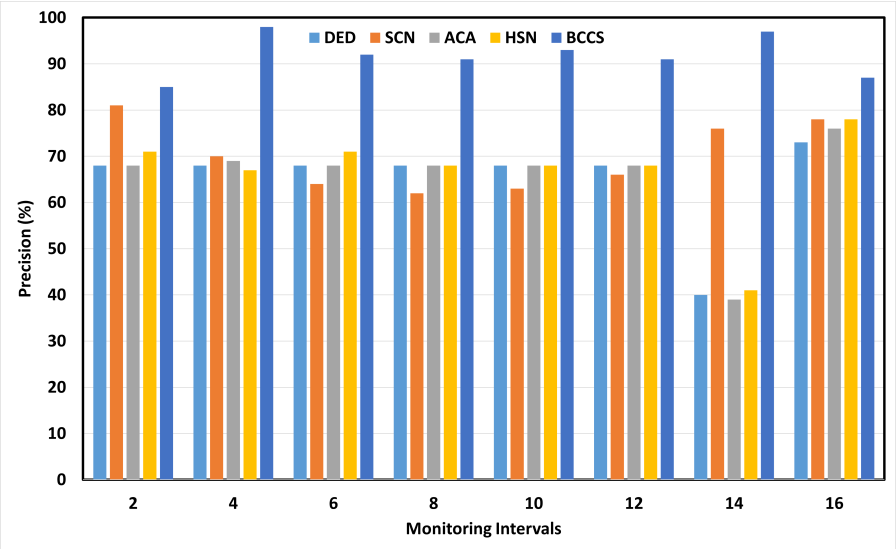

Figure 5. Precision (monitoring intervals).

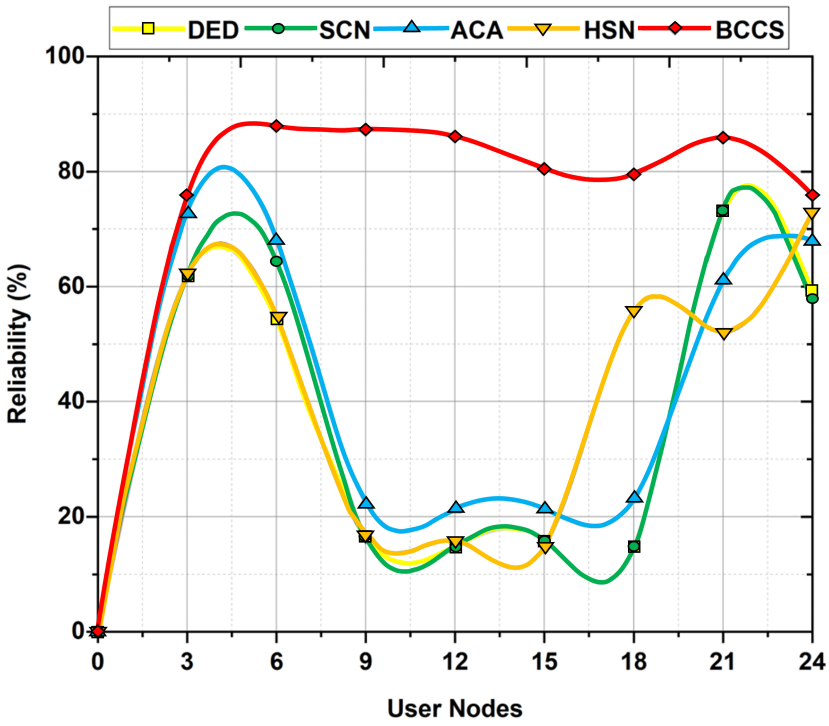

Figure 6. Reliability (user nodes).

