IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, May 2022
Impact Factor: 6.252

An Analytical Approach for Optimization of Block Chain Security for Internet of Things

Mr. Harshal Nikam[1] and Dr. R. M. Deshmukh[2]
Professor and Head, Department of Electronics and Telecommunication[2]
Dr. Rajendra Gode Institute of Technology & Research, Amravati, Maharashtra, India
harshalnkm@gmail.com[1] and ravindra.dshmkh@gmail.com[2]

Abstract: *The number of smart devices or IOT devices either it may be a smart phone, smart home, tablet or any wearable devices are connected to internet are increasing day by day. Due to this numerous number of security threats are searching for loopholes that are ready to exploit any type of network. Security threats have become critical challenges against the backdrop of recent rapid raising advancements of IOT technology that demands continuous and responsive action. As a demanding technology Internet of Things (IoT) needs best information security features for effective IOT smart city and technological activity development. In this paper an Implementation of IoT system using Block Chain Security Analysis for Malicious Attack and Intrusion Prevention is presented. The block chain distributed behavior makes this system more immune and robust for a single failure. A Zero-Knowledge proof technique is applied for preventing the third party from checking user's original information. Integrity validation test and avalanche effect technique is processed for block chain, MD5 and SHA-256 which results the proposed block chain technology has better security.*

Keywords: Block Chain, Internet of Things, Intrusion Detection, Malicious Attack, Security Threats

I. INTRODUCTION

An Internet of Things (IoT) network is formed with the networking of internet-connected devices that are embedded with electronics, sensor devices, and other hardware that can be remotely observed and controlled. Things on the Internet can be associated with an automobile with sensors imparted to notify the driver when tire pressure is reduced, or any natural or human-made item dispensed an IP can move information over a system. Differently, enterprises utilize IoT to work all the more productively, better comprehend clients to convey upgraded client assistance, improve essential leadership, and increment the business's estimation. IoT is not a Internet-associated buyer gadget. IoT is the innovation that manufactures frameworks fit for detected by its own and reacting to upgrades from this present reality without human intercession. To build up a strategy stream for a distinct structure over which an IoT arrangement is assembled. Actuators are a thing regarding the Internet of Things, ought to be outfitted with sensors and actuators in this manner enabling to produce, acknowledge, and procedure signals. Data Acquisition Systems is the sensors' information begins in simple structure and changed over into computerized streams for further examination. Information procurement frameworks play out these information agglomeration and transformation techniques. Edge Analytics is the IoT information that has been digitalized, collected, and might require further handling before it enters the server farm. Cloud Analytics is the information that needs extra top to bottom procedure gets sent to physical server farms or cloud based frameworks. [7] AI and blockchain are among the key drivers behind innovation today. Both are introducing radical shifts in every aspect of our life and predicted to contribute trillions of US dollars to the global economy. The future is here, with autonomous cars and charming assistants who can make appointments on your behalf in natural conversations. And the arrival of new content and economy sharing platforms will mean that users will no longer be forced to trust "unreliable middlemen" such as Facebook, Yahoo, and Equifax. AI, as defined by Marvin Minsky and John McCarthy the fathers of the field is any task performed by a program or a machine that seems to require intelligence. AI systems often exhibit the following behaviors associated with human intelligence: planning, learning, reasoning, and problem solving, as well as social intelligence and creativity. The recent resurgence in AI is fueled by breakthroughs in machine learning, especially within the field of deep learning. It has also been driven by the explosion in available data, making the training of machine learning algorithms more effective. Besides bringing many exciting advancements, such as self-driving cars and delivery robots, .[13] AI also causes a series of concerns,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, May 2022
Impact Factor: 6.252

