Collaborative Learning for Cyberattack Detection in Blockchain Networks And Wireless Networks

Jegadeesan R , Midhun chakkaravarthy, Dr. Mudassir Khan
Computer Science and Engineering Jyothishmathi Institute of Technology and Science Karimnagar, India
Computer Science and Engineering King Khalid University , Saudi Arabia
CSE, Lincoln University College Malaysia

ramjaganjagan@gmail.com, midhun@lincoln.edu.my, mkmiyob@kku.edu.sa

Abstract— This blockchain network will serve two purposes, i.e., to generate the real traffic data (including both normal data and attack data) for our learning models and to implement real time experiments to evaluate the performance of our proposed intrusion detection framework. To the best of our knowledge, this is the first dataset that is synthesized in a laboratory for cyber attacks in a blockchain network. We then propose a novel collaborative learning model that allows efficient deployment in the blockchain network to detect attacks. The main idea of the proposed learning model is to enable blockchain nodes to actively collect data, learn the knowledge from data using the Deep Belief Network, and then share the knowledge learned from its data with other blockchain nodes in the network. In this way, we cannot only leverage the knowledge from all the nodes in the network but also do not need to gather all raw data for training at a centralized node like conventional centralized learning solutions. Such a framework can also avoid the risk of exposing local data's privacy as well as excessive network overhead/congestion. Both intensive simulations and real-time experiments clearly show that our proposed intrusion detection framework can achieve an accuracy of up to 98.6% in detecting attacks.

Keywords—*Cyberattack, Blockchain Networks, Wireless Networks, Bitcoin network, and Neural Network*

INTRODUCTION

Blockchain technology is quickly replacing older, more inefficient methods of data management and storage. Because it offers so many advantages over earlier methods, its implementation was inevitable. In contrast to conventional data management approaches, blockchain technology permits data storage across numerous nodes rather than a single central repository. Reduced likelihood of data bottlenecks and single points of failure is achieved by utilizing numerous nodes simultaneously for handling and receiving data. The ability to partition data storage is another intriguing feature of blockchain technology. It is impossible to remove or alter data bits once they have been confirmed; this is a permanent state. The immutability, autonomy, and audit ability of blockchain technology ensure that data is protected from unauthorized individuals. For this reason,

many people employ the technology that underpins blockchain. It touches on a variety of topics, including infrastructure, healthcare, the Internet of Things, and finances.

The crypto[6] currency and financial transaction industries have helped propel blockchain[8] technology to the forefront of public attention in recent years. Because of this, hackers find it quite appealing. The assault on the KuCoin crypto currency market in Singapore in September 2020 is one incident that lendscredenceto this assertion. The incident led to the theft of digital assets valued at about $281 million. One of the most famous bitcoin[1] platforms, Binance, had a major security flaw discovered in May2019. Bypassing the exchange's security safeguards, hackers secretly stole seven grand worth of bit coins from unsuspecting consumers. The result was a loss of almost $40 million for the exchange. North Korean hackers stole $400 million worth of digital assets from seven separate crypto currency platforms in 2201, according to a Chainalysis analysis dated January 2022. More and more, cybercriminals are aiming their attacks at platforms that facilitate the exchange of virtual currency. However, at this exact moment, certain crucial applications of blockchain technology are in jeopardy. Food and healthcare supply lines are two examples of these types of uses. Not only are these things costly and time-consuming, but they also endangering people's well-being. The significance of identifying and preventing hacks on blockchain networks is highlighted when this is considered.

Current security measures are ineffective against Brute Force Password (BP) and Transaction Flooding (FoT), the two most prevalent attacks on blockchain networks. Once authorization is granted, intrusion detection systems will no longer function. Because of this, users are free to execute whatever harmful applications or commands they like. There should be more than one authentication method to make hack detection systems more robust. Because of this, they will be less likely to be attacked. Blockchain vulnerabilities, such as the Byzantine Protocol (BP), Fork of Transaction (FoT), and Man-in-the-Middle (MitM) attacks, have been the subject of extensive study. The doctors took the patient's blood pressure readings using a Raspberry Pi, a MacBook Air, and a smart phone. The high utilization of both memory and CPU was clearly associated with the ability to detect BP attacks. Updating and verifying the Monero blockchain network record required the writers one month of labor..

