BioGecko

Vol 12 Issue 03 2023
ISSN NO:2230-5807

Development of an Artificial Intelligence Model for Detection of Novel Attack on E-Health Systems Using Blockchain

Prof. Dr. Hiteshkumar Nimbark
OM Engineering College, Gujarat, India

Abstract

The world is traveling to the next era of technological enhancements. Artificial intelligence is one such technology that touched almost every industry domain. The pre and post-pandemic scenarios have given birth to many needs in the healthcare sector. The core domains of the Healthcare and pharmaceutical sectors fall under the emergency support industries. E-health is a domain where blockchain can turn the table with many benefits. It can execute fast and automated decisions and actions using blockchain technology. However, detecting the novel attack on e-health systems is vital because such attacks can create warlike situations for health organizations. Hence, this paper presents the artificial intelligence model that can help detect the novel system attack. The proposed method analyzes the novel attacks based on packet loss via jitter events identification using the proposed AI-analyzer algorithm, which can log suspicious incidences.

Keywords: Block chain, artificial intelligence, machine learning, e-health system, novel attack

Introduction

We have deemed blockchain a discovery approach for reliability and security accumulation. In a more accessible view, blockchain is a ledger that stores the determined contracts to assist digital assets in a professional network looking up and gaining [1]. Presented by the bitcoin crypto currency, blockchain increased in popularity because of its exclusive capability to form a distributed economy and placed the base on a well-known digital currency sector. In a blockchain-based program used for logistic supply chain management of COVID-19 polymerase chain response (PCR) screening kits, intelligent contracts can perform a crucial function in monitoring the position of shipment pots of screening kits, determining problematic screening kits, monitoring the state of screening kits at the time of their delivery, and so enable authorities associates to gain access to data to evaluate marketplace demand and supply of screening kits in a precise area. A considerable part of the suggested systems has adopted central structures to gain access to store services and deal with data related to COVID-19. For instance, Singapore's contact reversing method, TraceTogether, employs Bluetooth technology to explore the close contact of a person with an infected patient with COVID-19 [2].

The covid-19 pandemic also improved the temperature sensor-based respiratory system monitoring system requirement. Featuring digital health information can help with classification accuracy if the level of privacy and secureness safety are essential system concerns. Because of its immutability features, blockchain has been recommended as a workable alternative to allow the personal health data market with privacy and security safeguards [3]. The decentralized characteristics of blockchain technology, using its characteristics just as immutability and visibility, make it possible to attain these kinds of goals. Irrespective of its probable gains, there are yet to be issues linked with the execution of blockchain technology in the IoT. This issue may include resource constraints, scalability concerns, and substantial computational requisites [4].

The major challenge is the safety of health care data with lesser communication expense and preventing signaling blockage amid entities. Research suggests a straightforward and practical blockchain-based strategy for e-health care to solve these kinds of concerns. The author (s) pursued to show the community trust amongst the receiver/ users and the critical generation center (KGC). Because of the features, just as tamper-resistant to contracts and responsiveness, blockchain technology keeps the data access protection and level of privacy of every receiver/end-user [5]. E-health systems are going through swift advancement. However, their level of privacy and reliability weaknesses continue to be distinguished. Because of source constraints of node devices and the utility of the decentralized concept, classic privacy solutions cannot fulfill the recent evolution of e-health systems. Thus, blockchain ensures the prospect of resolving these kinds of problems. Blockchain's features comprise allocated storage, data openness, tampering resistance, and good credit sharing, and are significantly preferred in various fields [6].

Blockchain technology can provide an assured alternative to deal with these challenges in a decentralized fashion with no centralized expert. It is essential for e-health services where the individual and the healthcare supplier frequently are needed to show their identification. Blockchain technology can establish digital identities and make their management simpler, thus providing an elevated level of control to the individual than what recent alternatives present. It can generate a digital identity on the blockchain, making it easier for people and agencies to control, providing them with better control through their details and how they manage them. It may produce higher reliability and protection for e-health functions [7].