from the creation of fake news such as fake and realistic photos, voice, and adult films to the invasion of privacy. There are also concerns about the monopolization of AI power by a few big players, such as Google, Microsoft, and Amazon, because of high barriers to acquiring data, talent, and computing resources. A blockchain is a public ledger, shared and agreed on by all users in a distributed network. Data records, for example, transactions, are stored in blocks together with hash values and timestamps. Every block is connected to the previous one, creating a chain (hence, the name). One key feature of blockchain is immutability; that is, it is almost impossible to modify any information without having network consensus Depending on the consensus protocol, that is, how the blocks are created, blockchain technologies are classified into two groups. In proof-of-work (POW) blockchains such as Bitcoin4 and Ethereum, users called miners participate in a mining process to solve a computationally hard problem to create a new block. The miner who won the right to create a block earns a block reward and collects the transaction fee. POW protocols are, in general, energy-consuming. Also, they are subjected to majority hash rate attacks when the block reward reduces, as seen in recent events with BitcoinGold, Verge, ZenCash, and other POW based cryptocurrencies.5 The new generation of protocols use proof-of-stake (POS) blockchains, in which there is no energy-consuming mining process. Instead, participants' chances of creating a block increase with the amount of coins the stake that they have. The most notable among this group are Nxt, Peercoin, delegated EOS, bitcoin mimic Ouroboros,6 iChing,5 and a recent hybrid POS+BFT Algorand7 from MIT.[15]. Minus the current hype surrounding cryptocurrencies, which distracts from blockchain's true potential, blockchain technologies indeed are powering a new serverless Internet and decentralized web future in which "users are in control of their own data, identity, and destiny." They will also revolutionize the healthcare system such that we will be able to track how our data records are used and have our own data copyrights. With the promising future, we will be given alternative, if not better, choices for every platform we know today, whether it is Facebook, EBay, Uber, Airbnb, or even the energy market. On one hand, blockchain suffers from weaknesses such as security, scalability, and efficiency. On the other, AI has its fair share of issues with trustworthiness, explain ability, and privacy. The marriage of these two technologies seems inevitable; they could complement each other to revolutionize the next digital generation. Blockchain will bring trust lessness, privacy, and explain ability to AI; in turn, AI can help build a machine learning system on blockchain for better security, scalability, and more effective personalization and governance.

II. Literature Work

Fernandez-Carames et al (2018) proposed a system that the IoT paradigm of the Internet of Things (IoT) is paves the way for a world where many of our everyday items are interconnected. A vision requires, in addition to other things, seamless authentication, information protection, security, power against assaults, and self-support.[2] The most relevant BIoT applications are portrayed to accentuate how blockchain can affect conventional cloud-focused IoT applications. This work aimed to evaluate the practical limitations and identify areas—BIoT design, like its architecture, the required cryptographic algorithms, or the consensus mechanisms. The present difficulties and potential advancements are point by point concerning numerous angles that influence the plan, improvement, and arrangement of a BIoT application. The point of directing future BIoT specialists and designers on a portion of the issues that should be handled before sending the up and coming of BIoT applications.

Kshetri et al (2017) proposed a technique blockchain is a data structure that enables a creation of a tamper-proof digital ledger of transactions and share them. This innovation uses public-key cryptography to sign transactions among parties. The ledger consists of cryptographically connected blocks of transactions, which form a blockchain. It is impossible or challenging to change or remove blocks of data— blockchain's role in improving by and extensive security in supply chain networks. With blockchain, it is possible to access changeless records for various transactions involving a product to understand critical vulnerabilities in the upstream production network. This innovation can likewise reinforce downstream production network accomplices' and gadget proprietors' preparatory and guarded cybersecurity measures recorded on the blockchain record. .[3]

III. Block Chain Technology

The three fundamental properties of blockchain technology as a data structure (i.e., distribution, immutability and decentralization, can benefit the Internet of Things (IoT), said Arthur Carvahlo, a blockchain expert and the Dinesh and Ila Paliwal Innovation Chair at the Farmer School of Business at Miami University.Carvahlo illustrated these properties and how they can benefit the Internet of Things (IoT) ecosystem by considering surveillance cameras as IoT devices. Say a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, May 2022
Impact Factor: 6.252