LITERATURE REVIEW

Title: Bitcoin: APeer-to-Peer Electronic Cash System, Author’s: S. Nakamoto.

Internet money transactions would be completely decentralized with decentralized peer-to-peer electronic cash. People can still multitask when a third party is involved, even while using digital messages. To reduce the likelihood of unnecessary expenditure, we propose a decentralized network design. The network verifies the legitimacy of transactions using a variety of hash-based

proof-of-work algorithms. In order to maintain the integrity of the transaction record, it is strictly forbidden to make any changes to items that contain a timestamp. The recorded occurrences were eventually tracked down to the most powerful CPU pool, confirming the case after numerousoccasions.Criminalshaveahardertimebreakingintothe network since the most powerful CPUs can construct the longest chain quickly. The network's[14] architecture can be arranged in a methodical way. Every node has the ability to join or exit the current network at any given moment. Everyone must verify the correctness of message transmissions, and the longest proof-of-work chain serves as a legal record of events that transpired while they were away.

Title: Applications of blockchains in the Internet of Things: A comprehensive survey, Author's: M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani.

Bitcoin, the first decentralized digital payment network, was built using blockchain technology. Major operational changes to digital currencies are being brought about by the employment of this technology. Another function of a blockchain is to record and confirm all network transactions in perpetuity. Since more and more people are utilizing this technology, non-business related topics, such as the Internet of Things, have recently gained more attention. A lot of individuals believe that in order to build a trustworthy, open, and secure Internet of Things, blockchain technology is essential. The study's overarching objective is to provide a detailed account of the most effective practices in this field at the present time. First, we'll fill you in on blockchains, explaining what they are, how they function, and how they can be utilized to construct independent systems that can be audited. We will start by examining the issues with the current centralized Internet of Things solutions. The presenter will discuss the ways in which blockchain technology has aided academic institutions and companies in creating a trustworthy and decentralized IoT ecosystem.

The urbanization of the world has given rise to numerous new ecological, socioeconomic, and political issues. In many cases, these issues significantly impact people's level of contentment and happiness. Residents of urban areas may have the belief that "smart city" concepts hold the key to resolving common issues. Smart towns can achieve these aims by enriching the lives of all residents, increasing access to public services, and optimizing the utilization of existing resources. In order to be successful, "smart cities" projects must integrate many forms of electronic communication and data storage. Despite its relative youth, blockchain technology offers numerous advantages that make it an excellent pick. Various elements are comprised in the set, including decentralization, automation, privacy, transparency, democratic governance, improved security measures, and reduced uncertainty. Blockchain technology will have a significant impact on the services provided

by smart cities, notwithstanding its imperfections. A comprehensive review of research on the potential applications of blockchain technology in smart cities is presented here. We will begin by providing you with some background information and a brief summary of the primary papers. After this, we will investigate the potential applications of blockchain technology in smart towns. Distributing energy, transporting people and commodities, providing health care, and managing the supply chain are all examples of applications for these types of networks[14]. Lastly, we will address several significant matters pertaining to the broader context.

Title: Blockchain and crypto currencies: Model,techniques, and applications, Author's:Y.YuanandF.-Y.Wang.

Advances in blockchain technology have been substantial in recent years. Blockchain is essential for decentralized record keeping and digital currencies such as Bitcoin[1]. Decentralized, autonomous civilizations that are impregnable to outside forces can emerge thanks to this technology. While this approach could be useful in certain cases, it is most effective when combined with preexisting systems, procedures, and resources. This paper's research on blockchain technology and digital currency was extensive. The article discusses the current state and potential future developments within the Bitcoin[1] and crypto[6] currency ecosystems. Along with the primary objectives, technical advantages, and six stages required to construct a blockchain[8], it covers a lot of other ground as well. Potential future applications of blockchain technology and digital money are discussed in this section of the article. More studies on this crucial and potentially useful topic may appear in scholarly journals down the road.

