Blockchain Enabled Cyber Security: A Comprehensive Survey

Atharva Deshmukh
Department of Computer Engineering
Terna Engineering College
Navi Mumbai, India
atharva1525@gmail.com

Amit Kumar Tyagi[0000-0003-2657-8700]
School of Computer Science and Engineering, Vellore Institute of Technology
Chennai, 600127, Tamilnadu, India.
amitkrtyagi025@gmail.com

Uppalaguptapu Venkata Eswara Abhichandan
Department of Computer Engineering
Terna Engineering College
Navi Mumbai, India
abhichandanuve @gmail.com

N Sreenath
Department of Computer Science and Engineering, Puducherry Technological University,
Puducherry, India
nsreenath@pec.edu

***Abstract*— This paper identifies research paths for blockchain in cyber security that need further research: Internet of Things (IoT) security has indeed been promoted as a critical industrial necessity, even though almost all publications on blockchain cyber security in literature pointed out that the security of IoT systems can be revived if it is backed by blockchain. Yet, few things are now known and talked about the decision-making and practicality of adopting the technology, or how it may be used realistically to correct existing IoT security risks and threats, providing scope for imagination and the construction of future vectors in this particular area. As a result, future research must establish measurable recommendations and methods that can assist in filling the gaps in the existing literature. There is also the potential to develop solutions for IoT devices with limited resources (operating on the periphery of the network) that are based on blockchain technology.**

Keywords—Blockchain, Smart Contract, Cryptocurrencies, Decentralized Applications, Cyber Security, Cyber-Physical Systems (CPS)

I. Introduction

Blockchain has become one of the most widely utilized concepts in recent years. Blockchain has shown its value in a wide range of industries, including healthcare, energy, transportation, logistics, agriculture, retail, and financial institutions. Decentralized, authenticated, and unchangeable information at cheaper prices is what makes blockchain special. Due to the following features, Blockchain is unique:

Trust: New information may only be added if a majority of computers in the network approve it after acceptable evidence is supplied that the information, which is sent cryptographically, is accurate. All network computers are updated with the new information over regular intervals after authenticating the information.

- Immutability and transparency: Once recorded, information cannot be edited, updated, or lost, resulting in an incorruptible historical record that remains in the system for the rest of time. Importantly, all individuals in the network may observe the modifications made to public blockchains, assuring openness.
- Disintermediation: All cooperating computers across the world maintain the ledger (database). Meaning two parties may make a transaction without the requirement for a trusted central authority to verify or validate the records of their exchanges.
- Lower costs and greater speeds: As a result of removing the monopolistic influence of big middlemen like banks or huge, centralized industry leaders, blockchain offers reduced transaction costs and higher speed in many applications (e.g., Airbnb).

978-1-6654-8035-2/22/$31.00 ©2022 IEEE

II. Literature Survey of Blockchain

Blockchain is a decentralized open ledger that records transactions across several computers. Cryptocurrencies such as Bitcoin and Ethereum may be used in virtually any industry including banking and healthcare as well as real estate, tourism, and supply chain. For the new concept, reinforcement learning integrating self-driving supply chain in the best method, we conduct a literature review as follows: As an example, consider the following: How blockchain may be used in AI [1] to increase reliability, security, transparency, and confidence of data. AI computations may use the database with diagrams to extract, organize designs, information, and anticipate solutions for future. The profound support learning approach proposed in [1] is similar to the benefit from our previous interactions. Similar to valid reasoning is the security-based control, that incorporates false prospective methods, and route. A deep defensing knowledge include fake prospective fields and methods for self-sufficient driving. Authors [1,2] highlighted that the Store network is a issue of the board referring to the problems such that the goods development, and raw materials must work in such a way that avoids wasting and unnecessary costs.