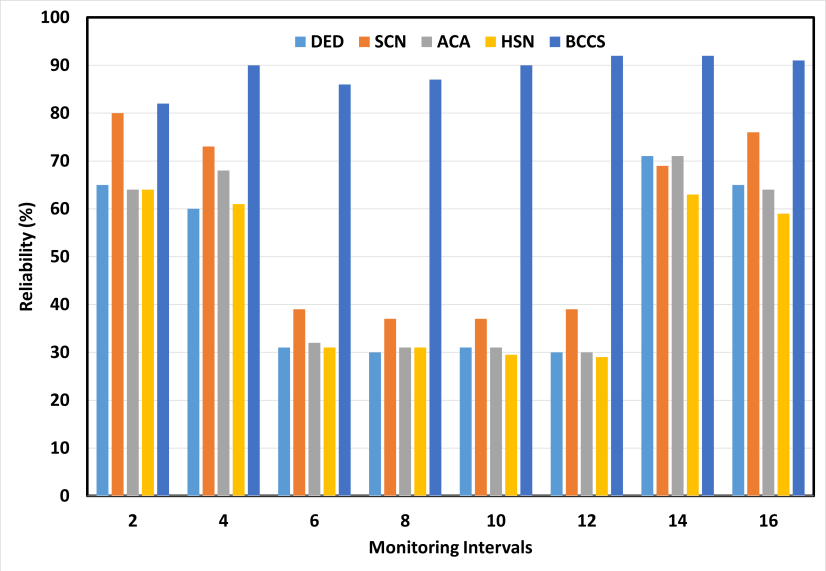

Figure 7. Reliability (monitoring intervals).

6.3. Security Rate

The security rate for user nodes and monitoring intervals of the proposed framework are shown in Figures 8 and 9, respectively. The healthcare data are transmitted to the user nodes, and the mapping parameters control the anticipated model as expressed by $\sum_{\gamma=1} \varphi_{2,p} \partial(i_m = \gamma)a$. The anticipated model is compared to the patient's historical data and indicates the condensed cost to trace the action. The outcome is transferred on a schedule, and it provides an advanced level of precision. The proposed model improves the security rate for numerous IoMT sensing networks with high precision. The proposed model forms an IoMT network, and the healthcare data are obtained and interconnected and used for data authentication and cybersecurity. In this case, the patient request is tagged if it is an emergency, and the response from the healthcare providers is immediately provided.

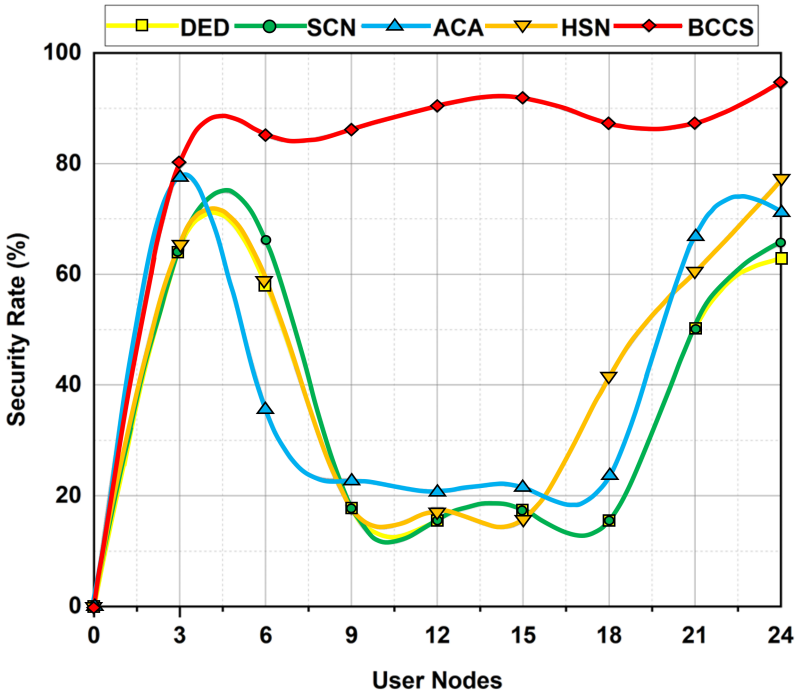

Figure 8. Security rate (user nodes).