2. Literature Review

Blockchain has a lot of potential functions in the energy marketplace, which can be noticed in peer-to-peer energy trading, IoT applications incorporating Blockchain, decentralized marketplaces, charging of electric vehicles, and e-mobility [8]. Among the most exciting uses of Blockchain is attack recognition. Attack recognition in Blockchain has ample scope of execution in the event of crypto currency and a smart contract. Mainly linked with Bitcoin, blockchain technology enables the usage of the digital ledger process with public key cryptography and then provides an unalterable, time-stamped chain of wellness information as its content. This concept provides a new basis for healthcare systems and encourages decentralization, immutability, and interoperability [9]. The author recommended employing Blockchain to control the diverse slices in a network robustly and safely. This distributed framework stores info with no alternative entity to assure data reliability and consistency. The author proposed implementing a network chopping option for non-public Networks (NPNs) in health conditions implementing blockchain technology. The alternative seeks to present efficiency solitude throughout wireless networks and a level of privacy [10].

Hyperledger is a Linux framework alternative that can be employed as a foundation system for employing business blockchain. It deploys five frameworks for diverse types of environments and consensus systems. Hyperledger Fabric is a critical execution that allows flexible consensus algorithm execution, smart contract incorporation, and Internet of Things (IoT) support. Subsequently, many of this article's arguments entail its usage and the flexibility it provides. It is significant to observe that it is merely a platform and will not provide a natural business alternative for Blockchain in any circumstance [11]. E-health tasks are a collection of health-related processing alternatives that consider the internet to offer solutions. These uses can range from monitoring a patient's physiological data to the prescription administration procedure in hospital facilities. Among the main issues of E-health is the reliability and security of the data file developed or altered by these kinds of applications. E-health utility data are receptive, considering that they can present details regarding the disease and the solution of a specified patient. That shows illegal persons must not gain access to it. Blockchain alludes to the technology applied to produce Bitcoin. Employing it in many different applications is workable because of its features. Presently, there are analyses on the consider Blockchain technology in applications that require its functionality. IoT is among those applications that suit the usage of Blockchain. [12].

The author shows a specific system for migrating impartial standard e-health systems to a solitary blockchain-based environment. More particularly, the author addressed the concerns of impact in data structures for conventional relational databases and blockchain file sources. The alternative explains the conversion procedure and data harmonization in a specific system for Big E-health data. The execution and examination reveal that critical advancements in data storage, access control, and seamless estimate can be accomplished [13]. The author shows an option to move existing e-health units to a specific Blockchain-based unit, where any services provider can accomplish the entry point to large-scale medical info of patients flawlessly. A critical blockchain network links specific & independent e-health programs without needing them to change their intrinsic procedures. Direct access to patient data files in digital resources kept in off-chain storage is managed with patient-centric programs and policy transactions. With the aid of emulation, we show that the proposed solution can interconnect different e-health systems efficiently [14].

Data snagged from clinical relationships among patients and the care facilities and health info gathered simply by medical sensors provide a unique data resource, alluded to as patient medical records (PMRs), which can be analyzed in different approaches to improving the execution of healthcare solutions. Indiscriminate processing of PMR might cause the security infringement or privacy of patients. The author presented the design and implementing of an e-Health consent management framework, depending on innovative blockchain technologies, for processing PMRs. This evaluation verifies that our system fulfills the criteria for consent administration in e-Health [15]. Healthcare has now become a substantial component of life as it is setting up life-changing improvements day-to-day regardless of artificial intelligence impact on the diagnostic program, specialized system, patient's data storage, access, protection, and any other healthcare smart solutions. Smart health data is an essential component to assist us in resolving healthcare needs. Various researchers are raising Blockchain in innovative health because of its secure, versatile, and trustworthy structures [16].

To our understanding, there are no professions taken out by AI in health care. The modest antique of AI into the market and the complexity of establishing AI into medical workflow have been slightly accountable for the need for job impact. The healthcare jobs most appropriate to be computerized may be those that require coping with digital data, radiology, and pathology, for example, alternatively than those with direct patient contact [17]. The existing system is structured on intelligent decision-making and can quickly produce a decision-making tree. The standard, low-complexity algorithmic pattern of the proposed system causes it appropriate for real-time applications. A proof-of-concept case study of the execution of the CDS was done on Arrhythmia disease [18].