SCM-related issues such as client requests, the availability of raw materials, the delivery dates, and the costs of raw materials are generally unpredictable. Fortification learning writing approach for describing a supply chain and executive's problem into a parametrized unending arm crook problem. A single car may be used to prepare a large number of vehicles by sharing its knowledge with all the other vehicles in the company utilizing blockchain technology, according to the authors [2]. Use of Reinforcement learning in the preparation of a single automobile Self-driving technology that incorporates ai-based blockchain innovation. Some inconsistent data led to Tracking and Trailing

of Goods: The authors in [3], define Trailing of food is required to observe by every stages in the network of food production that assure keep food can hand over animal of standard quality, Hence, such scrutiny tells us such animal of halal cater for healthy nourishment be noteworthy in the food of halal manufacturing matrix. In [3,4], the authors show the many applications of blockchain in detail.

Because of the Pecking order of food, the dispensation, planning phase and few contagions too occurred without the understanding of both manufacturer and purchaser. The authors in [5] put forward the network of Halal inventory is a plan of action such that the essentiality of beginning halal out of reason of grant till it appears in front of the receiver. Currently, the network of halal inventory shall start at the farmland, additionally, the butcher house, in motion along with setting down aside the poultry things prior to the arrival on the receiver's side. Already stated is to make sure a certain halal is not applicable for objects or nourishment anyhow besides every pursuit inside goods structure that combine the control with balancing of the items(all the executives and material taking care of. The authors in [5] talked through the way Chain of Halal Food Supply may toil over a association blockchain as for the present mechanical, engineering and more, and application components. Including that out of which a type feature of a Peer-to-Peer system, grant & particulars segment appliance, and details safety empowerment, here Shared Registry Mechanism do increase confidence between all distinct players around the chain of stock , eventually allowing consumers to gain increasing amount of knowledge, moreover, defined conclusions.

Dolgui et al. talked over the Blockchain-oriented active creation of clever agreement plan & implementation in the chain of supply. The suggested idea sets up an instance that operates a potent method to work along with the operation, and management corporation when organizing the canny concurrence. The procedure is more valuable in view of the concurrence accomplishment phase. The usage of state-controlled elements in the representation parts in deliberation pursuits in the Blockchain which hence, gets hold of supervision inputs of computerized data, and control of contract execution, disturbance recognition[6,7]. The authors in [7] described the traceability of blockchain-enabled in the agribusiness chain of supply . The findings of the inquiry do help the professionals along with calculating the methods for Blockchain technology use in agriculture, creating a continual knowledge-driven farming chain of supply. The end results would likely contribute to the commanding in generating plans for faster use of Blockchain technology promising cleanliness and a sensible farming chain of supply[8]. Lately, the authors [8,9] created the framework on blockchain-based of the cross-border e-commerce chain of supply that ensures the chain of supply administration in case of the copy strike, forgery label strike, and forgery result strike. In Chain of Supply Management vital cover is Planning, from creator to customer in order to outstretch the result carefully and without that some corruption into the result [10]. Finally comforting the consumer is a greater sight in this chain of supply. However, in the surviving plan, it indicates that a few straggling occurs(Example: Harming Products because of misfortune, Cross-Infection into the Product) because of such incidents consumers become regretful. About this reference, the apt creator or manufacturer visions the loss of company.

III. Blockchain and its Evolution

Blockchain is a game-changing technology that spans the Internet of Information/Communications to the Internet of Value. They are opposed to one another. Uber and Airbnb are two examples of firms that were affected in the early 2000s because the information supplied may be copied and transmission was cumbersome. As a result, without the consent of an intermediary, such as a bank validating the availability of the money being delivered, it is difficult to ensure the trustworthiness of the information. The creation of trust between strangers is the main benefit of the Internet of Value, thanks to the usage of blockchain technology. Because confidence is built into the system, assets can be traded instantly and efficiently, eliminating the need for middlemen (third parties). Even more significant changes are likely as a result of the benefits of the Internet of Value.

