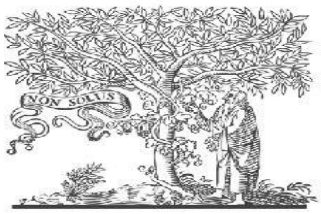
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 15th Nov 2021. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-11

DOI: 10.48047/IJIEMR/V10/I11/12

Title **Block chain based Malware Detection using Machine Learning Algorithms for IoT enabled E-Health Applications**

Volume 10, Issue 11, Pages: 73-82

Paper Authors
Dr. K.Nagarathna

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Block chain based Malware Detection using Machine Learning Algorithms for IoT enabled E-Health Applications.

[1]Dr. K.Nagarathna
Associate Professor, Department of Electronics and Communication Engg.,
Basaveshwar Engineering College, Bagalkot, Karnataka India

Abstract:

Due to increasing digitalization and the development of new technologies such as the IoT, the application of machine learning (ML) algorithms is rapidly expanding (IoT). ML algorithms are being used in healthcare, IoT, engineering, finance, and other fields in today's digital age. However, in order to predict/solve a specific issue, all of these algorithms must be taught. There's a good chance that the training datasets have been tampered with, resulting in skewed findings. As a result, we have suggested a blockchain-based approach to protect datasets produced by IoT devices for E-Health applications in this paper. To address the aforementioned problem, the suggested blockchain-based system makes use of a private cloud. For assessment, we created a mechanism that dataset owners may use to protect their data.

Keywords: Blockchain, IoT, Machine Learning.

Introduction

Most of the existing healthcare systems are built on centralised servers that require authorization from many organisations in the network in order to access the medical data. A delay in providing medical treatments adding to the potential for data leaking might result from all this. It's very uncommon for people to have no idea who is keeping and utilising their medical data without permission in these types of healthcare systems.

Machine learning and possible technologies have been widely used [1] in various research and development sectors. As a result of this massive utilisation, machine learning-based forecasts have become increasingly important in decision-making. The healthcare industry confronts numerous problems as the population continues to expand. It's indeed obvious that these questions need to be answered, that's what this article tries to accomplish [2]. IoT development teams emphasize resources allocation, safety, and internet connectivity. Information obtained by these apps is vast and constantly changing, making it more difficult to store in databases, and its conveyance poses safety problems. Well with help of BT's distributed system, we can address such obstacles [3]. Additional concern is that the machine learning model might be modified to provide beneficial outcomes in the health industry. Machine learning methods' capacity to analyse data and identify data patterns makes them more vulnerable to different sorts of assaults [4].

Due to its excellent properties, including such confidentiality, responsibility, data integrity, and secrecy, to mention a few, blockchain technology has attracted much interest. Since most IoT assets have essential features that render them prone to security attacks [21]. Healthcare is amongst the most rapidly growing sectors [22, 23]. Smarter fitness centres use IoT sensor-based fitness trackers that are placed on the learner to monitor their strenuous activities. Like the way instructors support student training, the Internet of Things is changing the fitness sector. In addition, IoT fitness sensors tackle a number of important concerns, including muscle strain, risk events, and training duration [24]. A broad range of applications has embraced machine learning in recent times [25]. To construct and forecast the future, these methods focus on data analysis to uncover underlying knowledge and useful information from previous data [6].AI and IOT combine to optimize the performance of IoT devices [29]. There is an IoT paradigm by Lee et. al. that is user-oriented and utilises 2 distinct sorts of methods [28].

Intelligent Things (IoT) has become a sector of tremendous influence, opportunity, and development with the expectation that there will be more than 50 billion linked items by 2020 [34]. For

IoT applications, Blockchain (BC), which was initially successfully utilised in cryptocurrency, has the lot of quality and potential high-security technology that protects your privacy [35, 36]. In the IoT, the use of blockchain can eliminate there is just room for one mistake and provide a safe and efficient way of storing and processing IoT data [37]. There is a risk that an IoT system will be slowed down due to a huge quantity of data which is produced by a big amount of IoT devices [38].

Furthermore, the supplier does not provide real-time upgrades, leaving the system exposed. Infrastructure (such as sensing devices and IoT gateway) and cybersecurity solutions can benefit from machine learning approaches. These systems may evaluate network traffic based on the current cyber-threat information, upgrade risk information database, and defend the underlying systems from new assaults.

The Internet connects and controls all smart gadgets, though. In an IoT-enabled industrial multimedia context, it also poses a serious danger to the communication. Heavily prone to replay, man-in-the-middle and impersonating threats; data leak; sensitive data alteration; and virus insertion. To protect such an ecosystem against different sorts of assaults, it is necessary to restrict interaction inside it. It's common to see machine learning techniques being used in health, IoT, technology and banking in today's world. In ability to forecast a certain issue, all of these methods must be trained. Machine learning techniques are vulnerable to malicious assaults in which non traceable modifications are inserted into the raw data, resulting in incorrect projections of the outputs, misleading machine learning systems [39].

