Exploring the Joint Potential of Blockchain and AI for Securing Internet of Things

Md. Tauseef, Manjunath R Kounte, Abdul Haq Nalband, Mohammed Riyaz Ahmed
School of Electronics and Communication Engineering, REVA University, Bengaluru, India

***Abstract*—The emergence of the Internet of Things (IoT) has revolutionized the way we interact with the physical world. The rapid growth of IoT devices has led to a pressing need for robust security measures. Two promising approaches that can enhance IoT security are blockchain and artificial intelligence (AI). Blockchain can offer a decentralized and tamper-proof framework, ensuring the confidentiality and integrity of IoT data. AI can analyze large volumes of real-time data and detect anomalies in response to security threats in the IoT ecosystem. This paper explores the potential of these technologies and how they complement each other to provide a secured IoT system. Our main argument is that combining blockchain with AI can provide a robust solution for securing IoT networks and safeguarding the privacy of IoT users. This survey paper aims to provide a comprehensive understanding of the potential of these technologies for securing IoT networks and discuss the challenges and opportunities associated with their integration. It also provides a discussion on the current state of research on this topic and presents future research directions in this area.**

***Keywords*—IoT; blockchain; AI; security; attacks; decentralization**

I. Introduction

The emergence of Industry 4.0 in the 21st century marked a significant change in the industrial paradigm, leading to improvements in social, economic, and political conditions[1]. Industry 4.0 enables the use of cyber-physical systems such as the IoT, big data analytics, cloud manufacturing, and fog computing, supported by cutting-edge technologies such as blockchain, AI, and mobile networks [2]. The integration of IoT, blockchain, and AI enhances human-machine interaction and brings the physical and digital worlds closer than ever before [3]. These technologies are expected to offer numerous benefits and opportunities, including self-awareness, self-prediction, self-comparison, self-reconfiguration, and self-maintenance [4].

The IoT is the driving force behind Industry 4.0, enabling seamless inter-connectivity of various devices and objects to construct a network infrastructure that continuously regulates and manages sensing, processing, and communication processes without human intervention [5]. The daily introduction of new applications and services is one of the many advantages of the IoT system. According to Statista [6], in 2020, there were about 50 billion IoT devices worldwide. By the end of 2025, that number is expected to reach over 75 billion devices.. Fig. 1 describes the timely growth in the number of IoT devices. The IoT market is expanding at an almost exponential rate. It was valued at USD 743 billion in 2015, which increased to approximately USD 1710 billion by the end of 2019 [7]. The global IoT market is expected to be worth

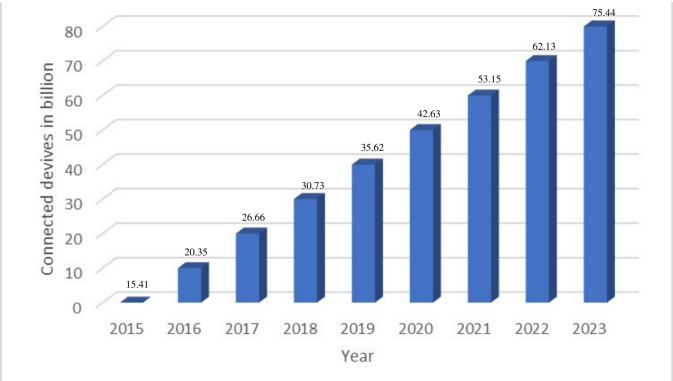

Fig. 1. Growth of IoT devices over the time 2015 to present.

186 billion dollars by the end of 2023, while the market for intelligent homes will be around 130 billion.

IoT has predominantly adopted the centralized architecture model for storing and processing sensor data. The central server serves as the network's manager, handling all requests from various nodes and overseeing task scheduling and distribution [8]. It saves costs by not requiring the installation of multiple workstations of hardware and software, as most processing tasks are managed by the centralized server. However, this architecture model has several challenges, including scaling issues due to the increasing number of IoT devices and various security and privacy concerns [9]. Table I summarizes the challenges posed by centralized IoT architecture. It is challenging to address the fundamental security concerns for such a large information ecosystem. Additionally, the centralized IoT model is susceptible to security breaches, single points of failure, and malicious assaults like DDoS and Sybil attacks[10][11].