Trusted peer-to-peer transactions would enable decentralized structures, decreasing the power of middlemen such as banks or corporations like Uber and Airbnb. The monopolistic influence of today's major actors might be significantly curbed by developing new participants that would use blockchain-based platforms of decentralized networks, democratizing the global economy and resulting in a more sustainable economic structure. Following Nakamoto's 2008 paper, blockchain applications gradually began to incorporate bitcoins, but they remained limited to cryptocurrencies until July 2015, when the Ethereum platform [was created, allowing the construction of smart contracts]. Almost simultaneously, Estonia began using blockchain technology in its governance procedures, including an e-health record system that included all of the country's people who had ever seen a doctor. Smart contracts and Decentralized Autonomous Companies (DAOs) were introduced in 2016, and they have the potential to radically revolutionize the legal profession and corporate management. Since 2016, a large number of companies have been developing new solutions that will revolutionize the economic environment and turn blockchain into a major technological force.

A. Improvement of Bloackchain Performance

Due to high processing costs, huge bandwidth overhead, and massive storage requirements, blockchain may be inappropriate for real-world application development. When a big number of organizations join the network, significant data volumes, frequent requests, and blockchain stability must all be considered. Only a few studies are currently being conducted to address the aforementioned problems. Researchers are focusing on improving cryptography's consensus algorithms, block size, and other elements. As a result, the writers concentrated on lowering latency, increasing throughput, and addressing other issues of blockchain scalability. Because the block size and generation interval in Bitcoin is the first step toward throughput increases and latency reduction, there is no threat to system decentralization.

To verify transactions and reach a consensus, cryptocurrency blockchain networks require consensus mechanisms. Writers adjusted the DPoS election method based on medical institutions' credit scores, which increased trust amongst a small number of medical organizations and secured the consortium blockchain's dependability. They devised a novel mining method known as Lightweight Mining (LWM), which necessitates less storage and processing. 'Sharing-hash-first' is a basic idea that ensures that all miners in the network are treated equally. To show that it can withstand rogue miners and Distributed Denial of Service (DDoS) attacks, the company released a video.

In addition, the authors proposed two loosely coupled blockchains based on two types of healthcare data, Electronic Medical Records (EMRs)/ Electronic Healthcare Records (EHRs) and Personal Healthcare Data (PH.D.). In the blockchain-based system, throughput and fairness are new problems for two types of data. As a result, two fairness-based packing algorithms

have been developed to improve the system's throughput and user fairness. Motivating miners to join the network is critical for maintaining a trustworthy and reliable blockchain in the actual application scenario. Researchers have proposed an incentive system to encourage medical researchers and healthcare officials to become data miners and help build the data economy by rewarding them for large amounts of data from hospital records. The authors proposed a selection technique within the incentive system. Providers with a higher chance of being chosen to perform the duty of new block creation have less significance and will receive significance as a bonus to reduce the selected likelihood in the future.

All transactions can be "seen" by any node in the blockchain network, which is an important point to remember. They could be used to avoid data forensic analysis by inference, protect individual information privacy, and enable computing without leaking input or output. In addition to the restrictions mentioned above, further aggressive blockchain protocol expansions will necessitate a fundamental protocol redesign. It is critical to improving the blockchain's underlying architecture to provide better service. Within the context of IoT, there is a massive volume and rapid rate of personal healthcare data streams generated by wearable devices. A large amount of data may be used in conjunction with big data and machine learning techniques to improve data quality and deliver a more intelligent health care service. However, a significant network delay may occur due to the physical distance between mobile devices and cloud servers, as well as traffic congestion on the cloud servers' cloud servers' servers.

IV. BLOCKCHAIN TECHNOLOGY AND ITS CONNECTION WITH SECURITY

A. The latest blockchain applications focused on security

It's worth noting that the scope of this literature evaluation is limited to blockchain applications for cyber security. During primary studies, the researchers found there were a whole lot of studies on finance and healthcare. However, the selection procedure focused on research that had a security focus at their heart. More than half of the papers published about cyber security blockchain practical applications address IoT, the potential to improve IoT security is enormous. Possibly due to the increasing use of IoT devices in our healthcare, vehicles, homes and more to the a growing need for IoT solutions. As with IoT security risks, the need for solutions may be sparked by media reports of assaults planned by exploiting such devices.