burglar is planning a sophisticated act on a high-profile target. To prevent the act from being recorded, the burglar can first attack the server running the database where the videos are stored, he said. The distributed aspect of blockchain means that data are replicated across several computers. This fact makes the hacking more challenging since there are now several target devices.[1]. The redundancy in storage brought by blockchain technology brings extra security and enhances data access since users in IoT ecosystems can submit to and retrieve their data from different devices, Carvahlo said. Continuing with this example, say the burglar is captured and claims in court that the recorded video is forged evidence. The immutability nature of blockchain technology means that any change to the stored data can be easily detected. Thus, the burglar's claim can be verified by looking at attempts to tamper with the data, he said.However, the decentralization aspect of blockchain technology can be a major issue when storing data from IoT devices, according to Carvahlo."Decentralization means that the computers used to store data [in a distributed fashion] might belong to different entities," he said. "In other words, if not implemented appropriately, there is a risk that users' sensitive data can now be by default stored by and available to third parties." .[16]

3.1 The Benefits of Blckchain and IoT

Enhanced security. Blockchain technology combines secure security with the ability to secure and allow transactions initiated by a trusted group and encryption while data is transferred and stored. Blockchain technology provides transparency about who has access, who does things and a record of all interactions. Also, the blockchain adds a layer of security in terms of encryption, the removal of a single point of failure and the ability to quickly identify a weak link across the network..[5]

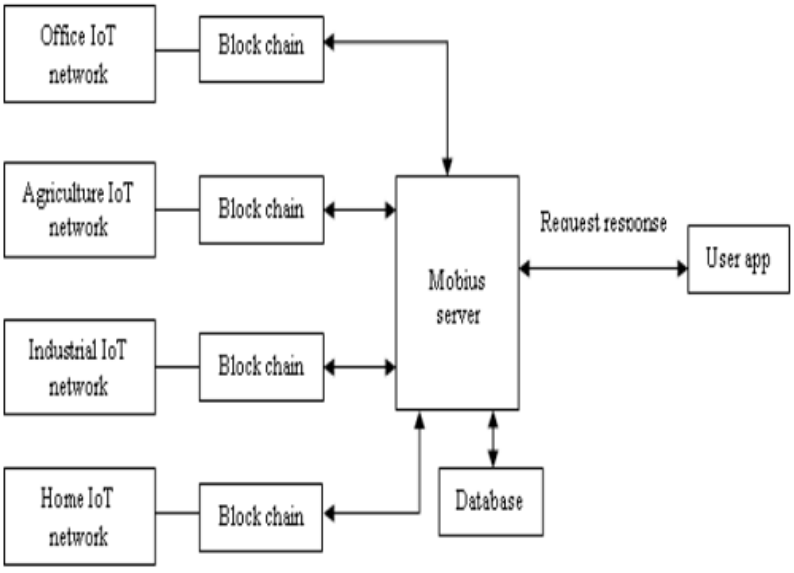
Reduced costs. With automatic transaction verification and blockchain processing steps, the entire ecosystem can be operated at a reduced cost. Transaction speed. This is especially true in the supply chain trade with many suppliers, manufacturers, distributors and consumers. With a blockchain that acts as a standard ledger, unscrupulous teams can exchange data directly with each other, complete manual processes and increase transaction speed.

IV. IoT System Using Block Chain Security Analysis

The frame work of IoT System using Block Chain Security Analysis for Malicious Attack and Intrusion Prevention and its operational analysis is shown in below Fig. 1. In the network, every IoT device is connected to a block which is having timestamp, data and hash value. Basically, hash is a unidirectional function that is fed to device data message #M1 of various length, message contains a definite messages set, M1, It will generate a digest of that message with a fixed and predetermined bit length, n1. Hence the function of hash belongs to device#1, h1 is represented as:

$$h_1 : M_1 \rightarrow \{0,1\}_2^n, with \;\; h_1(m_1) = m_1'$$

Figure 1. Framework Of Iot System Using Blockchain Security Analysis



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, May 2022
Impact Factor: 6.252