PROBLEM STATEMENT

The implementation of a strategy that takes use of the information that is gathered independentlybyeachnodeissomethingthatisstronglyencouraged.Thiswillensure the safety of the given training data sets, which are the raw data collected by each node in the network. Here, establishing the decentralized blockchain[8] network is crucial. We take a close look at all the possible data collection methods that each node in the network could employ to feed into a deep learning model. Using the provided data, a Centralized Server (CS) will send the model. Experts in computer science could provide bitcoin[1] networks[7] with technical support in two ways. Either the start or the end of the process is indicated by this. We will add each model immediately once the group system is purchased. As soon as the learning process is over, the "global model," the final version of the model, is transmitted to all participating nodes. After some time has passed and each learning node's deep learning framework[21] has matured, they will reach consensus on a single training model. This method reduces the likelihood of disclosure of specific information regarding the learning nodes in the network. To be more specific, it lets you spot possible threats in blockchain[8] networks.

We promise that the suggested method will find holes in the given network 98.6 percent of the time. Our suggested learning approach allows nodes in a network[14][23] to learn from each other by easing the sharing of data from individual models. Using this method, a lot of data can be sent between nodes without any important details being swapped.

A. ADVANTAGES OF PROPOSED SYSTEM

- A covert network[14][23] was implemented in our laboratory to conduct real-time testing of our proposed learning model without any awareness. This network[23] was set up to allow the use of real bitcoin[1] data. Making machine learning algorithms that can identify blockchain network vulnerabilities should be a breeze using the suggested BNaT dataset. The bulk of the data required to probe blockchain[8] network thefts is present in this file. Details were gathered by the research group. Please use the links provided to find out more about the collection.
- The Blockchain[8][15] Intrusion Detection (BC-ID) technology safeguards the blockchain network[14][23] and its data from illegal access. This software can quickly find attack[13] samples and label them correctly. Information pertaining to network[14][23] traffic is also monitored. It then uses this data to get attributes in the next step.
- To speed up the process of finding possible threats in decentralized blockchain networks[7][8][23], we suggest a collaborative decentralized learning method. With this method, entire nodes in the blockchain can trade models without compromising the integrity of their own data. Using this method, locating breaks becomes much easier. We used both online and offline sources to find out how effective our strategy was.
- The suggested method surpasses the state-of-the-art in machine learning, according to experiments and simulations. The creation and implementation of learning models in blockchain networks[7][8][23] for the purpose of real-time threat detection[24] and monitoring[22] is our principal focus. This will be achieved with the help of our research.

B. Existing System

The use of ML models to real-world blockchain[8] traffic, however, has gotten surprisingly little attention. This encompasses tests that aim to simulate attacks[13] on blockchain[8][14][23] networks or the generation of false data. This category is also being tested. The authors have devised a system to collect information about blockchain traffic. A publicly accessible Bitcoin[1] server was the starting point for visitors to observe and record data. Upon routing all traffic to this node, the transfer began. A device set up as a node in the Bitcoin[1][23] network was the target of their Denial of Service (DoS) attack[13], which they carried out using Eclipse. Because of this, they had a better understanding of illicit activity. A deep learning auto encoder model was built using the

data presented before. Applying this strategy could lead to problems. Throughout their research, the writers drew on databases that were available for both paid and unpaid access. The subsequent step was to create an LSTM capable of detecting frequently occurring cases within the dataset. After that, they used the information from their blockchain[8] to build a CGAN model. The goal was to make it look like low- rate distributed[10][16] denial of service (LDoS) attacks, therefore they succeeded. A whopping 93% of the time, the ranking was spot on.

The writers meticulously analyzed the network[14][23] trace pathways both prior to and following the breach. The Ethereum network[14] was hit by a Link Flood attack (LFA)[13]. The assault shared several characteristics of a distributed [10] denial of service (DDoS) assault. The authors assert that they used a Recurrent Neural Network (RNN) to analyze the trace route data and find network vulnerabilities. The study found that locating an attack[13] seems to be a 99.99 percent chance.