Following are some of the most security-conscious blockchain applications, according to recent research:

1. There are two types of authentication in the Internet of Things: First is authenticating the users to the devices and then authenticating their devices to the network. Firmware upgrades can be distributed securely using peer-to-peer networks. Threat detection and malware protection are two important aspects of cybersecurity.
2. Storage and sharing of data must be protected against unauthorized changes, hash lists must be used to search for data that should be preserved and kept securely, as well as data transferred must be validated and identical.
3. As containers, software-defined networks and virtual machines used for deployment of the application are becoming more prevalent, the use of blockchain enables the decentralized and resilient storage of essential authentication data.
4. User settings for Iot enabled devices like smart wearable, as well as the security of personal details transmitted securely to the third parties, are examples of private user data.
5. Navigating the World Wide Web and using web apps safely, as well as interacting with people via secure, encrypted ways through accurate DNS records.

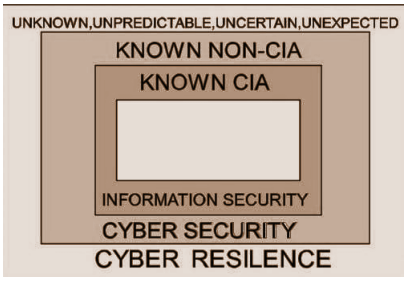

Figure 1: Security Requirements in Cyberspace

B. Use of Blockchain to improve Cyber Security

There is no silver bullet when it comes to cyber security, and blockchain and associated technologies are no exception. Rather than replacing current efforts, they just reinforce them. Immutable records are stored in blockchains via encryption and hashing. The majority of current security techniques rely on a single trusted authority to store encrypted data or validate information. Many bad actors may then concentrate their operations on a particular target to conduct Dos attacks, implant harmful material, and then steal or extort data. Because blockchains are decentralized and also don't require authorization from an individual in a group or network, they outperform current security techniques. Every member, or node, has a full copy of the historical information available, and extra data can be added to the chain of prior information by reaching agreement among the majority. There are several techniques for accomplishing this, but the basic reality is that a group with many members who have access to the same information will be able to safeguard itself more efficiently than a group which has a leader and many individuals who depend on their leader for their data, particularly when bad actors may be a group of individuals.

Based on the most security-focused blockchain applications described in section 4.1, we explore how blockchain was used to increase cyber security in Internet of things devices, network security, data storage and sharing of private end-user data, network security, navigation through World Wide Web.:

1. Internet of Things: Main private blockchains (like Hyperledger Fabric) are used to create permitted access control for nodes (devices) in the network, in order to prevent fraudulent access and securely monitor data management. Blockchain is also being used to enhance the security of software installation by enabling updates to be distributed peer-to-peer, allowing IoT devices to be recognised, verified, and transmit the data securely. In the past, blockchain was used to protect IoT connections and sessions while also detecting malicious activities. The proposed architecture in these works is as follows: The blockchain protocol, which lies in between the network's application and transport layers, employs token rewards in the same way as bitcoin does, but treats them as voting power units.

2. Data sharing and storage: Use of both public and private distributed ledgers is encouraged to remove a single point of failure in a storage ecosystem. Blockchain ensures that cloud data is protected from unwanted modifications, hash lists make it possible to search for data that can be preserved and securely store the data, and while maintaining the integrity of data transmitted could be confirmed between sender and receiver. So in a nutshell: Blockchain enhances sharing security and data storage through the use of encryption on client side, where the actual data owners have full and verifiable control over their data.

3. Network security: This category is dominated by works that make use of blockchains to enhance Software Defined Networks (SDN) and containers for authentication essential data storage. A clustered structure of SDN controllers with blockchain architecture is employed in such activities. For network security, the architecture uses private as well as public blockchains to provide peer-to-peer (P2P) communication between nodes in the network and SDN controllers.