Blockchain technology can help to address key security requirements in IoT, thanks to its "security by design" feature. The majority of IoT's architectural flaws can be fixed using blockchain's characteristics, including immutability, transparency, auditability, data encryption, and operational resilience. Blockchain is a decentralized network where all users have full control over peer-to-peer (P2P) monitoring of all network transactions[12]. Another technology that can strongly influence IoT is AI. Integration of AI into IoT devices can make them smart and intelligent [13]. AI can be used to train machines to understand novel material based on the training process they have already undergone.The goal of AI in IoT is to use IoT devices to gather relevant data and draw useful conclusions from that data. AIoT, or the merging of AI and the IoT, can be used to improve data analysis, human-machine

TABLE I. SUMMARY OF CHALLENGES IN CENTRALIZED MODEL OF IOT

Reference	IoT Challenge	Description
[9]	Security	Security is one of the primary issues (particularly DoS attacks) with centralized IoT design, because all data storage and processing operations are carried out by a single central server.
[10]	Single Point of Failure	Single point of failure is a problem since the server controls connections and carries out all processing tasks. If the server fails, the entire network of devices will stop working.
[14]	Access and Diversity	System should be accessible for all users with their dynamic needs. Yet, the centralized system requires that users access the data uniformly by adhering to the same protocols. Also, most of the centralized systems only support a single operating system, which restricts network diversity. IoT system includes heterogeneous and diverse devices, this will result in a serious issue that needs to be handled.
[15]	Inflexibility	A significant workload is generated by the centralised server's control over activities of communication and processing between all IoT network nodes. The centralized server schedules the workload to manage this workload and avoid peak-load problems. However, due to the constrained schedule and associated delay, this restricts user flexibility while performing their own duties.
[16]	Privacy	Sensitive data is among the real-time data types that IoT devices collect, such as habits, password, financial and personal information, etc. The centralised third-party server, which has complete control over this acquired data, keeps them all in one place while also violating their privacy. However, keeping it in one place could make it more vulnerable to intrusions.
[17]	Cost	The network's central server handles all of the communication and processing tasks, which place a heavy demand on the hardware and software needed to handle the workload. It also requires sizable storing storages that can hold data from diverse IoT devices.
[18]	Scalability	Among the main issues linked with the centralised architecture is scalability. Controlling and attempting to control all the network's nodes via a centralized server can scale successfully only in small networks. Using centralized system to big corporate organizations will be illogical. The centralised solution cannot scale and operate well since the number of Internet of Things devices is constantly growing.

interactions, and IoT operations [19]. The integration of decentralized AI has grown recently, enabling the execution and storage of an investigation or dynamic on verified, carefully annotated, and shared data on the blockchain in an automated, decentralized manner without middlemen[20][21]. Blockchain-based AI techniques can provide decentralized reasoning on how to promote safe and trust in the exchange of information and decision results over numerous independent operators who can can contribute, organize, and vote on additional decisions [22]. This paper presents the joint potential of blockchain and AI for securing the industrial IoT system. The contributions made by this paper are as follows:

•Details of numerous security concerns in IoT ecosystem are described.

•Presented a concise literature review on security issues and their solutions.

•An architectural framework that integrates blockchain and AI for a secured IoT has been proposed.

The remainder of the study is organised as follows; in Section II, we go over the background of the IIoT, Blockchain, AI, and security concerns with IoT. We provide a full assessment of the literature on security-related issues, challenges, and solutions in Section III. In addition, this part illustrates how blockchain and AI combine to create a safe IoT environment. We provide the proposed architectural framework for combining blockchain and AI to improve IoT security in Section IV. We present high-level blockchain-driven AI and AI-driven blockchain as examples of how AI and Blockchain can be applied in IoT use cases. Section V provides the conclusion to the research findings.