SYSTEM ARCHITECTURE

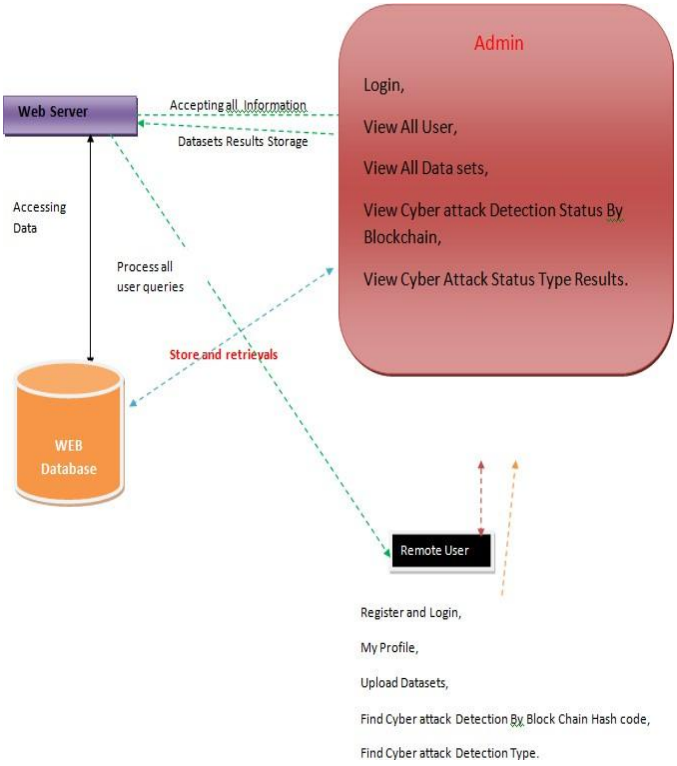
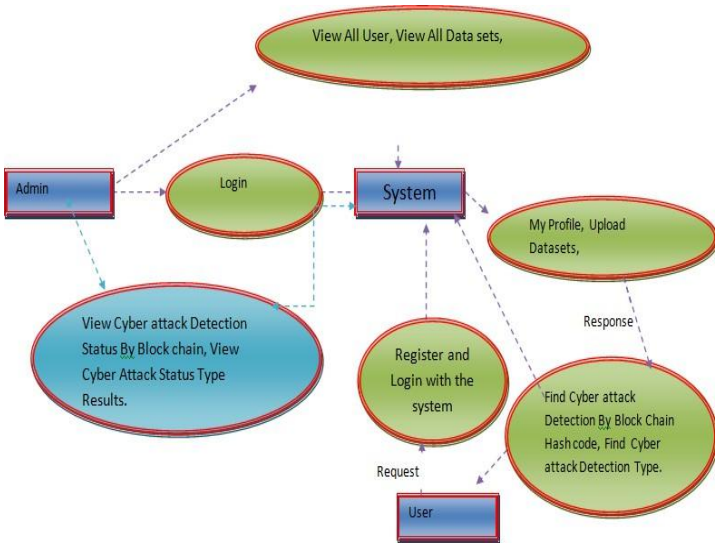


Fig. 1. System Architecture

Data Flow Diagram

One definition of the abbreviation "DFD" is "data flow diagram." Looking at the database plan could help you comprehend the data flow through the system orprocess. People who work as freelancers or in related fields often share resources and methods. There are no decision trees, sequences, or paths shown in the data flow diagram. This drawing tool can improve communication and collaboration amongst customers, direct staff, and upper management. We can evaluate the



efficacy of our current plans and goals with this approach.

Fig. 2. Data Flow Diagram level 0

An appealing way to show how two separate ideas have changed over time is via a SysML usage context map. Three separate visuals are employed to depict the data. Context diagrams are great for showing how something can be used in many situations, whether it's a formal or informal context. Due of their interconnections, things possess a plethora of additional features. There are a lot of key similarities between use case diagrams and UML behavioral diagrams. You might hear this kind of diagram called a use-case diagram somewhere. Researching the system's goals, the different kinds of users, and any needs that may emerge before, during, or after creation is the next step.

A "class diagram." Additionally, it shows the connections between class names and the many uses for those classes. The incorporation of these charts into models gives them the appearance of being three-dimensional. You can use many different patterns to draw attention to the connections between the photos. You will get all the necessary details to carry out any strategy in this book. Every single living thing can be grouped into subgroups according to shared traits, modes of communication, and social networks[7][23]. You may only expect partial results from this tool; it can only categorize things.