4. Private user data: While other categories have received more attention, Less emphasis has been paid to the application of blockchain to increase data privacy. Because blockchain is irreversible where everybody has a copy of the ledger, it is challenging to employ this for privacy purposes, particularly for data protection. Users' device preferences are stored in an encrypted way on the blockchain just so that the data can only be viewed and updated by the end-user.

5. Utility of the World Wide Web and navigation: Blockchain technology is used to improve the validity of wireless Internet access points by storing and monitoring access control data on a local ledger. In addition, the blockchain can also be utilized for navigating to the correct web page by using accurate Domain Name System (DNS) records, securely using online applications, and interacting with them through highly secured methods. To accomplish these solutions, a consortium blockchain was utilised, in which the consensus process is controlled by a pre-selected group of nodes within the network.

C. Blockchain methods to manage security without cryptocurrency token

A large number of main research groups agree that incentivizing miners with tokens, such as bitcoin's reward, is a well-established and reliable approach for reaching the longest chain consensus. To put it another way, innovative ways to token distribution demonstrate that there have been alternatives to paying the miners in the form of cryptocurrency token. This cryptocurrency token has value such that they allow recipient nodes to have more voting power. Votes are secure and anonymous, which can be verified at any moment and the more a node contributes to mining, the more voting power it will have over the chain's process in the future. According to this idea, each IoT device may charge other devices a token amount for delivering firmware updates. To ensure that transactions on the blockchain are secure and that consensus is reached, IBM's Hyperledger Fabric, for example, uses its chain code. In the application, monetary tokens are optional. One research looks into the idea of depending on several blockchain levels for transaction trust and authentication among hierarchical tiers. No system other than a PoW consensus mechanism that pays miners with a cryptocurrency token of value has been able to grow securely with the amounts of network activity witnessed on the Ethereum and Bitcoin networks, according to primary research.

V. PROPOSED SYSTEM

The world has made a transition to the digital era where everything is digitized or connected to the internet which has its improving share of advantages and disadvantages. Blockchain has its own set of working mechanisms connected to the internet, so it should not compromise the integrity, confidentiality, and also reach or availability of this service. Integrity is maintained when unnecessary modifications are exempted. confidentiality stands when unauthorized users don't have access to it. Availability is ensured when it is available and free from Dos or DDoS.

The data or records which are stored in the system use public-key cryptography which saves it from any cyber-attacks from adversaries attempting to do any unauthorized work on the stored data or record. Another way of providing some security is by assigning users with private keys which ensures the authenticity of the user while signing and transactions. Digital methods like encryption can be used to ensure security, privacy, and control access. Blockchain itself is created in a way where if some block is to be overridden or tampered with then every other block needs to be modified to make it look valid to other blocks and the whole chain. The system has a system of providing hash values to other blocks to keep them connected in a parent-child manner which creates incomprehensible hashes stored in the blockchain.

The system of blockchain itself has a structure that is not a decentralized one which helps to increase security and enables proper structure. The blocks which can also be referred to as nodes ensure no single point failure and makes it available. The concept of DPoS is used in which users will vote and elect delegates to validate the next block. This DPoS ensures no Dos or DDoS takes place as registration is required for any node to start sharing any information with other network users. The transactions which occur are validated by the witness so that no wrong practices can be caused making it difficult to perform malicious activities.

These characteristics position blockchain technology as a promising trend in the development of a typical example capable of providing a reliable, secure, and fault-tolerant communication route between authorities and society. The indirect benefits of blockchain technology, such as the reduction of bureaucracy, the elimination of paper usage, the reduction of transaction costs, and the control of corruption, have the potential to revolutionize the entire ecosystem and increase public trust. By making the hash system in blockchain a more accurate and hash-focused structure, the suggested method would provide enough security and boost efficiency.

VI. COMPARISON OF DEFENSIVE MECHANISMS

In this section, we will discuss several defense mechanisms and their comparisons in detail (refer table 1).