Block chain:

A blockchain can indeed be viewed as a decentralised architecture with built-in security to boost transaction trust and integrity [5]. Following the Internet, blockchain has transformed the flow of information and media. As a result, blockchain technology is viewed as a paradigm-shifting invention and the precursor to a new economic era [7]. One way to think of blockchain is as a relational network that consists of ordered blocks, where the committed blocks are immutable [11]. Several researchers have utilisedblockchain in the construction of an eHealth system, although it is not well known. Researchers from Malamas and colleagues employed Blockchain technology to create a framework for medical devices that may have the ability to serve as forensics tool [40]. Using smart contracts on Blockchain, the system allows for fine-grained permission. Blockchain, according to Mytis et al. [41], ensures the integrity and non-repudiation of information retrieved from a conventional biological database. Using a lightweight Blockchain, Ismail et al. [42] have suggested a healthcare architectural architecture. There are several functions assigned to BC nodes that are based on geography. However, IoT devices are generally underpowered. On the whole, some research was discarded since it was largely concerned with technical elements of blockchain technology and/or its architectural design

By sharing database records among many users active in the blockchain network, a blockchain improves on the traditional centralised architecture [5].Smart contracts will decide the blockchain economic model rules wherever stimulatory operations are enforced autonomously [7]. There are essentially three types of blockchain technology [6].

a) Public blockchain
b) Consortium blockchain
c) Private blockchain

Apps are used in nearly every business for mapping, tracing, and speeding up commodities flow. Data is encoded on a blockchain and is moving forward with fresh information as it moves past by the supply chain [8, 9, and 10]. Through hardware and software solutions, blockchain technology may also be utilised to improve security and dependability in distributed networks [18, 19, 20]. There have been three generations of blockchains depending on the desired audience (Zhao et al., 2016): Blockchain version 2 (which incorporates SCs) and a programming environment that go well beyond bitcoin transactions; and Blockchain version 3 (which comprises in areas beyond the previous two versions, such as e-commerce) [11]. It's true that there are a few studies focusing on the function of blockchain in IoT development [12, 13] and large data management in a decentralised way [14]. A method to medical data accessibility on the Blockchain was developed by Ramani et al. [17]. As long as a patient consents, it's possible to get medical treatment professionals to add and retrieve patient health data. There was idea of a separate blockchain which was examined for security evaluations. They did not, however, use a simulator or create a prototype to test the performance of the suggested approach.

Access Control:

Unwanted cyberattacks monitoring and prevention are significant challenges in IoE. An access control system that requires two factors to verify each other before generating a private key for safe interactions

can help overcome these difficulties, as per the authors. The sensing data of different smart devices in an IoE system is analyzed safely at surrounding fog servers, and authorized customers can also obtain the real-time data straight from authorized smart devices via access control mechanisms [69].

As a critical component of cybersecurity, access control limits what actions users may do on services. When working with e-Health services and information, access control is essential for determining which data is provided to which client. As a result, third-party access to these data resources must be controlled. A recipient's right to access resources in a system is controlled by access control, which determines which actions are permitted for particular users [72]. Controlling who may see your health information, whether it's your private or medical information, is not a simple process, especially since other parties (such as insurance companies or physicians) may need accessibility to it for various reasons (such as billing). We are still working towards unified and integrated electronic healthcare systems (e-health), which makes this a particular issue [73].

Access Control System (ACL) are among the most prevalent techniques. As the name suggests, an ACL is a list of topics that may access an item, together with their level of access (or permissions). Access control problems have been solved in e-Health situations utilising DLT and, more especially, blockchain thanks to the extensive use of these technologies. According to Maesa et al. [74], ABAC may be implemented with the help of distributed ledger technology using the XACML reference model.

Moreover, the whole access control method is constructed on a blockchain-based identity management system in a trustless IoT environment, which provides safety and confidentiality for users. Blockchain is used in Concentrate to capture ownership identities and preserve them on trustless peer-to-peer systems in order to maintain a collect of ownership names. These identified owners may then apply access control policies to objects within the same control domain, and the connections between objects could create a feedback mechanism to impact the formation of access policies.

Machine Learning:

As the name suggests, machine learning (ML) is the subject of research that focuses on creating applications that learn via experience. Without directly programming it [76], it is the capacity to educate a computer [77]. In addition to philosophy, information theory, probability and statistics, control theory, psychology and neuroscience, computational complexity, and artificial intelligence [77], ML draws on a wide range of fields. It's important to note that ML algorithms are application-specific. In machine learning, there are a variety of algorithms, including supervised, semi-supervised and unsupervised. Numerous advantages may be gained by utilising machine learning-based systems Large amounts of training data may be used to train them, and then they can aid clinical practise in identifying risk and devising therapy using inductive inference. Because they do not require human intervention, these technologies can help decrease the risk of human mistake [79].