3. Research Methodology

Blockchain technology is a framework that saves blocks of information. Blockchain, described as a sequence of data blocks, is a time-stamped series of immutable information. This backup is alluded to as Digital Ledger. This data in the block is anchored in the perception that it is hard to tamper. The various other users can see the block data of the network system, and thus it is transparent. The blockchain is a blend of the pursuing three methods: Cryptographic Keys, a peer-to-peer network comprising a distributed ledger, and procedures for keeping the trades of data of the block. The beginning block in the blockchain network system is called Genesis block, so its earlier hash is zero. The beginning block does not reference any previous block. If modification happens in any block ‘x,’ in a blockchain that comprises ‘n’ blocks, it gets mirrored in the earlier hash, and so the block hash of each block. Fig.1 shows the proposed methodology, which uses artificial intelligence to analyze time series data system logs to detect novel attacks using distributed blockchain systems.

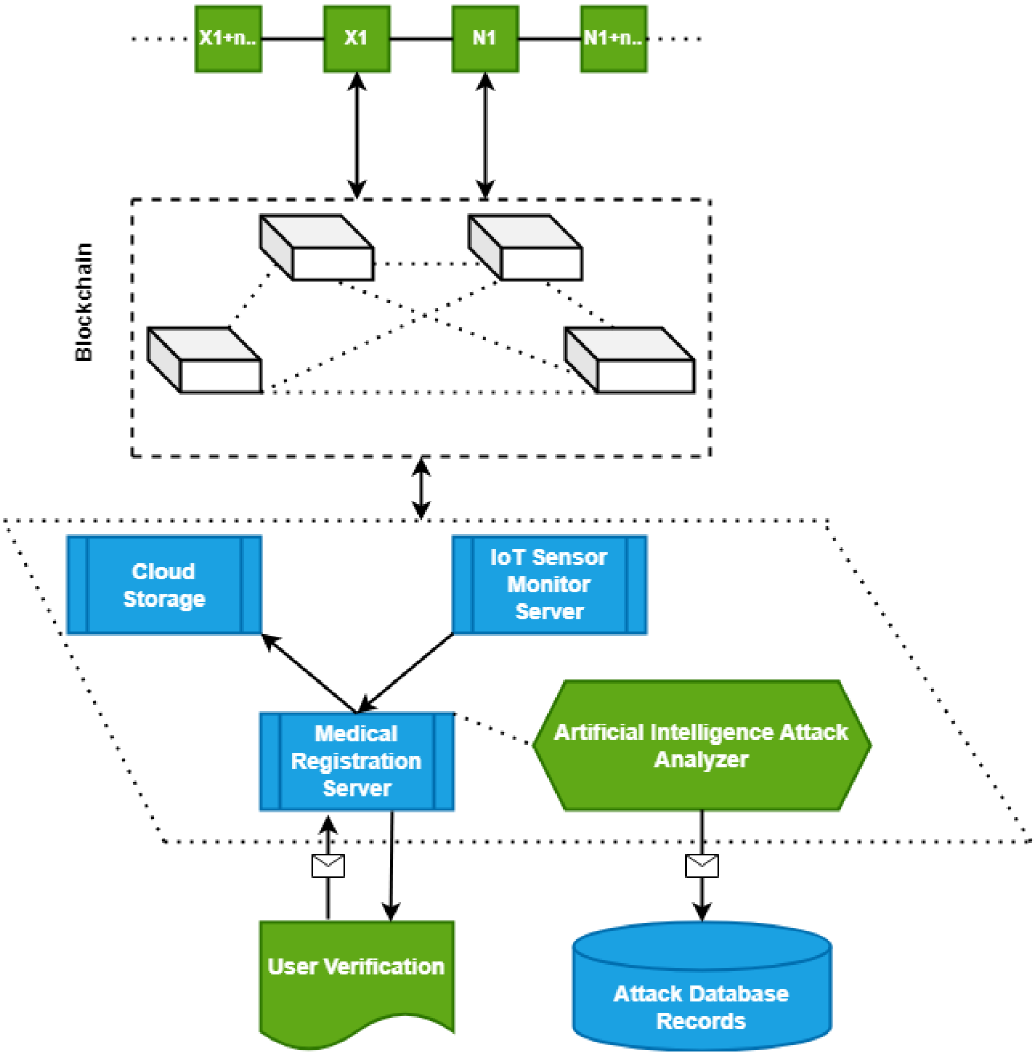
X1+n..
X1
N1
N1+n..
Blockchain
Cloud Storage
IoT Sensor Monitor Server
Medical Registration Server
Artificial Intelligence Attack Analyzer
User Verification
Attack Database Records