1. Proactive Defense: This focuses on an independent assessment and judgment of procedural behaviour, which can be more proactive in identifying and addressing risks. It can protect the information system's security by fending off intruders. The most popular active defensive technique is honeypot technology, which creates purposeful system weaknesses to lead hackers to attack. This detects eavesdropping hackers and gathers various hacker attack weapons for subsequent protection. The absence of passive defence is compensated for by proactive defence, taking into account subjective variables and taking active defensive measures in the event of an assault. trusted Computing technology, Vulnerability scanning, Trap technology, and few more different technologies are included in proactive defensive technology.

2. Blockchain: Although a blockchain is not an information defense system, its unique features can enable greater anti-interference and data confidentiality. At the end of the resultant packet, each perceptual device assigns a fixed private key and adds a digital signature encrypted with multiple private keys. The whole system's information node chain creates a mesh structure, giving the data channel a high level of redundancy. The digital signature makes it very hard for hackers to fake sensor data, moreover decrypting the data content is impossible. Even if an attacker disables a portion of the network's data

channel, the highly redundant mesh topology permits data to be carried across alternative data paths.

Table 1. Proactive defense, passive defense, and the blockchain: Advantages and Disadvantages

Categories	Advantages	Disadvantages
Firewall Technology	1. Monitoring the network access to strengthen the security. 2. Checking of the information to reject suspicious attacks	1. The original defense system is no longer defensive after the attack is successful. 2. Legitimate users' illicit activities cannot give a superior defense.
Intrusion monitoring	1. Keep an eye on the attacker's tracking line. 2. The hacker's flood attacks are detected as legitimate users.	1. Without user input, it is impossible to compensate for system flaws. 2. It is impossible to prevent a cyberattack without the engagement of the user.
Honeypot Technology	1. Evaluation of the captured behaviour to learn more about the hacker. 2. Regulate the Intruder's behaviour to lessen the damage.	1. Only track and capture activities that have direct interaction with it. 2. Allow the attacker to see the real operating system.
Trusted computing	1. Build absolute trust roots stored outside the trusted platform. 2. Build the trust chain among the connected devices.	1. The trusted root is stored outside the trusted platform module. 2. Once the component is changed the value of PCR needs to be recalculated.
Blockchain	1. Establishes a trust mechanism. 2. Removes the harmful parts. 3. Ensures Data integrity. 4. Controls the access Right Of Information Network.	1. It is difficult to balance between the degree of decentralization and the effect of the consensus. 2. Difficult to balance between storage capacity and processing performance.

VII. Popular Challenges with Blockchain

Blockchain itself has some challenges some of which are related to the technological part of it and others which are related to virtual currencies.

In General: When we try to adapt the blockchain technology to the current IT systems their integration will bring some changes, these changes may not lead to complete replacement of current systems but some investment is required and there will be some difficulties which will be faced while trying to get people who are fit to handle and work with the technology. These issues are actually serious, already available solutions and systems which are open may alleviate those, which also occurred when internet was a new technology. The other problem associated with it is the requirement of electricity which is in a large amount to power all the computers which are connected to the respective networks. There are technologies which are developed to be used as alternatives to avoid this problem. DeepMind, for example, tracks data changes using Merkle trees rather than requiring verification from all the machines that are networked. The most important goal is the immutability and safety of the data involved rather than to maintain the trust between the users or parties who are involved, such trees enable for secure and efficient verification of the contents of data structures which are massive.

A. Blockchain and Artificial Intelligence

Blockchain is a game-changing technology that, among other things, allows for the secure and trustworthy storing and transmission of data. Artificial intelligence is the new tech that changed the world of tech having the capability to detect different patterns and analyze data of vast or big amounts. This naturally results in a complementary relation between both the blockchain and artificial intelligence which properly and securely stores data and detect patterns from it to learn from it respectively. We can see some examples on how combining these two technologies result in a massive breakthrough like Decentralized Autonomous Organizations, Smart Contracts, the Internet of Things , Medicine, Autonomous Vehicles and many other areas of application are likely to gain. In many circumstances, AI could not be employed without assurances about the security and trustworthiness of the data supplied by blockchain, and the opposite is also true, the usefulness of many applications related to blockchain would be less or limited if AI were not available or integrated with them.