II. BACKGROUND

The Industrial Internet of Things (IIoT) emerged from the intersection of manufacturing technology, industrial automation, and data sharing. Fig. 2 illustrates the timeline of the significant events that have contributed to IIoT's development. The evolution of Industry 4.0 has been fuelled by numerous game-changing advancements, including the availability of low-cost sensors, big data analytics, AI and machine learning (ML), the IoT, robotics, edge computing, standard communication protocols, and enhanced security technologies such as encryption, authentication, and intrusion detection. As IIoT continues to progress, it has the potential to revolutionize various industries, such as manufacturing, logistics, healthcare, and energy. The impact of IIoT on these sectors is expected to be substantial, with efficiency, safety, and productivity improvements. For example, IIoT devices can help identify bottlenecks and optimize production processes in manufacturing, while in healthcare, connected devices can monitor patient health and aid in timely interventions. Overall, the IIoT represents a significant opportunity for businesses to transform their operations and unlock new value.

A. Evolution of Industry 4.0

The development of Industry 4.0 can be traced through several key milestones. It began with the digitization of production processes, which involved integrating digital technology like sensors and smart machines into industrial equipment and systems. This increased automation and data collection, laying the foundation for the next phase. The second phase involved the development of interconnected factories and supply networks. This was made possible through the adoption of IoT technologies, which allowed machines and gadgets to communicate with each other and share data in real time. Connected factories and supply chains became a reality, and this marked a significant advancement in Industry 4.0's evolution. The third phase saw the emergence of advanced analytics and artificial intelligence technologies that could analyse and make sense of the massive amounts of data produced by connected factories and supply networks. These technologies are employed to raise productivity, anticipate and avoid equipment breakdowns, and improve the production cycle. As machines and robots become more sophisticated, a collaboration between humans and machines has become a primary focus of Industry 4.0. This involves developing systems that allow people and machines to coexist in harmony, with machines handling routine jobs and people focusing on those that require creativity and problem-solving abilities. With the increased use of digital technology, cybersecurity has emerged as a critical issue for Industry 4.0. Companies have invested in technology and procedures to secure their systems from cyber-attacks, and this has become a hallmark of Industry 4.0's development.

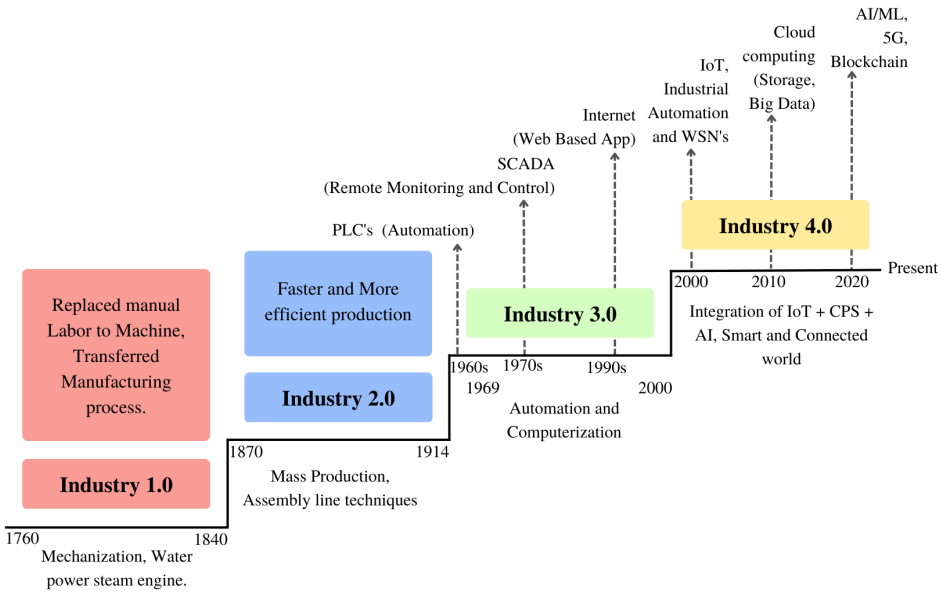

Fig. 2. Evolution of industrial revolution 4.0.