Accordingly, machine-learning techniques are utilised to provide reliable results from huge complex datasets, and the resulting outcomes may be used to anticipate and identify flaws in IoT-based devices. To tackle data security problems, current Iot systems are increasingly using Blockchain (BC) technologies. As a result of this, ML algorithms and BC methods have been studied in depth. Hence the need for a comprehensive assessment of initiatives done in previous decades to tackle both safety and privacy challenges utilising combined Machine learning and Blockchain methods.

In order to train a machine-learning system, information is necessary. Use past patient information to determine predictions about new patients, for instance, patients are hesitant to provide their data because they are worried about their security. This has been addressed in the research [81, 81, 82]. Using non-linear kernel SVM, the scientists developed a novel application framework e-Diag to accurately categorise patient info, while maintaining user data and services provider's models confidentiality [82]. According to the report, previous investigations had employed HE methodologies that were unsuitable for online medical prediagnosis. Medical insurance expenses can also be predicted using machine learning [84, 85]. A study has also been conducted on the current use of machine learning and blockchain in healthcare, as well as its applications, difficulties, and privacy concerns [86, 87]. It's been shown that certain machine learning techniques may be highly useful in minimising security and privacy threats. In the sections that follow, we'll go into more depth about each of these techniques.

Using a method called re-linearization, Sun et al. [83] presented a better version of completely

HE that reduces the size and distortion of the additive cypher text. Other features included a private hyperplane decision-based classification, a private Naive Bayes categorization, and a private decision-trees comparability. As part of an earlier research project, the same authors succeeded in cutting user-server loops in half, without sacrificing privacy or security

Malware Detection:

The categorization features comprise the permissions required by the programme (given by the uses-permission tag) and the components in the uses-features group. They utilised classification technique to categorize Android systems into benign and malicious programs [89]. Bot-net assaults (malware attacks such as mirai and reaper) have recently drawn the interest of researchers. When IoT-enabled industrial multimodal environments are attacked, the connection is interrupted. Aside from that, the hackers may be able to remotely manipulate the smart gadgets and alter their functionality. The existence of malware assaults in such an environment requires a powerful detection method. To identify malicious in an IoT based multimedia for industrial applications environment using a machine learning techniques reserached is being done [90]. In order to find virus, it uses algorithms to observe behaviour of the system and evaluate it as either regular or unusual. Instead than relying on patterns or signatures, categorization is typically based on machine learning algorithms that employ heuristics and rules rather than patterns [91]. Some of the key reports found in the research are:

- Basic reports providing a summary or trend of dangerous software detection, as well as the system and the consequence (cleaned or left alone), are an excellent place to start when analysing malware detection trends [92].
- As a result of this, several organisations have been able to avert catastrophic harm by logging "leave-alone" occurrences from anti-virus programmes [92].
- It's important to keep track of all failures in anti-virus protection since today's malicious software is highly prepared to defeat anti-virus programmes [92].
- By having internal connections to known malware IP addresses, a company's vital data will be protected from being stolen by malicious software operators. This report may be created using logs (such as firewall logs) and a public blacklist of IP addresses [92].
- The "Bottom 10" (as opposed to "Top 10) data might help you determine which types of malware are the least common in your company [92].

Malware Detection Using IoT:

Based on the kind of technique, IoT malware detection approaches may be divided into two primary categories: dynamic and static analysis. In the dynamic method [64], executables are monitored and aberrant activity is detected. Most contemporary malware, according to Alex et al. [65], is formed by copying the source code from the internet, or a version of the dangerous code written by the malware author. This study provides a brief overview of the current development and growth of IoT malware by analysing, evaluating, and synthesising numerous research such as [66], [67], and [68] as well as manually analysing several IoT malware samples. Furthermore, the research investigated probable security flaws in Iot systems for four levels, including sensor, middleware, application, network.

There are several possible benefits and incentives for building an IoT framework that is built on a BC-based architecture [78]. The centralisedIoT approach is vulnerable to DDoS assaults, according to the study. There's also a point of failure in its design, which puts the reliability of IoT services in danger. Current IoT security mechanisms are centralised since they rely on third-party security services, which creates data integrity concerns for IoT devices and systems. Ali et al. showed how BC-based IoT security solutions may overcome all of these concerns. IoT cyber risks have been addressed with Different classifiers and BC methods, but integrating these two is something new that has to be investigated.

According to Alsunbul and coworkers [70], they developed a network security system that detects and prevents unwanted access attempts by replacing the regular protocol with a new one that is generated on the fly. Cloud computing security solution by Chang and Ramachandran [71] to guarantee that only authorised and authenticate the firewall and controlling the access are the first security layers that protect the network and information.l. As a second layer,maintenance of user identities and intrusion detection are employed in order to re-identify users and eliminate any malware. A top-down security strategy is provided via convergent encryption, the third layer.