In the same manner it is generated for device #2 to N:

$$h_2: M_2 \rightarrow \{0,1\}_2^n, with\ h_2(m_2) = m_2'$$

$$h_N: M_N \rightarrow \{0,1\}_2^n, with\ h_N(m_N) = m_N'$$

In the environment of presented system, open server platform of Mobius IoT is utilized for implementing a system which will share the sensor information from device to application and applied it to the server of block chain. Etherium's smart contract is utilized in block chain environment for putting the power data over the network of block chain thus all users will prove it and reliability is increased. Utilizing the created smart card with the proof function of Zero Knowledge, utilized the anonymity-enhanced block chains for preventing data or account information from being disclosed. The configuration of system including Office IoT network.[6]

Agriculture IoT network, Office IoT network and Office IoT network. There are 4 kinds of devices which can produce transactions by placing the data in a smart contract of block chain. Provided a decentralized security system utilizing block chain for IoT based network since there are several drawbacks in centralized security techniques.[9]. This block chain technique has several security benefits compared to traditional defense system like high integrity, third party security is not involved, secured communications and peer-to-peer authentication and many more. The user sends 'device ID', 'password' and 'user ID' are utilized as the password of block chain smart meter via Mobius server for registering member. In the block chain the Mobius server asks a new account with the password from transmitted information of a member and account address response is received. Device ID, user ID is stored by Mobius server and account address is transmitted to member application in the database.[10]. In block chain smart contract is selecting the addresses of account which are in the server's database. After creating the block, the user transmits the member ID to Mobius software for retrieving the process and server retrieves uploaded data to the block by matched block chain address in the database, displays the data in the user application.[11]. The Zero knowledge proof is a proof technique where information is known without exposing any information. Zero knowledge proof concept is introduced in block chain, which can prove a work or transaction without disclosing the transaction information or virtual money information to outside world. It is a proof technique that satisfies the properties like Zero knowledge, impracticality and completeness. .[8]

V. THE PRAPOSED NOVEL CONSENSUS ALGORITHM-PROOF OF AUTHENTICATION

The proposed Proof-of-Authentication is a new consensus algorithm proposed in this paper to build a lightweight and sustainable blockchain for resource-constrained devices. This consensus algorithm introduces an authentication mechanism during block validation. In other respects, it follows traditional communications. Fig. 2 provides a comparative overview of the proposed PoAh with the more common Proof-of-Work and Proof-of-Stake consensus algorithms. At the very beginning of the process, network precipitants generate transactions (Trx) with the sensed or collected data assembled to form a block. In the figure blocks are represented as B = {T rx1, T rx2, , T rxn}.

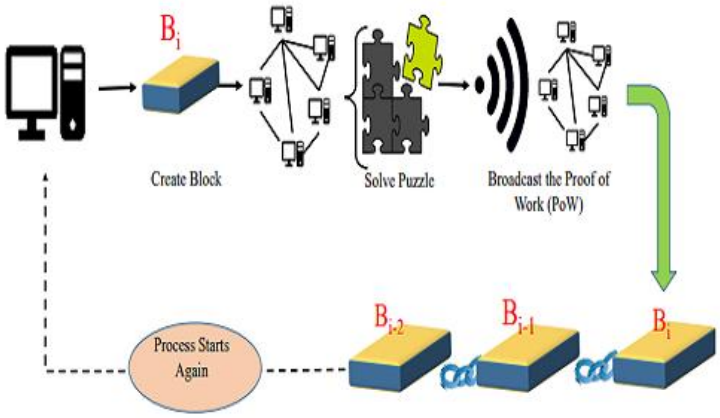


Figure 2: Proof-of-Work (PoW) consensus algorithm

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, May 2022
Impact Factor: 6.252

The nodes broadcast the blocks for further evaluation and/or validation by trusted nodes in the network. We follow the standard IoT deployment steps to create the initial trusted node set based on geographical location. Trusted nodes are reachable from any part of the network. The proposed model adopts the ElGamal crypto-system for encryption and decryption, i.e. y = g x (mod p) where x is the private key PrK and y is the public key PuK.[13]. The large prime numbers for modulus operation p and generator function g are publicly known to all the network devices. Prior to block broadcast, the network user makes the public key PuK, i.e. y, available to the network and signs the block using its own private key PrK, .[14]

VI. CONCLUSION

In this paper, Implementation of IoT System using Block Chain Security Analysis for Malicious Attack and Intrusion Prevention frame work is described. The block chain provides outstanding decentralized security system which is integrated and implemented into IoT based networks for defending from various threats, intrusions and attacks. A Zero-Knowledge proof technique is applied for preventing the third party from checking user's original information via block retrieval. Various tests have been performed and it is proved that IoT system utilizing block chain technique is solving the security issues which are arise in communication among IoT devices.