Fig.1 Proposed methodology

As shown in Fig. 1 above, in an allocated blockchain framework, the X1 and N1 blocks are supposed to be too diverse request capability blocks communicating with blockchains. Blockchains are connected with cloud servers, IoT servers, and medical registration servers, frequently susceptible to novel attacks. It triggered the request and response after the customer's confirmation. In the proclaimed circumstances, end users will get entry points to cloud servers, IoT devices, and medical registration servers. In the circumstance of confirmation of the user, if confirmation is successful, a jitter happens. The proposed AI analyzer will record the occurrence log for further repeated confirmation. It can utilize the log file to determine the attacker network node and change the network's topological patterns. The forward and reverse request/response will confirm the time frame and level of breach. Further, the following algorithm provides the pseudo-code.

Proposed Algorithm: AI-Analyzer

```
1. Input: log dataset, time series dataset, incoming server request
2. String serverID, clientID, requestID, GatewayID, IPaddress, msgTimeStamp
3. array authenticationArr[]          // details of login credentials validation
4. array sensorsArr[ ]      // holds sensor list for e-health system
5. array networkTraficLog[] //stores jitter timestamp and serverID
6. String AckReq                  // Confirmable request or NonConfirmable request log
7. array msgBlockchain []
8. array msgStatus[] //records Flag 0 and 1
```

```
9. get ( requestID, AckReq]
10. if msgDelay [] && AckReq == 1
11. requestID = ='Valid'
12. else
13. requestID = = 'Jitter'
14. Store serverID, clientID, requestID, GatewayID, IPaddress, msgBlockchain [],   msgTimeStamp
15. if authenticationArr [] != null && AckReq = =1
16. validateReq()
17. accessServer ()
18. else
19. logEvent() //Stores event in database
20. go to step 10
21. if requestID = = 'Jitter'
22. identify_msgBlockchain() // identify block of event
23. freezBlock() //stop access to identified block only
24. SetBlockStatus() // acknowledgement to e-health system about the event
25. CalculatePacketLoss() // Based on msgTimeStamp difference
25. else
23. Set AckReq = =1
24. End
```

The proposed algorithm provides a strategy for detecting novel network attacks using artificial intelligence for blockchain data handling. The core merit of this algorithm is that it keeps the system working in the event of an attack on blocks by separating single-block access to the attacker. So, with healthcare systems rest of the servers works finely. We tested the algorithm using time series data by adding a delay in the request timestamp to simulate the attack. The following section provides the test results.

4. Result and Analysis

To test the proposed algorithm log dataset, time series dataset, and incoming server request are analyzed. The log dataset maintains all server requests and response time stamps. We used an event dataset (i.e., a time series dataset) and calculated packet loss and jitter, as shown in the proposed algorithmic steps. Following Fig. 2 shows the comparative analysis for 'jitter' incidences. We analyzed the data run with and without the proposed algorithm.