Blockchain and AI in IoT:

In recent years, ninety percent of the world's data has been generated (IBM, 2017). a) The IoT and b) Population Growth (Stats, 2017). While the blockchain and IoT technologies consists a huge amount of potential on their own, their symbiotic connection opens up many more possibilities. Among many other things, Atlam et al. [29] provided an outline of the Internet OT and AI , as well as possibilities and rewards in diverse AI-based IoT applications. He also explained blockchain technology, which is classified into 3 sub-categories: blockchain feature and its classification; blockchain usage; consensus mechanism; and current problems. On the Ethereal platform, Wright et al. [30] introduced an intelligent agreement that relies on intelligent border. For the verification of edge devices in the transaction trade, the proposed platform provides accurate offload computation on nodes.

With the assistance of Salah et al. [31], researchers analyzed the resilience and efficacy of blockchain-enabled AI as well as open problems that make application of artificial intelligence in the Blockchain. The authors also discuss blockchain uses, as well as outstanding concerns, while focusing on AI. On the basis of the following levels of IoT study, Qian et al. found that blockchain technology offers stability for various open study and IoT gadget challenges. To identify abnormal network behaviour, this process utilizes identity verification and ML algorithms [32]. Almost all of the research cited above focuses on blockchains that are connected with AI. In terms of speed, delay, and safety, these investigations have a long way to go.

Increasing network capacity raises the likelihood of an attacker. A conventional network such as a company's office has less problems than an IoT network. In contrast, IoT devices that communicate with one other are generally multi-vendor gadgets that use multiple standards from various manufacturers.

In concerns to documenting financial transactions, blockchain was initially designed to do just that (e.g., Bitcoins and other cryptocurrencies). Since all transactions are visible, any alterations may be tracked and identified with relative ease." Cryptocurrencies such as blockchain can be used to improve IoT security. We'll now look at two instances of how blockchain may be used to secure IoT devices. When a transaction is performed, a block is produced. The block is sent to the nodes in the network, which is broadcast to all nodes. In bitcoin, one of the nodes validates the block and present it to the network. It is only added to a node's chain of blocks if the block is validated and refers to the prior block in the right manner [75].

AI enabled Blockchain malware detection using IoT in E-Health Applications:

A method to medical data accessibility on the Blockchain was developed by Ramani et al. [17]. As long as a patient consents, it's possible to get medical treatment professionals to add and retrieve patient health data. In order to assess security, the notion of a private blockchain was considered. They did not, however, use a simulator or create a prototype to test the performance of the suggested approach. Due to its relevance in overcoming the compatibility and safety problems of the EHR and EMR technologies in eHealth, blockchain technology has experienced a surge in the health industry. We will be presenting a paper assessment of current research articles on block chain connected to e-health and discussing prospective directions for future research and patterns that may be pursued using this tech as a focal point in the future [33]. Numerous advancements, such as IOT, Internet of Healthcare Devices, Collaborative Training, etc. have contributed to a dramatic increase in electronic information created by Internet - of - things based gadgets in the health industry. In order to diagnose patients in a timely way, machine-learning techniques are essential. To protect medical datasets collected by Iot devices in health apps, this study proposes a methods based on blockchain [39].

With the help of blockchain, these techniques may be made more secure and reliable. An eHealth (mobile health) mobile phone software for cognitive behavioural treatment for sleeplessness was developed and evaluated by a group of researchers [62]. As part of the application, patient health records is sent to a blockchain network. Because of the characteristics of the blockchain, the EMRs in the system were safe and impervious to manipulation after validation, and the patient had access and control over the info [63].

A few of the services covered by distant medication care include constant vital signs tracking with smart or implanted devices sensors, arrhythmia identification and fall detection, implantable cardioverter regulation and tracking of expectant mothers as well as cancer treatment response tracking and glycogen measurement [43]. Due to blockchain's ability to solve important problems such as automated claim validation [53] and public health

management [54], the healthcare industry is a good contender for blockchain technology [50, 51, 52]. For collecting and storing data, the vast majority of Iot applications are centrally controlled. Consequently, these devices are prone to a data loss, especially when dealing with a massive amount of end-to-end interactions [44]. Traditional electronic medical systems can be crippled by malware such as Ransomware and Demand of Service (DoS) intrusions [45].

For example, experts have used blockchain technologies to overcome privacy issues about the administration of medical information and healthcare facilities, as well as safety and third-party faith problems. In addition to network access, safe storage, and exchange of medical information without the need to rely on private entities or mediators, blockchain can also protect the personal data [46, 47]. It has been intended to handle health data independently using blockchain-based ehealth frameworks [43, 48, 49].

Three primary constituents make up healthcare: (a) core providers of medical care services, such as physicians, nurses and hospital administrators; (b) critical services associated with medical care services, such as medical research and health insurance [59]; and (c) beneficiaries of medical and health-related services, such as patients or the public. For the purpose of promoting, maintaining, or recovering beneficiaries' health, the healthcare system is described as contact-based and technology-based remote monitoring services provided by constituency service providers [60, 61].