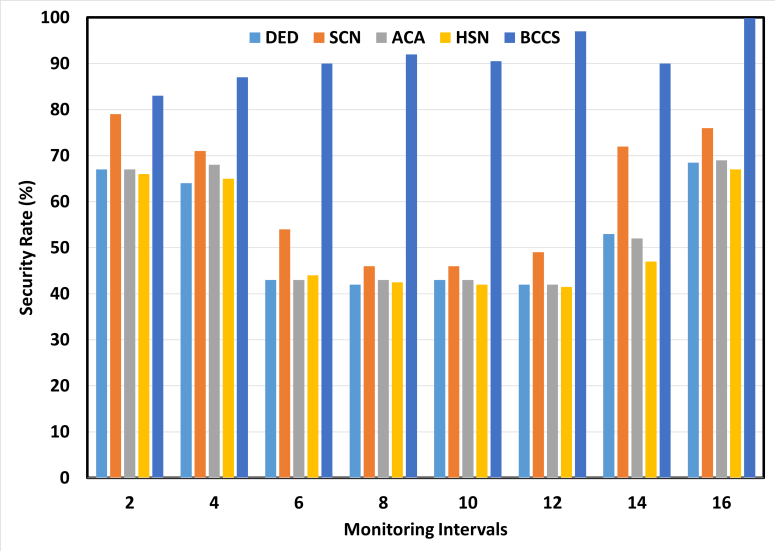

Figure 9. Security rate (monitoring intervals).

6.4. Latency Rate Analysis

The latency rate for user nodes and monitoring intervals decrease and exhibit better performance than the conventional IoMT healthcare data security approaches, such as DED, SCN, ACA, and HSN, as shown in Figures 10 and 11, respectively. The healthcare data are identified from the patient history, and the improved functional performance is expressed as $\sum_{\alpha\in\beta\wedge\mu,\gamma=I}\omega_p\partial(b=\alpha)\partial(i_m=\mu)\partial(i_a=\gamma)$. Collected healthcare data are accessed through authentication from biometric signs and user desires. Here, several IoMT sensors are used, the investigation of a neighboring state is repeatedly executed, and the results are recorded. The user node data are used to predict data for mapping with the patient's historical data. The patient's behavior is recognized accurately for the effective allocation of resources. This study utilized the input coordination position state. The study supervises the utilization of blockchain technologies in healthcare industries to create a more secure and trustworthy IoMT framework. Hence, this study uses the Blockchain-Assisted Cybersecurity (BCCS) model to ensure healthcare data protection and privacy among IoMT sensor networks. The experimental results are listed in Tables 1 and 2, respectively.

Table 1 lists the BCCS performance metrics results compared with the conventional IoMT healthcare data security approaches for user nodes. The proposed model provides enhanced outcomes in all performance metrics compared to the conventional IoMT healthcare data security approaches. Moreover, the proposed model provides better precision, reliability, security rate, and latency rate by 31.01%, 16.83%, 32.25%, and 70.50%, respectively.

Table 1. Experimental results for user nodes.

Performance Metrics	DED	SCN	ACA	HSN	BCCS
Precision (%)	67.6	77.4	86.9	84.1	98.1
Reliability (%)	73.1	73.9	73.9	72.1	87.9
Security Rate (%)	65.1	65.2	77.1	75.9	96.1
Latency Rate (%)	13.1	14.9	8.6	13.9	4.1