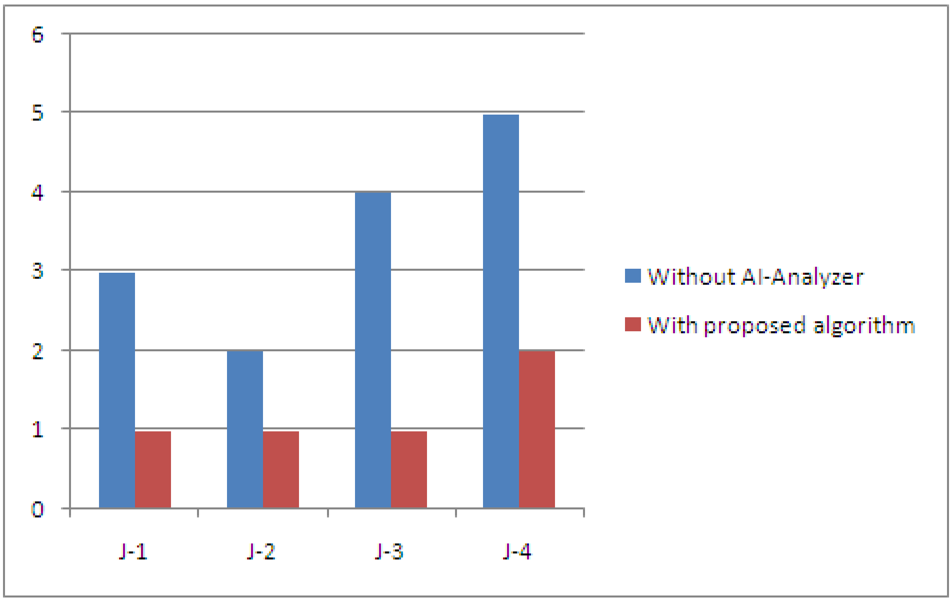

Fig. 2: Comparative analysis for jitter incidences using proposed algorithm

Similarly, we analyzed the overall system performance for packet loss when blockchain interactions are via multiple servers. Fig. 3 shows the overall system performance for the proposed algorithm and is compared with the system run without the proposed algorithm.

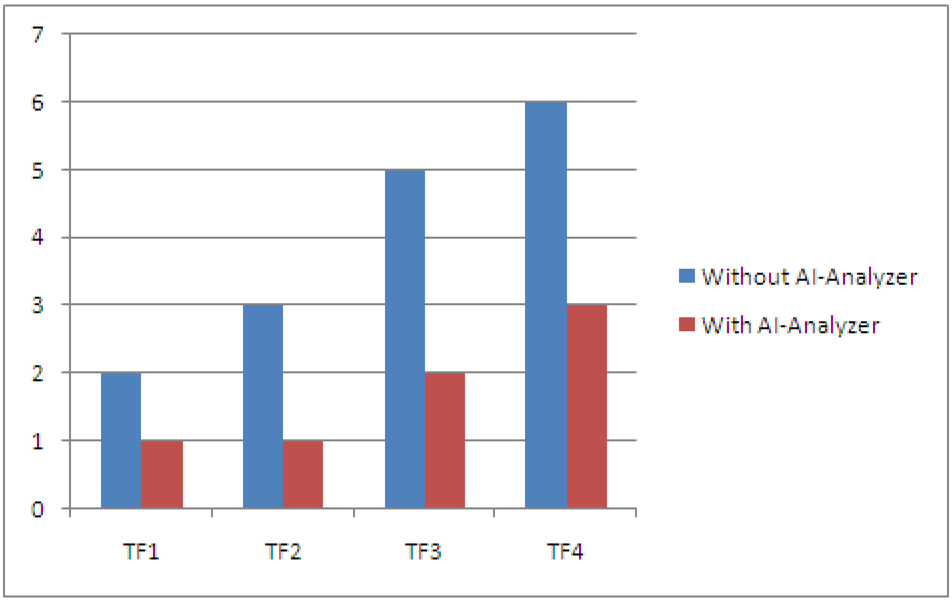

Fig. 3: System performance for packet loss

The medical registration server cannot be shut down as it is for patient security, and hundreds of sensors, actuators, and devices are connected with it. So, blockchain security can be provided in chunks where the multi-server scenario is present.

5. Conclusion

This paper presents the artificial intelligence model that can detect a novel system attack. The proposed method analyzes the occurrences of the novel attacks employing time series data, which is processed using the proposed algorithm 'AI-analyzer' and calculated packet loss. It analyzes the system performance for jitter events. The proposed research can benefit e-health systems for multiple server support where the system shutdown of the blockchain network can be avoided using alternative topological routing. The proposed research provides a facility to record the logs for suspicious incidences. This artificial intelligence model can support IoT applications with a blockchain framework for many domains like healthcare, agriculture, automation, etc. Future research can also be done in the pharmaceutical domain to secure the industry's supply chain management.