TABLE II. SECURITY ATTACKS IN IOT ECOSYSTEM

IoT Level	IoT Layer	IoT Protocol	IoT Security Attacks
Deployment	Application	CoAP, MQTT,AMQP ,REST	DDoS Attack, Repudiation Attack, SQL Injection Attack, Cross-Site Scripting, Parameter Tampering, Slowloris Attack, HTTP Flood Attack
Data	Transport, Network	UDP,TCP, DCCP, RSVP, SCTP,CLNS,QUIC,DDP,IGMP EIGRP,IPsec, ICMP,IPv6,IPv4, RIM, OSPF	Smruf Attack, SYN Flood,Mitnick Attack,Injection Attack, DoS Attack, Opt-ack Attack IP Address Spoofing, Worm Hole Attack Byzantine Attack, Resource Consumption Attack, Black Hole Attack
Device	Physical	ISDN,DSL, USB, IDA, CAN,Bluetooth, Ethernet	Access Control Attack, Disconnection of Physical Links, Physical damage

B. Security Concerns in IoT

The IoT devices gather and transmit vast amounts of data, including sensitive or private information such as medical records or video footage from home security systems. Ensuring the security of this data is critical to protect privacy and prevent identity theft. Unfortunately, IoT devices are frequently targeted by cybercriminals because they are often insecure and provide an easy entry point to a larger network. Successful cyber-attacks can result in data breaches, financial losses, and even physical harm. Additionally, many critical infrastructure systems, such as power grids and transportation systems, are controlled by a large number of IoT devices [23]. If these systems are compromised, the consequences can be severe, including widespread disruption, financial losses, and even loss of life. It is essential that IoT devices adhere to strict data privacy and security regulations in industries such as healthcare and banking to avoid legal repercussions and reputational harm. To ensure the security of IoT devices, it is necessary to implement security measures at three different levels: device, data, and deployment [24]. These levels correspond to the IoT's architectural layers, with specific protocols used in each tier of the IoT architecture to protect against related security attacks (Table II). Techniques such as encryption, authentication, and access control can be used to secure sensitive data from unauthorized access. IoT devices are often deployed in remote or harsh environments, making them vulnerable to physical attacks such as theft or manipulation. Physical security measures such as tamper-evident seals, firmware upgrades, and patches can help guard against these risks. Additionally, cyber attackers can compromise IoT devices and use malware such as DDoS, HTTP flood, SQL injection, and parameter tampering to control the devices and exploit their vulnerabilities. It is crucial to protect against these threats by regularly updating firmware and applying security patches.

C. Blockchain for IoT Security

Blockchain technology offers solutions to several security challenges facing IoT systems, such as data privacy, data integrity, and device authentication. By providing a secure, decentralized, and immutable system, it can defend against DDoS attacks, data manipulation, and unauthorized access. Its architecture combines hash algorithms with decentralized ledgers that use public and private keys, offering a potent alternative to the internet [25]. Blockchain ensures secure data storage and can prevent rogue IoT devices from entering the network. It can also reduce the costs of litigation caused by disagreements [26]. Transactions are protected by a consensus mechanism that ensures their integrity even in the presence of faults or hostile conditions, thus enabling a stable blockchain [27]. Moreover, blockchain can be combined with smart contracts to increase dependability and radio-frequency identification is safeguarded by attribute-based access control mechanisms [28]. In blockchain, each block contains its data, the previous block's hash, and the security hash code. It can offer secure

TABLE III. ENABLERS OF SECURED IOT SYSTEM

	Blockchain for IoT Security
Data privacy	PData can be protected by using blockchain to store it in a decentralized, tamper-proof manner. Blockchain's public-key encryption ensures that only authorized parties can access the data.
Data integrity	Data integrity is guaranteed by the tamper-proof ledger in blockchain, which is immune to hacking and data modification. This guarantees the accuracy and dependability of the data that IoT devices collect.
Device authentication	Blockchain offers a safe and decentralized method for IoT device authentication. Each gadget can be given an own digital identity, making it simple to trace it down and confirm its legitimacy
DDoS	Blockchain establishes a distributed network of nodes capable of validating and verifying data sent by IoT devices. By limiting the amount of devices that may access the network, this can assist avoid DDoS attacks.
	AI for IoT Security
Anomaly detection	AI assists in identifying potential security concerns, such as malicious activity or unexpected network traffic, and alerting security teams to take appropriate action by detecting anomalies in the behaviour of IoT devices and networks.
Predictive maintenance	IoT device monitoring and forecasting of potential failures and maintenance needs. By doing this, security lapses brought on by unsecured or infected devices may be avoided.
Behavioral analytics	Investigate trends in the actions of IoT users and devices to look for potential security risks. An IoT device may have experienced a security breach if it suddenly starts transmitting significant amounts of data at odd hours.
Cyber threat intelligence	To address potential security concerns in IoT devices and networks, collect and evaluate data about known cyber threats and vulnerabilities. This can assist businesses in taking preventative measures to safeguard their networks and devices from threats.
Identity and access management	For IoT networks and devices, AI can be utilised to enhance identification and access control. In order to assist prevent unauthorised access to devices and networks, this may also include user authentication, authorisation, and access control.