B. Government Operations

Generally leaving some of the governments who try new tech, some of the governments are still hesitant to adopt new technologies, AI and blockchain are not an exception, especially when AI is still in its early stages, except for some applications. We can never imagine what all developments will be occurring in it; in fact the development in artificial intelligence boosted up abruptly in the last few years. The artificial intelligence these days have set focus on assistants managed digitally who answer questions proposed to them in language naturally with images and facial recognition related technologies. The future potential, on the other hand, is enormous, with anticipated benefits in the billions of dollars. From combating evasion of tax to formulating or developing fiscal policies and monetary policies , AI might be used in a variety of ways. If the buzzword "cognitive AI" becomes a reality, it will have far-reaching ramifications in terms of not just saving billions of dollars, but also offering better services to the general users or public and also increasing democratization. Governments in a fewer number only like Dubai's have the intention to make good use of blockchain by having it integrated in several of their operations. This will in turn improve efficiency, decrease the bureaucracy and also save huge amounts of money .

C. gital Currency

Although it is not very much clear on how AI may be integrated with the blockchain technology which is used in bitcoins and other available cryptocurrencies, there is a possibility in the future when robots and DAOs, which own property and hold assets, are implemented. They will have to either deploy artificial intelligence(AI) to perform transactions like M2M or make payments using bitcoins..

D. Supply chain Operations

Blockchain technology is employed by many organizations for its logistics aspects like scheduling, planning chores etc. Apart from this logistics employment of AI it is already being used in supply chains but the integration of blockchain and AI is still in its early stages. One of the major challenges faced would be to successfully apply the AI part to all the remaining elements of the supply chain in the future in an efficient and viable way. One of the examples that can be taken to consideration is Amazon which is a pioneer in artificial intelligence(AI) responding to clients by giving them a comprehensive experience achieved by incorporating the AI with information producing efficient results.

E. Autonomous Vehicles and Internet of Things

Continuous monitoring of information traffic from several linked AVs and the method to calculate the routes based on several factors like weather conditions, day, time and several other factors helped the AVs to evolve to a new level. AI integration with the autonomous vehicles started to understand different patterns which are changing continuously and help choose a route which eases the travel or journey if at all necessary. By continuously monitoring traffic information from linked AVs and learning to calculate the route based on the time, day, weather conditions, and a variety of other aspects, AI can help AVs go beyond simply following a fixed course for transporting people from point A to point B. When the AI

determines that traffic patterns are changing, it can even change the course of a journey if necessary.

F. Standards and Regulations

New technologies should be taken with caution if they reach the market without some type of vetting, such as a cost-benefit analysis. As a result, we must adopt common standards, norms, and regulations to increase compliance, security, interoperability, and other considerations. One of the examples would be that multiple independent and trusted processes will likely be required to assess ,evaluate various blockchain solutions for different settings or applications in terms of capacity, throughput, security, latency, privacy and many more. This will also allow us to regulate any misconduct or any infractions noticed and implement respective sanctions.

Further, researchers can refer several mechanisms on blockchain and uses of blockchain in different sectors (with analysis of threat in detail) in [11-20].

VIII. Conclusion and Future Work

This paper provides a theoretical and qualitative examination of privacy and security in blockchain-enabled cyber security. It demonstrates that immutability, encryption, and the decentralized administration and control provided by blockchain technology would provide the necessary privacy and security in many systems. Additionally, decentralized, distributed, and investable cryptocurrency tokens are moreover vigorous & safe blockchains that hold up the researcher's proposed applications, and because of the same cause, cryptocurrencies shall enlarge along with the acquisition of blockchain security technologies. Although Bitcoin is the most famous decentralized cryptocurrency along with the extended and most dependable blockchain, there has been spreading interest into creating a scientifically user friendly architecture of cryptocurrency which shall permit for the legitimate(forensic) inquiry of the doubtful transactions of cryptocurrency, like the above mentioned is used in cybercrime like terrorism financing and ransomware.