We require a decentralized network to provide resilience and sustainability, and to minimize several more traffic [55]. Information that has not been maintained on the user's computer or in cloud services must be moved to block chain networks. As a result, we utilize a minimal digital signature [56] technique to verify that information is not changed .In order to process IoT massive data, we require cloud servers. There is a risk, though, that it will create an issue with trustworthy third parties. So we record all activities in separate areas and then construct a composite hash of the each block to achieve this goal. With electronic signature and a minimal Ring system [56], we're able to maintain privacy. It is possible to sign secretly using a ring signature because the sign is mingled with the other individuals (the ring), and that no one (excluding the signatory) recognizes who inked it. We use a double encryption algorithm to secure sensitive information from attackers. Securing the same content with two keys is not what is meant by the double cryptography here, but rather encryption techniques followed by encryption of key that was used for encryption. Use ARX techniques to protect messages, then cipher the key using recipient public key. Defensively, we use Diffie –Hellman key exchange to send the shared key, which makes it very difficult for an adversary to obtain those [57, 58].

Referrence:

[1] Mahdavinejad, Mohammad Saeid, MohammadrezaRez- van, MohammadaminBarekatain, PeymanAdibi, PayamBarnaghi, and Amit P. Sheth, ”Machine learning for Inter- net of Things data analysis: A survey,” Digital Communi- cations and Networks., vol. 4, no. 3, pp. 161–175, 2018.

[2] MazinAlshamrani "IoT and artificial intelligence implementations for remote healthcaremonitoring systems: A survey", (https://doi.org/10.1016/j.jksuci.2021.06.005), 2021

[3] SUDEEP TANWAR 1, QASIM BHATIA 1, PRUTHVI PATEL1, APARNA KUMARI1, PRADEEP KUMAR SINGH 2, AND WEI-CHIANG HONG 3" Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward"

[4] Manoj M K , Thippa Reddy Gadekallu, Sivarama Krishnan S,NeerajKumar,SaqibHakak, Sweta Bhattacharya " Blockchain based Attack Detection on Machine Learning Algorithms for IoT based E-Health Applications", (https://doi.org/10.1016/j.jksuci.2021.06.005), 2020

[5] NasirEl Bassam, Distributed Renewable Energies for Off-Grid Communities (Second Edition) Empowering a Sustainable, Competitive, and Secure Twenty-First Century,(https://doi.org/10.1016/B978-0-12-821605-7.00007-6) Chapter Twenty - Blockchain 2021, Pages 447-450

[6] D.Jeyabharathi, D.Kesavaraja, D.Sasireka, Handbook of Research on Blockchain Technology, Chapter 7 - Cloud-Based Blockchaining for Enhanced Security (https://doi.org/10.1016/B978-0-12-819816-2.00007-1), 2020, Pages 171-181

[7] Madhusudan Singh, ShihoKim, Advances in ComputersVolume 115, Chapter Four - Blockchain technology for decentralized autonomous organizations,(https://doi.org/10.1016/bs.adcom.2019.06.001), 2019, Pages 115-140

[8] A. Haleem, M. Javaid, Additive manufacturing applications in industry 4.0: a review, Journal of Industrial Integration and Management, 4 (4) (2019 Dec 4), Article 1930001

[9] S. Perera, S. Nanayakkara, M.N.N. Rodrigo, S. Senaratne, R. Weinand, Blockchain technology: is it hype or real in the, construction industry?, Journal of Industrial Information Integration, 17 (2020), Article 100125

[10] Y. Zuo, Making smart manufacturing smarter–a survey on blockchain technology in Industry 4.0, Enterprise Inf. Syst. (2020), pp. 1-31

[11] Fran Casino, Thomas K.Dasaklis, ConstantinosPatsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telematics and Informatics Volume 36, (https://doi.org/10.1016/j.tele.2018.11.006) March 2019, Pages 55-81

[12] A. Vetro, J.C. De Martin, Blockchain for the Internet of Things: a systematic literature review, 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), IEEE (2016), pp. 1-6

[13] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access, 4 (2016), pp. 2292-2303

[14] E. Karafiloski, A. Mishev, Blockchain solutions for big data challenges: a literature review, IEEE EUROCON 2017–17th International Conference on Smart Technologies, IEEE (2017), pp. 763-768

[15] IBM, 2017. 10 Key Marketing Trends for 2017, https://www-01.ibm.com/common/ssi/cgi-bin/ssialiashtmlfid=WRL12345USEN

[16] Stats, I.W., 2017. Internet usage statistics, The internet big picture, http://www.internetworldstats.com/stats.htm.

[17] VidhyaRamani, Tanesh Kumar, An Bracken, MadhusankaLiyanage, and Mika Ylianttila. Secure and efficient data accessibility in blockchain based healthcare systems. In 2018 IEEE Global Communications Conference (GLOBECOM), pages 206–212. IEEE, 2018.