data transfer over IoT device nodes, and its lightweight and sustainable algorithm employs decentralized techniques for authentication in distributed resource-constrained systems [29]. Certain companies might be capable to handle dependability issues with a double-chain design that uses data and transaction blockchain for storage, distribution, and data reliability, but there are risks related to privacy vulnerability [30]. Various studies have examined the use of blockchain in securing IoT, such as [31] and [32], which provided an overview of the security issues with IoT and how blockchain can be applied to address them. However, [33] critically analyzed the limits of using blockchain-based IoT platforms, offered a taxonomy of blockchain typologies, weighing their benefits and drawbacks in incorporating them into IoT. Several ideas have been proposed for using blockchain and AI technologies to address specific security issues of IoT, such as allowing smart contracts, IoT devices to update their firmware, or developing a system in which devices can acquire "money" by exchanging resources or data for goods or services [34]-[36]. Table III summarizes how blockchain and AI technologies individually help address security concerns of IoT.

D. AI for IoT Security

The integration of AI into the IoT devices can significantly enhance their performance and security. AI can simulate human learning processes such as decision-making, problem-solving, and object identification, making IoT devices intelligent and more efficient. By combining AI and IoT, businesses can generate useful data and obtain insights, making their operations more effective [37]. One of the main benefits of using AI in IoT is its ability to quickly identify potential security threats and holes. AI can examine network traffic and user activity trends, identify vulnerabilities, and prioritize them according to their severity [38]. With AI, businesses can automate the patching of IoT devices, ensuring that they are up-to-date with the latest security patches, reducing the chance of security breaches [39]. AI can also track user and IoT device behaviour, detecting any unusual activity that might point to a security breach, allowing organizations to respond quickly to threats. Secure access control, offloading, and virus detection can be provided by AI-based authentication employing machine learning to preserve data privacy [40]. By using the analytical capabilities of AI, businesses can uncover patterns and make better decisions about IoT data collection. AI can enhance the object identification technique utilized by smart cameras, enabling them to recognize dangerous objects like knives and guns instantly. However, AIoT frameworks are prone to data security and privacy issues. To address these issues, researchers are developing solutions such as blockchain, which offers greater protection than conventional security measures since it cannot be altered. Many AIoT applications can incorporate blockchain to boost security. The security concerns that blockchain and AI address when used independently with IoT are listed in Table IV. Overall, the combination of AI and IoT can significantly enhance businesses' operations and security. By using AI, businesses can identify potential threats quickly, automate patching, and make better decisions about data collection. Integrating blockchain into AIoT applications can enhance security, ensuring data privacy and reducing the risks of security breaches.

TABLE IV. IOT SECURITY CONCERNS ADDRESSED BY BLOCKCHAIN AND AI

Security Issues Addressed by Blockchain	Security Issues Addressed by AI
Verification of Identity	Intrusion detection system
Self-healing and detection of firmware	Malware detection
Address space and privacy preservation	Anomaly detection
Secured communication and data integrity	Unauthorized IoT devices identification
Authorization and authentication	Distributed denial-of-service
Information sharing and access control	Jamming attack, Spoofing attack
Secure computation and storage	Authentication, Eavesdropping
Trust-management	False data injection, Impersonation

E. Convergence of Blockchain and AI for IoT Security

The combination of blockchain, IoT, and AI is becoming exceptionally important in the realm of digital transformation, particularly for IoT security. With this convergence, new business strategies are emerging that involve the creation of autonomous profit centers made up of autonomous agents, such as sensors, vehicles, machines, trucks, cameras, and other IoT devices. These autonomous agents will have digital twins through IoT, enabling them to independently send and receive money through blockchain technology and make decisions using AI and data analytics. As a result, we predict that