The ability to foresee and head off problems is crucial for any project manager. Your level of success in life is influenced by your ability to think independently, create links, and recognize similarities. In order to discover new categories, the strategy makes use of observational data and a very rigorous statistical method. The most common way to show activities is with an activity graph, which shows the connection between two things. Some people have a natural talent for putting into words all the different mental pictures needed to make a well-informed choice. The ability to generate multiple mental models is critical for making a well-informed choice.

IMPLEMENTATION

C. MODULES:

- *Admin*

The only person who knows the password to this area is the administrator. Users are granted access to a wide range of functionalities upon successful login, such as viewing all individuals and navigating through all databases. The following resources provide more information about how Blockchain[8] chooses and ranks the steps of cyber attack detection[24]

- *View and Authorize Users*

The module provides a comprehensive list of all allowed users to the supervisor after processing Members of the administrative team have access to user profiles that contain personal information including names, email addresses, and physical addresses. Another alternative is to provide users with access permissions.

- *User*

You can expect to meet n people in this region. You must finish the registration process before you can continue. The database will be updated with the user's details once the registration procedure is finished. He will be granted access to his login and the associated legal privileges once the registration and payment processes are finished. A plethora of services are available to consumers once they successfully log in. Among these capabilities are the ability to see profiles, access datasets, view incursions, and verify registration and identification. Make sure you're familiar with the many types of attacks[13] that target blockchain[8] hash codes.

OUTPUT DESIGN AND RESULTS

Performing a validation test to determine the strategy's efficacy is crucial. A system's usefulness is greatly affected by the quantity of high-quality, meaningful data it generates. Using the user-selected operational mode can help all stakeholders understand how the system is supposed to work. Think on the format (picture or text) that you will use to save the final product on your computer.

➢ *Validation Checking*

To determine the veracity of a claim, take into account the following:

➢ *Text Field:*

Use the specified characters to keep the text box inside the permitted character limit. This isn't necessarily the case, even when certain tables have a specific arrangement. Inputting the incorrect number will result in the display of an error notice.

➢ *Numeric Field:*

The digits 0 through 9 are all that are relevant here. The test will be deemed unsuccessful and a message will be sent to the recipient if no letters are found. The outcome is readily apparent as a result of the thorough integration of all components. In every step, getting your hands on models is essential. The system's components were thoroughly tested before assembly. In order to identify coding mistakes, we conduct an exhaustive analysis of the program's empirical test outcomes. Every part has to work on its own while the test is underway. If the data is inaccurate, the system might not function properly, according to the review.

➢ *Preparation of Test Data*

Subsequent research has validated these findings. Verifying the accuracy of the test results is a prerequisite to assessing the system. The method's efficacy can be evaluated with up-to-date data. Other security holes can be discovered during the forthcoming system testing using sample data. We have previously examined the assessment techniques that can address these concerns. An additional facet of this is preserving the modifications for prospective future applications.

People require instructions on how to utilize new tools properly. At the end of the project life cycle, prospective clients were given a detailed explanation of how everything worked. This method should be easier for those who have trouble using technology to adopt, which will improve their ability to learn and communicate.