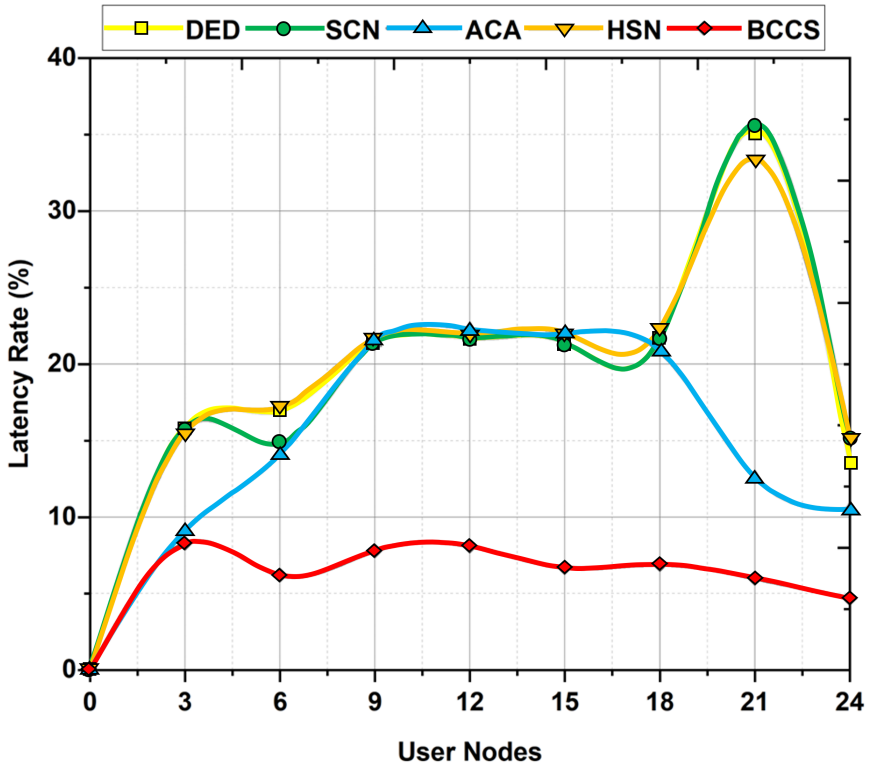

Figure 10. Latency rate (user nodes).

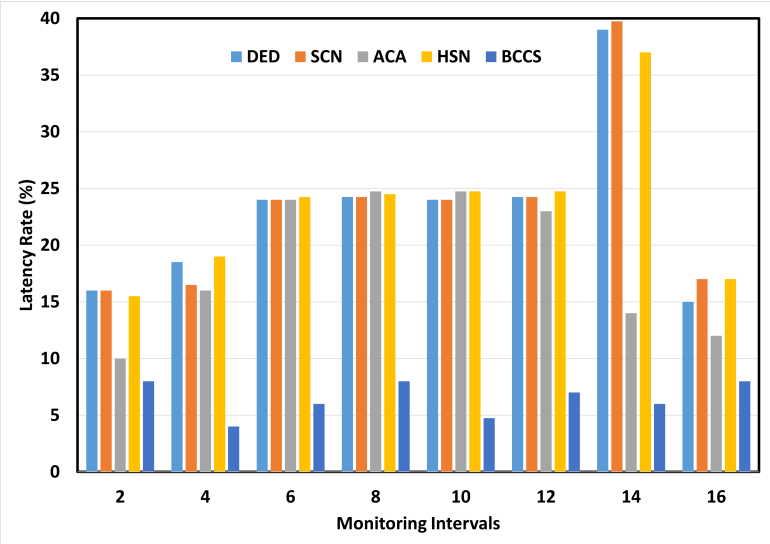

Figure 11. Latency rate (monitoring intervals).

Table 2. Experimental results for monitoring intervals.

Performance Metrics	DED	SCN	ACA	HSN	BCCS
Precision (%)	70.9	80.8	76.1	78.2	99.3
Reliability (%)	65.1	79.9	71.7	64.3	99.4
Security Rate (%)	68.2	80.2	69.1	65.9	99.8
Latency Rate (%)	15.1	16.2	10.1	17.6	4.3

Table 2 lists the BCCS performance metrics results compared with the conventional IoMT healthcare data security approaches for monitoring intervals. The proposed model provides better precision, reliability, security rate, and latency rate by 99.3%, 99.4%, 99.8%, and 4.3%. Concurrently, the DED model for monitoring intervals delivers poor results. Moreover, the proposed model provides better precision, reliability, security rate, and latency rate by 28.60%, 34.50%, 31.66%, and 75.56%, respectively.

7. Conclusions

In this study, Blockchain-Assisted Cybersecurity (BCCS) for the IoMT in the healthcare industry is developed. Using a conventional in-depth approach and blockchain with the IoMT can significantly enhance IoMT cybersecurity. Initially, the constructed security features of blockchain, such as heterogeneous encrypted communications methods and digital signatures, can provide significant protection to IoMT healthcare information. Second, integrating blockchain with existing safety techniques, such as authorization and access control, can improve cybersecurity. Finally, intelligent contracts incorporated in IoT sensors can automatically activate auto-upgrading programs to upgrade the IoT instrument software continuously, improving cybersecurity. The experimental outcomes show that the proposed system has a high security rate of 99.5% and the lowest latency rate of 4.1% compared to traditional approaches. In all, the reliability of the proposed system gives the highest rate of 99.8%.