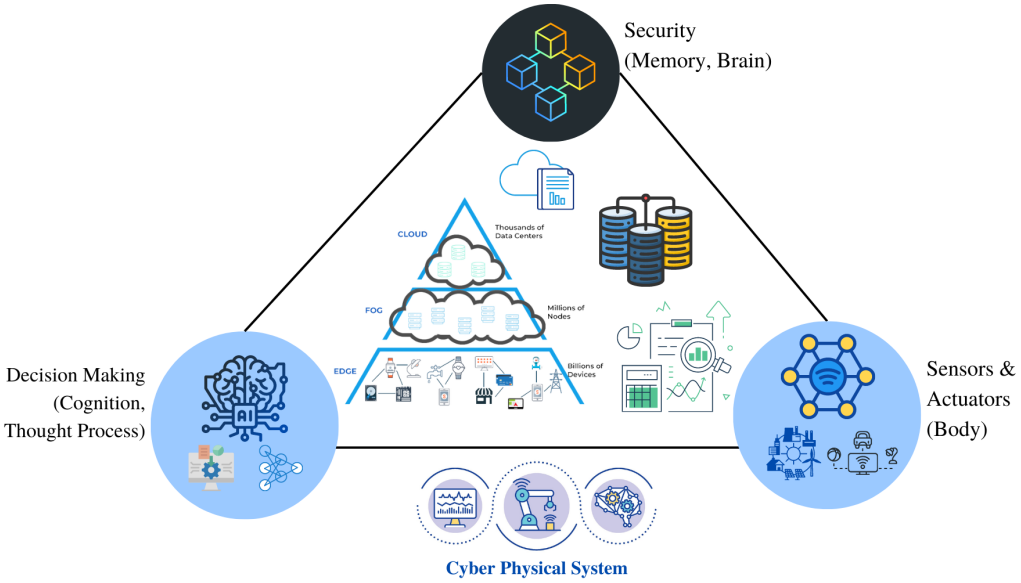

Fig. 3. Convergence of blockchain, AI towards secured IoT.

industrial firms will undergo a digital transition as these autonomous business models continue to evolve.

In recent years, IoT devices have collected an enormous amount of data centrally, causing security and space issues [41]. However, the integration of AI, blockchain and IoT offers a solution to this problem by creating a distributed database [42]. Decentralized AI, which is a growing concept, integrates these two technologies to allow for distributed, unmediated execution and storage of data on the blockchain without middlemen. Blockchain is expected to be a reliable platform for storing vast volumes of data that AI works with. With the blockchain's smart contract functionality [43], it is possible to keep track of member participation and transactions while accessing information. An autonomous system and machine can then choose exact and reliable option outcomes that are verified and acknowledged by all blockchain mining centers [44]. These decisions cannot be contested and can be supported by anyone with a stake in the outcome.

Blockchain, AI, and IoT have successfully combined, as seen in Fig. 3. The integration of these technologies can address several critical issues such as accuracy, latency, centralization, privacy and security issues in IoT. Decentralized reasoning provided by blockchain-based AI algorithms can benefit a large number of independent operators who may contribute, organize, and vote on new decisions [45]. Blockchain databases have hash values that are digitally signed to ensure secure and reliable processing of transactions. AI algorithms are used to solve issues related to accuracy, latency, security, and privacy, and to enhance big data analysis. The decentralization of blockchain networks eliminates the single point of failure in a cloud server, making it more efficient and reliable for data analysis. By integrating AI and blockchain technology, the IoT can be aided with better decision-making capabilities.

To further enhance the integration of blockchain, AI, and IoT, there are several areas that need to be addressed. For instance, the integration of these technologies requires a strong and secure infrastructure, as well as effective governance and regulatory frameworks. There is also a need to address the ethical and social implications of using these technologies, such as issues related to data security, privacy and bias. Moreover, the adoption of blockchain, AI, and IoT will require a significant investment in research and development, as well as in the training of personnel to effectively manage and maintain these technologies. Nevertheless, the benefits of this convergence are substantial, including increased efficiency, improved security, and better decision-making processes. As these technologies continue to evolve, it is likely that we will see even more innovative ways to combine them. The convergence of blockchain, AI, and IoT has the potential to transform the way we live, work, and interact with one another. It is an exciting time to be at the forefront of this convergence and to witness the transformative power of technology.