[18] K. Fan, Y. Ren, Y. Wang, H. Li, Y. Yang, Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G, IET Commun., 12 (5) (2018), pp. 527-532

[19] S.C. Cha, S.C. Hung, J.F. Chen, S.C. Syu, T.Y. Tsai, On the design of a blockchain-based reputation service for android applications, Adv. Sci. Lett., 23 (3) (2017), pp. 2179-2184

[20] S. Suzuki, J. Mura, Blockchain as an audit-able communication channel, Proc. Int. Comput. Softw. Appl. Conf., 2 (2017), pp. 516-522

[21] Faisal Jamil 1 , Hyun Kook Kahng 2 , Suyeon Kim 3 and Do-Hyeun Kim 1,"Towards Secure Fitness Framework Based on IoT-Enabled Blockchain Network Integrated with Machine Learning Algorithms"

[22] Jamil, F.; Hang, L.; Kim, K.; Kim, D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital.Electronics 2019, 8, 505.

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

[24] Kranz, M. Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry; John Wiley & Sons: Hoboken, NJ, USA, 2016.

[25] Jamil, F.; Iqbal, N.; Imran; Ahmad, S.; Kim, D. Peer-to-Peer Energy Trading Mechanism based on Blockchain and Machine Learning for Sustainable Electrical Power Supply in Smart Grid. IEEE Access 2021, pp. 1–1.

[26] Ahmad, S.; Jamil, F.; Iqbal, N.; Kim, D. Optimal Route Recommendation for Waste Carrier Vehicles for Efficient Waste Collection: A Step Forward Towards Sustainable Cities. IEEE Access 2020, 8, 77875–77887.

[27] Luca Brunese, Francesco Mercaldob, Alfonso Reginelli, Antonella Santone, Procedia Computer Science 159 (2019) 1787–1794

[28] Lee, S.W.; Prenzel, O.; Bien, Z. Applying human learning principles to user-centered IoT systems. Computer 2013, 46, 46–52.

[29] Atlam, H.F.; Walters, R.J.; Wills, G.B. Intelligence of things: Opportunities challenges. In Proceedings of the 2018 3rd Cloudification of the Internet of Things (CIoT), Paris, France, 2–4 July 2018; pp. 1–6.

[30] Wright, K.L.; Martinez, M.; Chadha, U.; Krishnamachari, B. SmartEdge: A smart contract for edge computing. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications

(GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1685–1690.

[31] Salah, K.; Rehman, M.H.U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and open research challenges. IEEE Access 2019, 7, 10127–10149.

[32] Qian, Y.; Jiang, Y.; Chen, J.; Zhang, Y.; Song, J.; Zhou, M.; Pustišek, M. Towards decentralized IoT security enhancement: A blockchain approach. Comput.Electr. Eng. 2018, 72, 266–273.

[33] SuselGóngora Alonso ,Jon Arambarri, Miguel López-Coronado, Isabel de la Torre Díez " Proposing New Blockchain Challenges in eHealth", 2019.

[34] Minhaj Ahmad Khan, Khaled Salah, Iot security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems, 82 (2018), pp. 395-411

[35] Nils Siegfried, Tobias Rosenthal, Alexander Benlian, et al. Blockchain and the industrial internet of things: A requirement taxonomy and systematic fit analysis. Technical report, Darmstadt Technical University, Department of Business Administration, 2020.

[36] Regio A Michelin, Ali Dorri, Marco Steger, Roben C Lunardi, Salil S Kanhere, Raja Jurdak, and Avelino F Zorzo, Speedychain: A framework for decoupling data from blockchain for smart cities. In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pages 145–154, 2018.

[37] Yong Yu, Yannan Li, Junfeng Tian, Jianwei Liu, Blockchain-based solutions to security and privacy issues in the internet of things, IEEE Wireless Communications, 25 (6) (2018), pp. 12-18

[38] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo, Antonio Puliafito Blockchain and iot integration: A systematic survey Sensors, 18 (8) (2018), p. 2575

[39] Thippa Reddy Gadekallu, Manoj M K, Sivarama Krishnan S Neeraj Kumar* ,SaqibHakak ,Sweta Bhattacharya "Blockchain based Attack Detection on Machine Learning Algorithms for IoT based E-Health Applications" arXiv:2011.01457v1, Nov 2020

[40] VaggelisMalamas, Thomas Dasaklis, Panayiotis Kotzanikolaou, Mike Burmester, and SokratisKatsikas.A forensics-by-design management framework for medical devices based on blockchain. In 2019 IEEE World Congress on Services (SERVICES), volume 2642, pages 35–40. IEEE, 2019.

[41] P Mytis-Gkometh, G Drosatos, PS Efraimidis, and E Kaldoudi. Notarization of knowledge retrieval from biomedical repositories using blockchain technology. In International Conference on Biomedical and Health Informatics, pages 69–73. Springer, 2017.