Fig. 3. Admin Home Page

Fig. 4. User Home Page

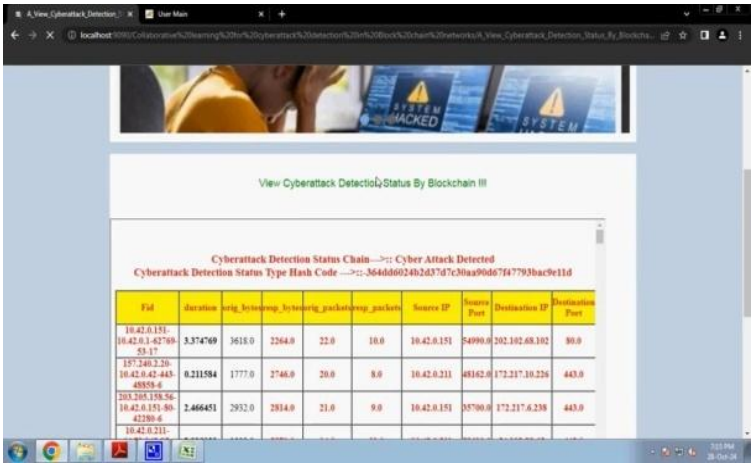


Fig. 5 View Cyber attack Detection Status By Blockchain

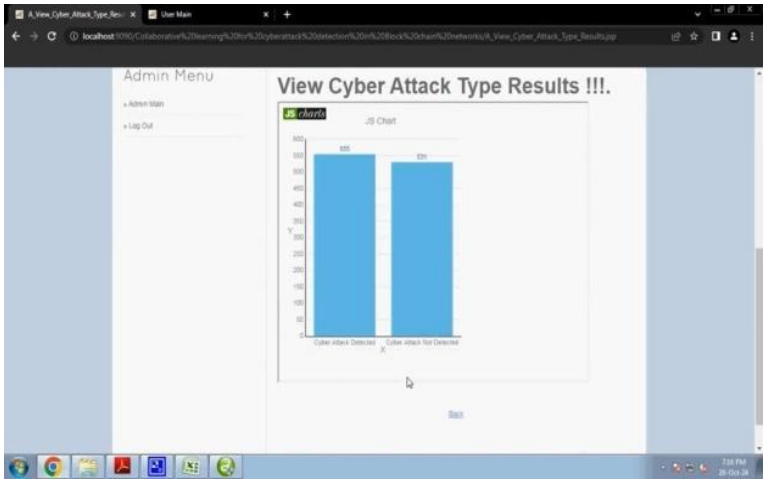


Fig. 6. View Cyber Attack Type Results in BarChart

CONCLUSION

The implementation of a fresh strategy for collaborative learning, we conducted an investigation to identify potential weak points in blockchain networks. We created a blockchain network as part of our research that was only accessible by those with restricted access. To train our algorithms, we utilize both positive and negative datasets provided by blockchain network participants. It is employed in order to assess the efficacy of the learning approach that is currently being used. This, in turn, ensures that our learning model is fully compatible with the bitcoin ecosystem. Because the nodes that comprise a blockchain network gather, analyze, and distribute data beforehand, they can foresee and thwart attacks. By employing this novel approach, the advantages of blockchain technology are maintained while centralized learning techniques are improved. It is able to achieve this goal by resolving issues like the cyber security threats connected to centralized learning systems and the systems' vulnerability to congestion. There is both theoretical and quantitative evidence to support the proposed structure. For blockchain networks to increase their level of security, the data must cover a greater variety of potential dangers.

D. FUTURE ENHANCEMENT

The Centralized Server (CS) can be a boot node or any full node in the blockchain network. The CS will then aggregate all the trained models and send the aggregated model (i.e., the global model) back to the participated learning nodes. By repeating this process, the learning nodes can gradually update their deep learning models and finally reach convergence (to the global training model). In this way, we can not only improve the accuracy of detecting cyber attacks in blockchain networks but also eliminate the risks of exposing local data of learning nodes over the network. Our proposed model can achieve an accuracy of up to 98.6% in detecting cyber attacks in the considered network. Moreover, in our proposed learning model, even though the nodes do not need to share their raw data, they still can learn useful information from other nodes in the network through extracting information from shared trained models.

REFERENCES

[1] S.Nakamoto, “Bitcoin: APeer-to Peer Electronic Cash System, ”2008. [Online]. Available:https://bitcoin.org/bitcoin.pdf

[2] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of blockchains in the Internet of Things: A comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, Dec.2018.

[3] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, “A survey of blockchain technology applied to smart cities: Research issues and challenges,” IEEE CommunicationsSurveys&Tutorials,vol.21,no.3,pp.2794–2830,Feb.2019.

[4]S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, “Interoperability and synchronization management of blockchain-based decentralized e-healthsystems,” IEEE TransactionsonEngineeringManagement,vol.67,no.4,pp. 1363–1376, June 2020.

[5] Y. Yuan and F.-Y. Wang, “Blockchain and cryptocurrencies: Model, techniques, and applications,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1421–1428, July 2018.