Author Contributions: All authors have substantially contributed towards methodology, validation, formal analysis and preparation of the original draft. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by University of Jeddah, Saudi Arabia, under grant No. MoE-IF-G-20-05.

Data Availability Statement: Not applicable.

Acknowledgments: The authors, acknowledge with thanks the University technical and financial supports. We are thankful for the technical support of Sajjad Hussain Chauhdary, Sajid Saleem and Mohammed A. Alqarni.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ray, P.P.; Dash, D. Blockchain for IoT-based medical delivery drones: State of the art, issues, and future prospects. *Blockchain Technol. Emerg. Appl.* **2022**, 137–176. [CrossRef]
2. Razdan, S.; Sharma, S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE Tech. Rev.* **2022**, *39*, 775–788. [CrossRef]
3. Elsayeh, M.; Ezzat, K.A.; El-Nashar, H.; Omran, L.N. Cybersecurity architecture for the Internet of Medical Things and connected devices using blockchain. *Biomed. Eng. Appl. Basis Commun.* **2021**, *33*, 2150013. [CrossRef]
4. Sharma, A.; Tomar, R.; Chilamkurti, N.; Kim, B.G. Blockchain based smart contracts for Internet of Medical Things in e-healthcare. *Electronics* **2020**, *9*, 1609. [CrossRef]
5. Alqaralleh, B.A.; Vaiyapuri, T.; Parvathy, V.S.; Gupta, D.; Khanna, A.; Shankar, K. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. *Pers. Ubiquitous Comput.* **2021**, 1–11. [CrossRef]
6. Nguyen, T.N.; Zeadally, S.; Vuduthala, A.B. Cyber-Physical Cloud Manufacturing Systems With Digital Twins. *IEEE Internet Comput.* **2021**, *26*, 15–21. [CrossRef]
7. Karrupusamy, P.; Balas, V.E.; Shi, Y. *Sustainable Communication Networks and Application: Proceedings of ICSCN 2021*; Springer: New York, NY, USA, 2022.
8. Hu, L.; Nguyen, N.T.; Tao, W.; Leu, M.C.; Liu, X.F.; Shahriar, M.R.; Al Sunny, S.N. Modeling of cloud-based digital twins for smart manufacturing with MT connect. *Procedia Manuf.* **2018**, *26*, 1193–1203. [CrossRef]
9. Dash, R.K.; Nguyen, T.N.; Cengiz, K.; Sharma, A. Fine-tuned support vector regression model for stock predictions. *Neural Comput. Appl.* **2021**, 1–15. [CrossRef]
10. Khan, F.; Jan, M.A.; ur Rehman, A.; Mastorakis, S.; Alazab, M.; Watters, P. A secured and intelligent communication scheme for IIoT-enabled pervasive edge computing. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5128–5137. [CrossRef]
11. Yang, S.; Yin, D.; Song, X.; Dong, X.; Manogaran, G.; Mastorakis, G.; Mavromoustakis, C.X.; Batalla, J.M. Security situation assessment for massive MIMO systems for 5G communications. *Future Gener. Comput. Syst.* **2019**, *98*, 25–34. [CrossRef]