[42] Leila Ismail, HunedMaterwala, SheraliZeadally, Lightweight blockchain for healthcare, IEEE Access, 7 (2019), pp. 149935-149951

[43] A.D. Dwivedi , G. Srivastava , S. Dhar , R. Singh , A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2) (2019) 326 .

[44]B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, M. Peng, When internet of things meets blockchain: Challenges in distributed consensus, IEEE Netw. 33 (6) (2019) 133–139, doi:10.1109/MNET.2019.190 0 0 02.

[45] R. Abdolkhani, K. Gray, A. Borda, R. DeSouza, Patient-generated health data management and quality challenges in remote patient monitoring, JAMIA Open (ooz036) (2019), doi:10.1093/jamiaopen/ooz036

[46] Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System [Online]. Available: http://bitcoin.org/bitcoin.pdf, Citeseer (2008).

[47] G. Drosatos, E. Kaldoudi, Blockchain applications in the biomedical domain: A scoping review, Comput. Struct.Biotechnol. J. 17 (2019) 229–240, doi:10.1016/j.csbj.2019.01.010/

[48] M.A .Uddin , A . Stranieri , I. Gondal , V. Balasubramanian , Continuous patient monitoring with a patient centric agent: A block architecture, IEEE Access 6 (2018a) 32700–32726 .

[49] M.A .Uddin , A . Stranieri , I. Gondal , Balasubramanian , A patient agent to manage blockchains for remote patient monitoring, Stud. Health Technol, Inform. 254 (2018b) 105–115.

[50] T.T. Kuo, H.E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, J. Am. Med. Inform. Assoc., 24 (6) (2017), pp. 1211-1220

[51] S. Alla, L. Soltanisehat, U. Tatar, O. Keskin, Blockchain technology in electronic healthcare systems, IISE Annual Conf. Expo, 2018 (1) (2018), pp. 754-759

[52] K.J. Cios, B. Krawczyk, J. Cios, K.J. Staley, Uniqueness of medical data mining, How the New Technologies and Data They Generate Are Transforming Medicine (2019)

[53] S. Angraal, H.M. Krumholz, W.L. Schulz, Blockchain technology: applications in health care, Circ. Cardiovasc. Qual. Outcomes, 10 (9) (2017), Article e003800

[54] M. Mettler, Blockchain technology in healthcare: the revolution starts here In 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), September (2016), pp. 1-3

[55] Dr. AshutoshDharDwivedi, ShaliniDhar,GautaumShrivastav," A Decentralized Privacy-Preserving Healthcare Blockchain for IoT (2019)

[56] Malina, L.; Hajny, J.; Dzurenda, P.; Ricci, S. Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions. In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, Porto, Portugal, 26–28 July 2018; pp. 526–531.

[57] XiaoyangZhu,youakimbadir "Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions (2018)

[58] Jo˜ao Pedro Dias , Lu´ıs Reis, Hugo Sereno Ferreira, ˆAngelo MartinsBlockchain for Access Control in e-Health Scenarios (2018)

[59] S.M. Campbell, M.O. Roland, S.A. Buetow, Defining quality of care, Soc. Sci. Med., 51 (11) (2000), pp. 1611-1625

[60] L. Liao, M. Chen, J.J. Rodrigues, X. Lai, S. Vuong, A novel web-enabled healthcare solution on healthvault system, J. Med. Syst., 36 (3) (2012), pp. 1095-1105

[61] L. Devadass, S.S. Sekaran, R. Thinakaran, Cloud computing in healthcare, Int. J. Stud. Res. Technol. Manag., 5 (1) (2017), pp. 25-31

[62] Ichikawa D, Kashiyama M and Ueno T (2017) Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR MhealthUhealth 5(7): e111.

[63] Hannah S Chen, Juliet T Jarrell, Kristy A Carpenter, David S Cohen and Xudong Huang, "Blockchain in Healthcare: A Patient-Centered Model" (2019)

[64] Nguyen H.T., Ngo Q.D., Le V.H., A novel graph-based approach for IoT botnet detection, Int. J. Inf. Secur. (2019), pp. 1-11

[65] Allix K., Jerome Q., Bissyande T.F., Klein J., State R., Traon Y.L., A forensic analysis of android malware – How is malware written and how it could be detected?, Presented at the IEEE 38th Annual Computer Software and Applications Conference (2014), pp. 384-393

[66] Costin Andrei, Zaddach Jonas, Iot malware: Comprehensive survey, analysis framework and case studies, BlackHat USA (2018)

[67] Angrishi Kishore, Turning internet of things (IoT) into internet of vulnerabilities (IoV): IoT botnets, (2017), arXiv preprint arXiv:1702.03681

[68] De Donno Michele, Dragon Nicola, Giaretta Alberto, DDoS-Capable IoT malwares: Comparative analysis and mirai investigation, Security and Communication Networks, Wiley (2018)

[69] BasudebBera, Ashok Kumar Das, Mohammad S. Obaidat, PandiVijayakumar, Kuei-Fang Hsiao "AI-Enabled Blockchain-Based Access Control for Malicious Attacks Detection and Mitigation in IoE"

[70] S. Alsunbul, P. Le, J. Tan, B. Srinivasan, A network defense system for detecting and preventing potential hacking attempts, 2016 International Conference on Information Networking (ICOIN) (2016), pp. 449-454

[71] V. Chang, M. Ramachandran, Towards achieving data security with the cloud computing adoption framework, IEEE Trans. Serv. Comput., 9 (1) (Jan.-Feb. 1 2016), pp. 138-151

[72] V. C. Hu, D. Ferraiolo, and D. R. Kuhn, Assessment of access, control systems.US Department of Commerce, National Institute of, Standards and Technology, 2006.