The above research examines self-archived announcements trying to make use of blockchain for cyber security along with a detailed survey of the extensively used applications of blockchain security. Our discoveries show us how the IOT, and the machine visualization and networks, online applications, public-key cryptography, safe storage, and the certification schemes of Personally Identifiable Information, lend themselves well to innovative blockchain applications. This research is confined to a framework and theoretical debate, the active future effort will be to apply the framework and then further investigate its full potential in a real-world setting. As the world is still growing in terms of technology and its scale it would require an understanding of contemporary changes needed to keep data in a more secure and private way. Understanding the changing technology and the level of access to be provided to users have to be paired and then that potential needs to be understood.

References

[1] Emanuel Ferreira Jesus, Vanessa R. L. Chicarino, Célio V. N. de Albuquerque, Antônio A. de A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack", Security and Communication Networks, vol. 2018, Article ID 9675050, 27 pages, 2018. https://doi.org/10.1155/2018/9675050

[2] M. Pilkington, Blockchain technology: principles and applications. research handbook on digital transformations, F. X. Olleros and M. Zhegu, Eds., 2016.

[3] C. Natoli and V. Gramoli, "The Blockchain Anomaly," in Proceedings of the 15th IEEE International Symposium on Network Computing and Applications, NCA 2016, pp. 310–317, IEEE, November 2016.

[4] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in Proceedings of the 13th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA 2016, IEEE, Agadir, Morocco, December 2016.

[5] Surjandari, I., Yusuf, H., Laoh, E. et al. Designing a Permissioned Blockchain Network for the Halal Industry using Hyperledger Fabric with multiple channels and the raft consensus mechanism. J Big Data 8, 10 (2021). https://doi.org/10.1186/s40537-020-00405-7

[6] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in the internet of things: Challenges and Solutions, 2016,"

[7] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation, vol. 2, pp. 6–10, 2016.

[8] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623, Kona, Big Island, HI, USA, March 2017.

[9] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2017.

[10] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?" IT Professional, vol. 19, no. 4, Article ID 8012302, pp. 68–72, 2017.

[11] Amit Kumar Tyagi, "Analysis of Security and Privacy Aspects of Blockchain Technologies from Smart Era' Perspective: The Challenges and a Way Forward", in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.

[12] Amit Kumar Tyagi, G Rekha, Shabnam Kumari "Applications of Blockchain Technologies in Digital Forensic and Threat Hunting", in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.

[13] Shabnam Kumari, Amit Kumar Tyagi, Aswathy S U, "The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities and Challenges", in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.

[14] Tibrewal I., Srivastava M., Tyagi A.K. (2022) Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_1

[15] Amit Kumar Tyagi, Aswathy S U, G Aghila, N Sreenath "AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology" IJIN, Volume 2, Pages 175-183, October 2021.

[16] Meghna Manoj Nair, Amit Kumar Tyagi, Richa Goyal, Medical Cyber Physical Systems and Its Issues, Procedia Computer Science, Volume 165, 2019, Pages 647-655, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.01.059.

[17] Amit Kumar Tyagi, G. Aghila, "A Wide Scale Survey on Botnet", International Journal of Computer Applications (ISSN: 0975-8887), Volume 34, No.9, pp. 9-22, November 2011.

[18] Amit Kumar Tyagi. Article: Cyber Physical Systems (CPSs) – Opportunities and Challenges for Improving Cyber Security. International Journal of Computer Applications 137(14):19-27, March 2016. Published by Foundation of Computer Science (FCS), NY, USA.

[19] G. Rekha, S. Malik, A.K. Tyagi, M.M. Nair "Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security", Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 72-81 (2020).

[20] S. Mishra and A. K. Tyagi, "Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technolgy," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 123-128, doi: 10.1109/I-SMAC47947.2019.9032557.