12. Manogaran, G.; Alazab, M.; Shakeel, P.M.; Hsu, C.H. Blockchain assisted secure data sharing model for Internet of Things based smart industries. *IEEE Trans. Reliab.* **2021**, *71*, 348–358. [CrossRef]
13. Khan, F.; Kumar, R.L.; Kadry, S.; Nam, Y.; Meqdad, M.N. Cyber physical systems: A smart city perspective. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 3609–3616. [CrossRef]
14. Jegadeesan, S.; Azees, M.; Kumar, P.M.; Manogaran, G.; Chilamkurti, N.; Varatharajan, R.; Hsu, C.H. An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications. *Sustain. Cities Soc.* **2019**, *49*, 101522. [CrossRef]
15. Ahmed, S.H.; Bashir, A.K.; Guibene, W. Introduction to the special section on emerging technologies for connected vehicles and ITS networks. *Comput. Electr. Eng.* **2019**, *75*, 309–311. [CrossRef]
16. Fang, L.; Yin, C.; Zhu, J.; Ge, C.; Tanveer, M.; Jolfaei, A.; Cao, Z. Privacy protection for medical data sharing in smart healthcare. *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* **2020**, *16*, 1–18. [CrossRef]
17. Zhang, P.; Pang, X.; Kibalya, G.; Kumar, N.; He, S.; Zhao, B. GCMD: Genetic correlation multi-domain virtual network embedding algorithm. *IEEE Access* **2021**, *9*, 67167–67175. [CrossRef]
18. Younan, M.; Houssein, E.H.; Elhoseny, M.; Ali, A.E.M. Performance analysis for similarity data fusion model for enabling time series indexing in internet of things applications. *PeerJ Comput. Sci.* **2021**, *7*, e500. [CrossRef]
19. Raza, M.; Kumar, P.M.; Hung, D.V.; Davis, W.; Nguyen, H.; Trestian, R. A digital twin framework for industry 4.0 enabling next-gen manufacturing. In Proceedings of the IEEE 2020 9th International Conference on Industrial Technology and Management (ICITM), Oxford, UK, 11–13 February 2020; pp. 73–77.
20. Xu, X.; Chen, Y.; Zhang, J.; Chen, Y.; Anandhan, P.; Manickam, A. A novel approach for scene classification from remote sensing images using deep learning methods. *Eur. J. Remote Sens.* **2021**, *54*, 383–395. [CrossRef]
21. Zhang, R.; Ve, S.; Jackson Samuel, R.D. Fuzzy efficient energy smart home management system for renewable energy resources. *Sustainability* **2020**, *12*, 3115. [CrossRef]
22. Xue, K.; Deng, Y.; Zhang, H.; Pandiyan, S.; Manickam, A. Cycling environment investigation and optimization of urban central road in Qingdao. *Comput. Intell.* **2021**, *37*, 1217–1235. [CrossRef]
23. Muñoz-Araque, D.; Garcia, M.H.; Garcia, P.G.; Montenegro, C. Navigation of resources from tangible object recognition to improve virtual tours in botanical gardens. In *Information Technology and Systems: Proceedings of ICITS 2020*; Springer: New York, NY, USA, 2020; pp. 525–534.
24. Thapliyal, M.; Ahuja, N.J.; Shankar, A.; Cheng, X.; Kumar, M. A differentiated learning environment in domain model for learning disabled learners. *J. Comput. High. Educ.* **2022**, *34*, 60–82. [CrossRef]
25. Ramesh, S.; Yaashuwanth, C.; Muthukrishnan, B.A. Machine learning approach for secure communication in wireless video sensor networks against denial-of-service attacks. *Int. J. Commun. Syst.* **2020**, *33*, e4073. [CrossRef]
26. Gupta, D.; Rani, S.; Ahmed, S.H.; Garg, S.; Piran, M.J.; Alrashoud, M. ICN-based enhanced cooperative caching for multimedia streaming in resource constrained vehicular environment. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4588–4600. [CrossRef]
27. Srivastava, A.K.; Grotjahn, R.; Ullrich, P.A. A multimodel technique for estimating future changes in extreme precipitation. In Proceedings of the AGU Fall Meeting Abstracts, San Francisco, CA, USA, 9–13 December 2019; Volume 2019, p. A51Q-2832.
28. Hammachukiattikul, P.; Sekar, E.; Tamilselvan, A.; Vadivel, R.; Gunasekaran, N.; Agarwal, P. Comparative study on numerical methods for singularly perturbed advanced-delay differential equations. *J. Math.* **2021**, *2021*, 6636607. [CrossRef]
29. Abbas, K.; Tawalbeh, L.A.; Rafiq, A.; Muthanna, A.; Elgendy, I.A.; Abd El-Latif, A.A. Convergence of blockchain and IoT for secure transportation systems in smart cities. *Secur. Commun. Netw.* **2021**, *2021*, 5597679. [CrossRef]
30. Abd El-Latif, A.A.; Abd-El-Atty, B.; Mazurczyk, W.; Fung, C.; Venegas-Andraca, S.E. Secure data encryption based on quantum walks for 5G Internet of Things scenario. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 118–131. [CrossRef]
31. Gao, J.; Wang, H.; Shen, H. Machine learning based workload prediction in cloud computing. In Proceedings of the IEEE 2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 3–6 August 2020; pp. 1–9.
32. Gao, J.; Wang, H.; Shen, H. Task failure prediction in cloud data centers using deep learning. *IEEE Trans. Serv. Comput.* **2020**, *15*, 1411–1422. [CrossRef]
33. Ray, P.P.; Dash, D.; Kumar, N. Sensors for Internet of Medical Things: State-of-the-art, security and privacy issues, challenges and future directions. *Comput. Commun.* **2020**, *160*, 111–131. [CrossRef]
34. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-chain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731. [CrossRef]
35. Li, X.; Tao, B.; Dai, H.N.; Imran, M.; Wan, D.; Li, D. Is blockchain for Internet of Medical Things a panacea for COVID-19 pandemic? *Pervasive Mob. Comput.* **2021**, *75*, 101434. [CrossRef]
36. Wazid, M.; Das, A.K.; Shetty, S.; Jo, M. A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things. *IEEE Access* **2020**, *8*, 88700–88716. [CrossRef]
37. Dai, H.N.; Imran, M.; Haider, N. Blockchain-enabled Internet of Medical Things to combat COVID-19. *IEEE Internet Things Mag.* **2020**, *3*, 52–57. [CrossRef]
38. Kumar, R.; Tripathi, R. Towards design and implementation of security and privacy framework for Internet of Medical Things (iomt) by leveraging blockchain and ipfs technology. *J. Supercomput.* **2021**, *77*, 7916–7955. [CrossRef]