[73] W. O. Nijeweme-d'Hollosy, L. van Velsen, M. Huygens, and H. Hermens, "Requirements for and barriers towards interoperable ehealth, technology in primary care," IEEE Internet Computing, vol. 19, no. 4, pp. 10–19, July 2015.

[74] D. Di Francesco Maesa, P. Mori, and L. Ricci, "Blockchain based access control," Distributed Applications and Interoperable Systems: 17th IFIP WG 6.1 International Conference, DAIS 2017, Held as Part of the 12th International Federated Conference on Distributed Computing Techniques, DisCoTec 2017, Neuch ˆatel, Switzerland, June 19–22, 2017, Proceedings, pp. 206–220, 2017.

[75] Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo, , Digital Communications and Networks, Volume 4, Issue 3, August 2018, Pages 149-160

[76] T. M. Mitchell, Machine Learning, 1 ed. New York, NY, USA: McGraw-Hill, 1997.

[77] P. Louridas and C. Ebert, ''Machine learning,'' IEEE Softw., vol. 33, no. 5, pp. 110–115, May 2016.

[78] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, KoustabhDolui, Fabio Antonelli, and Mubashir Husain Rehmani. 2019. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys and Tutorials 21, 2 (2019), 1676–1717.

[79] HEMANTHA KRISHNA BHARADWAJ, AAYUSH AGARWAL, VINAY CHAMOLA, NAGA RAJIV LAKKANIGA, VIKAS HASSIJA4, MOHSEN GUIZANI, BIPLAB SIKDAR, A Review on the Role of MachineLearning in Enabling IoT Based Health care Application.

[80] Qi Jia, LinkeGuo, ZhanpengJin, and Yuguang Fang. 2018. Preserving model privacy for machine learning in distributed systems. IEEE Transactions on Parallel and Distributed Systems 29, 8 (2018), 1808–1822.

[81] 85 Xindi Ma, Jianfeng Ma, Hui Li, Qi Jiang, and Sheng Gao. 2018. PDLM: Privacy-Preserving Deep Learning Model on Cloud with Multiple Keys. IEEE Transactions on Services Computing (2018), 1–13

[82] Hui Zhu, Xiaoxia Liu, Rongxing Lu, and Hui Li. 2017. Efficient and Privacy-Preserving Online Medical Prediagnosis Framework Using Nonlinear SVM. IEEE Jounral of Biomedical and Health Informatics 21, 3 (2017), 838–850.

[83] Xiaoqiang Sun, Peng Zhang, Joseph K. Liu, Jianping Yu, and WeixinXie. 2018. Private machine learning classification based on fully homomorphic encryption. IEEE Transactions on Emerging Topics in Computing 6750, c (2018)

[84] R. Tkachenko, I. Izonin, v. chopyak, N. Kryvinska,and N. Lotoshynska, "Piecewise-linear approach formedical insurance costs prediction using sgtm neural-like structure," 11 2018.

[85] R. Tkachenko, I. Izonin, P. Vitynskyi, N. Lotoshynska,and O. Pavlyuk, "Development of the non-iterativesupervised learning predictor based on the itodecomposition and sgtm neural-like structure formanaging medical insurance costs," Data, vol. 3

[86] A. Qayyum, J. Qadir, M. Bilal, and A. Al-Fuqaha,"Secure and robust machine learning for healthcare:A survey," IEEE Reviews in Biomedical Engineering,pp. 1–1, 2020.

[87] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta,"Blockchain-based remote patient monitoring inhealthcare 4.0," in 2019 IEEE 9th International Con-ference on Advanced Computing (IACC), 2019, pp.87–91

[88] Stephen D. Gantz, Daniel R. Philpott, in FISMA and the Risk Management Framework, 2013

[89] F. Tchakounté, F. Hayata, in Mobile Security and Privacy, 2017

[90] SumitPundhir ,Ashokkumardas,mohammadwazid "MADP-IIME: malware attack detection protocol in IoT-enabled industrial multimedia environment using machine learning approach",2021

[91] M. Sprengers, J. van Haaster, in Cyber Guerilla, 2016

[92] Anton Chuvakin, Kevin Schmidt, Chris Phillips, Logging and Log Management 2013, Pages 207-217