References:

[1]Huynh-The, T., Gadekallu, T. R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., & Liyanage, M. (2023). Blockchain for the metaverse: A Review. Future Generation Computer Systems.

[2]Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2023). Blockchain and COVID-19 pandemic: Applications and challenges. Cluster Computing, 1-26.

[3]Alsuqaih, H. N., Hamdan, W., Elmessiry, H., & Abulkasim, H. (2023). An efficient privacy-preserving control mechanism based on blockchain for E-health applications. Alexandria Engineering Journal, 73, 159-172.

[4] Meisami, S., Meisami, S., Yousefi, M., & Aref, M. R. (2023). Combining Blockchain and IOT for Decentralized Healthcare Data Management. arXiv preprint arXiv:2304.00127.

[5]Saxena, S., Arya, N., Bharti, S. K., & Dwivedi, V. (2023, March). A Lightweight and Efficient Scheme for e-Health Care System using Blockchain Technology. In 2023 6th International Conference on Information Systems and Computer Networks (ISCON) (pp. 1-5). IEEE.

[6]Xiang, X., & Zhao, X. (2022). Blockchain-assisted searchable attribute-based encryption for e-health systems. Journal of Systems Architecture, 124, 102417.

[7]Satybaldy, A., Hasselgren, A., & Nowostawski, M. (2022). Decentralized Identity Management for E-Health Applications: State-of-the-Art and Guidance for Future Work. Blockchain in Healthcare Today, 5(Special Issue).

[8]Gadekallu, T. R., Manoj, M. K., Kumar, N., Hakak, S., & Bhattacharya, S. (2021). Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications. IEEE Internet of Things Magazine, 4(3), 30-33.

[9]CHELLADURAI, M. U., Pandian, S., & Ramasamy, K. (2021). A blockchain based patient centric electronic health record storage and integrity management for e-Health systems. Health Policy and Technology, 10(4), 100513.

[10]Gonçalves, J. P. D. B., De Resende, H. C., Municio, E., Villaça, R., & Marquez-Barja, J. M. (2021, January). Securing E-Health Networks by applying Network Slicing and Blockchain Techniques. In 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-2). IEEE.

[11]Biswas, S., Sharif, K., Li, F., & Mohanty, S. (2020). Blockchain for e-health-care systems: Easier said than done. Computer, 53(7), 57-67.

[12]Moreira Neto, M., Coutinho, E. F., Moreira, L. O., & de Souza, J. N. (2020, March). Toward blockchain technology in iot applications: An analysis for e-health applications. In Internet of Things. A Confluence of Many Disciplines: Second IFIP International Cross-Domain Conference, IFIPIoT 2019, Tampa, FL, USA, October 31–November 1, 2019, Revised Selected Papers (pp. 36-50). Cham: Springer International Publishing.

[13]Biswas, S., Sharif, K., Li, F., Latif, Z., Kanhere, S. S., & Mohanty, S. P. (2020). Interoperability and synchronization management of blockchain-based decentralized e-health systems. IEEE Transactions on Engineering Management, 67(4), 1363-1376.

[14]Biswas, S., Sharif, K., Li, F., Alam, I., & Mohanty, S. P. (2020). DAAC: Digital asset access control in a unified blockchain based e-health system. IEEE Transactions on Big Data, 8(5), 1273-1287.

[15]Agbo, C. C., & Mahmoud, Q. H. (2020, October). Design and implementation of a blockchain-based e-health consent management framework. In 2020 ieee international conference on systems, man, and cybernetics (smc) (pp. 812-817). IEEE.

[16]Naqvi, M. R., Aslam, M., Iqbal, M. W., Shahzad, S. K., Malik, M., & Tahir, M. U. (2020, June). Study of block chain and its impact on Internet of Health Things (IoHT): challenges and opportunities. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-6). IEEE.

[17]Davenport, T., & Kalakota, R. (2019). The potential for artificial intelligence in healthcare. Future healthcare journal, 6(2), 94.

[18]Naghshvarianjahromi, M., Kumar, S., & Deen, M. J. (2019). Brain-inspired intelligence for real-time health situation understanding in smart e-health home applications. IEEE Access, 7, 180106-180126.