REFERENCES

[1]. Ouaddah, A.; Mousannif, H.; Elkalam, A.A.; Ouahman, A.A. Access control in the Internet of Things: Big challenges and new opportunities. Comput. Netw. 2017, 112, 237–262

[2]. Rajneesh Kumar, Shekhar Verma, G S Tomar, "Thwarting Address Resolution Protocol Poisoning using Man In The Middle Attack in WLAN", International Journal of Reliable Information and Assurance Vol.1, No.1, pp.8-19, 2013

[3]. Diana Yacchirema, Carlos Palau, "Interworking of Onem2M-Based IoT Systems and Heterogeneous IoT Devices", 2020 XLVI Latin American Computing Conference (CLEI), Year: 2020

[4]. S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities," IEEE Consum. Electron. Mag., vol. 5, no. 3, pp. 60–70, July 2016.

[5]. Jianming Liu, Ziyan Zhao, Jerry Ji, Miaolong Hu, "Research and application of wireless sensor network technology in power transmission and distribution system", Intelligent and Converged Networks, Volume: 1, Issue: 2 , Year: 2020

[6]. Yang, H.K., Cha, H.J. and Song, YJ, 2019. Secure identifier management based on blockchain technology in NDN environment. IEEE Access, 7, pp.6262-6268.

[7]. A. Pentland and E. Castello Ferrer, "Blockchain: A New Framework for Robotic Swarm Systems," Media Lab Research MIT; www.media.mit.edu/projects/blockchain-a-new-framework-for-swarm-robotic -systems/overview.

[8]. N. De, "Hacks, Scams, and Attacks: Blockchain's 2017 Disasters," 29 Dec. 2017, coindesk; www.coindesk .com/hacks-scams-attacks -blockchains-biggest-2017-disasters.

[9]. Basic Attention Token (BAT): Blockchain Based Digital Advertising, white paper, Brave Software, 13 Mar. 2018; www.basicattentiontoken.org /BasicAttentionTokenWhitePaper - 4.pdf.

[10]. N. Lomas, "What Do AI and Blockchain Mean for the Rule of Law?," 12 May 2018, Techcrunch, https:// techcrunch.com/2018/05/12/what -do-ai-and-blockchain-mean-for -the- rule-of-law.

[11]. L. Fan and H.-S. Zhou, "A Scalable Proof-of-Stake Blockchain in the Open Setting (or, How to Mimic Nakamoto's Design via Proof-of-Stake," 2018; https:// eprint.iacr.org/2017/656.pdf.

[12]. J.I. Wong, "Every Cryptocurrency's Nightmare Scenario is Happening to Bitcoin Gold," 24 May 2018, Quartz; https://qz.com/1287701/bitcoin -golds-51-attack-is-every -cryptocurrecnys- nightmare -scenario.

[13]. A. Hern, "AI Used to Face-swap Hollywood Starts into Pornography Films," 25. Jan 2018, The Guardian; www.theguardian.com/technology /2018/jan/25/ai-face-swap -pornography-emma- watson-scarlett -johansson-taylor-swift-daisy-ridley -sophie-turner-maisie-williams.

[14]. G. Wood, "Web3 Foundation," 2017; https://web3.foundation.

[15]. B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based architecture for collaborative ddos mitigation with smart contracts," in IFIP International Conference on Autonomous

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, May 2022
Impact Factor: 6.252

Infrastructure, Management and Security. Springer, Cham, 2017, pp. 16–29.

[16]. A. Kousaridas, S. Falangitis, P. Magdalinos, N. Alonistioti, and M. Dillinger, "Systas: Density- based algorithm for clusters discovery in wireless networks," in 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2015, pp. 2126–2131