[6] “The 10 Biggest Crypto Exchange Hacks In History,” Accessed: Feb. 14, 2022. [Online].Available:https://crystalblockchain.com/articles/the-10-biggest- cryptoexchange-hacks-in-history

[7]“North Korean Hackers Have Prolific Year as Their Unlaundered Crypto currency Holdings Reach All-time High,”Accessed:Feb.14,2022.[Online]. Available:https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-yearas-their-total unlaundered-cryptocurrency-holdings-reach-all-time-high

[8] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, “Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities,” IEEE Access, vol. 7, pp. 85 727–85 745, Jun. 2019.

[9] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, “Blockchain based soy bean trace ability in agricultural supply chain,” IEEEAccess, vol.7,pp. 73295–73 305, May 2019.

[10] S. Bu, F. R. Yu, X. P. Liu, P. Mason, and H. Tang, “Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks,” IEEE transactions on vehicular technology, vol. 60, no. 3, pp. 1025–1036, Dec. 2010.

[11] X. Wang, X. Zha, G. Yu, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, “Attack and defence of ethereum remote apis,” in 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.

[12] J. Ot´avio Chervinski, D. Kreutz, and J. Yu, “Analysis of transaction flooding attacks against Monero,” in IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, May 2021, pp. 1–8.

[13] J. Choi, B. Ahn, G. Bere, S. Ahmad, H. A. Mantooth, and T. Kim, “Blockchain- based man-in-the-middle (mitm) attack detection for photovoltaic systems,” in IEEE Design Methodologies Conference (DMC), July 2021, pp. 1–6.

[14] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network intrusion detection for IoT security based on learning techniques,” IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671–2701, Jan. 2019.

[15] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, “Survey on SDN based network intrusion detection system using machine learning approaches,” Peer-to-Peer Networking and Applications, vol. 12, no. 2, pp. 493–501, Mar. 2019.

[16] M. Idhammad, K. Afdel, and M. Belouch, “Distributed intrusion detection system for cloud environments based on data mining techniques,” Procedia Computer Science, vol. 127, pp. 35–41, Jan. 2018.

[17] K.-D.Lu, G.-Q.Zeng, X.Luo,J. Weng, W. Luo, and Y.Wu, “Evolutionary deep belief network for cyber-attack detection in industrial automation and controlsystem,” IEEE Transactionson Industrial Informatics,vol.17,no.11,pp. 7618–7627, Nov. 2021.

[18] L.Vu, V.L.Cao, Q.U.Nguyen, D.N.Nguyen, D.T.Hoang, and E.Dutkiewicz, “Learning latent representation for iot anomaly detection,” IEEE Transactions on Cybernetics, pp. 1–14, Sep. 2020.

[19] C. Tan, F. Sun, T. Kong, W. Zhang, C. Yang, and C. Liu, “A survey on deep transfer learning,” in Int. Conf. on Artificial Neural Networks. Rhodes, Greece: Springer, Oct. 2018, pp. 270–279.

[20] M.U.Hassan,M. H.Rehmani, and J.Chen, “Anomaly detection in blockchain networks: Acomprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 289–318, Jan. 2023. [21] P. Kumar, R. Kumar, G. Gupta, and R. Tripathi, “A distributed framework for detecting DDoS attacks in smart contract- based Blockchain- IoT systems by leveraging fog computing,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 6, pp. 1–31, June 2021.

[21] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, “A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks,”IEEE InternetofThingsJournal,vol.8,no.12,pp.9463–9472,June 2020.

[22] J. Kim, M. Nakashima, W. Fan, S. Wuthier, X. Zhou, I. Kim, and S.-Y. Chang, “Anomaly detection based on traffic monitoring for secure blockchain networking,”in IEEE International Conference on Blockchain and Cryptocurrency (ICBC),Sydney, Australia, May 2021, pp. 1–9.

[23] Z. Liu and X. Yin, “LSTM-CGAN: towards generating low-rate DDoS adversarial samples for blockchain-based wireless network detection models,” IEEE Access, vol. 9, pp. 22 616–22 625, Feb. 2021.

[24] W. Cao, Y. Huang, D. Li, F. Yang, X. Jiang, and J. Yang, “A blockchain based link-flooding attack detection scheme,” in IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), vol. 4, Chongqing, China, June 2021, pp. 1665–1669.