39. Rayan, R.A.; Tsagkaris, C. Blockchain-based IoT for personalized pharmaceuticals. In *Internet of Medical Things*; CRC Press: Boca Raton, FL, USA, 2021; pp. 51–62.
40. Ray, P.P.; Dash, D.; Salah, K.; Kumar, N. Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases. *IEEE Syst. J.* **2020**, *15*, 85–94. [CrossRef]
41. Rahman, M.A.; Hossain, M.S. An internet-of-medical-things-enabled edge computing framework for tackling COVID-19. *IEEE Internet Things J.* **2021**, *8*, 15847–15854. [CrossRef] [PubMed]
42. Meng, W.; Li, W.; Zhu, L. Enhancing medical smartphone networks via blockchain-based trust management against insider attacks. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1377–1386. [CrossRef]
43. Arul, R.; Raja, G.; Almagrabi, A.O.; Alkatheiri, M.S.; Chauhdary, S.H.; Bashir, A.K. A quantum-safe key hierarchy and dynamic security association for LTE/SAE in 5G scenario. *IEEE Trans. Ind. Inform.* **2019**, *16*, 681–690. [CrossRef]
44. Lee, H.J.; Soe, M.T.; Chauhdary, S.H.; Rhee, S.; Park, M.S. A data aggregation scheme for boundary detection and tracking of continuous objects in WSN. *Intell. Autom. Soft Comput.* **2017**, *23*, 135–147. [CrossRef]
45. Riya, K.; Surendran, R.; Tavera Romero, C.A.; Sendil, M.S. Encryption with User Authentication Model for Internet of Medical Things Environment. *Intell. Autom. Soft Comput.* **2023**, *35*, 507–520. [CrossRef]
46. Raja, G.; Kottursamy, K.; Dev, K.; Narayanan, R.; Raja, A.; Karthik, K.B.V. Blockchain-Integrated Multiagent Deep Reinforcement Learning for Securing Cooperative Adaptive Cruise Control. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 9630–9639. [CrossRef]
47. Sadayapillai, B.; Kottursamy, K. A Blockchain-Based Framework for Transparent, Secure, and Verifiable Online Examination System. *J. Uncertain Syst.* **2022**, *15*, 2241002. [CrossRef]