The Big Data revolution has been a key driver of the AI revolution, as it enables businesses to divide vast databases into manageable, organized components. Additionally, the value of data has propelled the development of blockchain technology, as its distributed ledger offers a new, more efficient way to store data. This combination has the potential to significantly transform how information is handled, analyzed, and shared, ultimately making operations inside a company more efficient and effective. As AI continues to evolve, we may see the emergence of new AI systems, such as logic-based systems, bio-inspired systems, collaborative agents, cyber-physical intelligent systems, and ubiquitous AI or pervasive intelligence systems, which could fundamentally change our daily lives.

Machine Learning, a branch of AI, has gained significant popularity in recent years due to its ability to analyse huge data flows. It has found applications in various fields such as business, entertainment and research. Many countries and organizations, including Google, Amazon, Facebook, Microsoft,

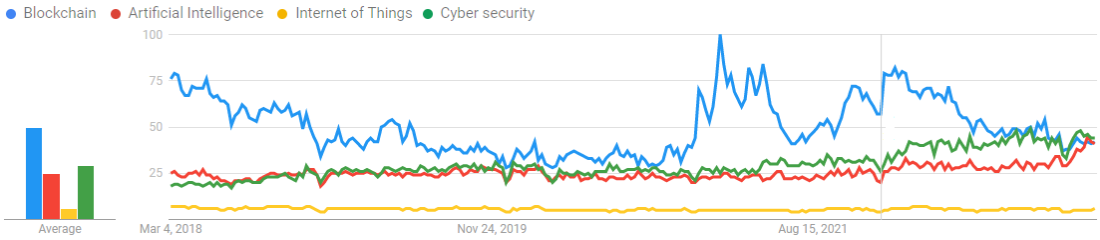

Fig. 4. Research trends in blockchain, AI, IoT and cyber security.

IBM, Apple, Intel, Alibaba, Baidu, and Uber, have invested heavily in developing cutting-edge ML goods, programs and platforms that can be used as cloud services to run ML models effectively, known as MLaaS. Cloud computing is a popular and cost-effective platform for running ML models used in many IoT and smart city services and applications, such as text classification, automated language processing, facial recognition, speech recognition, computer vision and speech synthesis. Additionally, several nations have launched ambitious national AI initiatives in less than a year [46], indicating the potential impact of ML and AI on various sectors.

The integration of Blockchain, AI, and IoT has been the subject of many experiments and hypotheses, but further research is necessary to develop a functional and reliable digital component that properly combines the three. Cloud computing is crucial in today's world and facilitates online connectivity. However, the vast amount of data handled by this system highlights the need for automated systems with quality of service (QoS) standards. The convergence of Blockchain, AI, and IoT is identified as a critical technology to meet this requirement. Consequently, the extensive use of AI and blockchain integration will bring about exciting advancements in Industry 4.0. Instead of only discussing software, algorithms, automation, robotics, and hardware, businesses are now exploring more sophisticated concepts such as producing and manufacturing items on-demand, dematerialization, and disintermediation. Industry 4.0 emphasizes distinct pillars including information transparency, support, and connection, and it represents the first major revolution that moves from a tech-centric state to a more sophisticated one.

III. Literature Review

A. Security Requirements in IoT

IoT devices need strong security measures to prevent unwanted access and data breaches since, like any linked system, they are susceptible to cyber-attacks. In the IoT ecosystem, some of the primary security requirements are; only devices or users that have been authenticated can access the network. This can be done via techniques including digital certificates, biometric identity, two-factor authentication, and password protection. To prevent unlawful interception, data transferred between IoT devices should be encrypted[47]. Data in transit and at rest should be protected using robust encryption techniques like Advanced Encryption Standard (AES) and RSA algorithm. Access control - It is important to prevent unauthorized access to network data. This group can include additional access control techniques as well as attribute- and role-based access control. IoT devices should be built to constantly download and install firmware upgrades to address security holes and enhance functionality. In order to prevent malicious firmware updates, devices should provide a method for confirming the integrity of firmware upgrades. Physical security - In order to avoid unwanted access or tampering, IoT devices should be physically secure[48]. These can include steps like secure boot procedures, tamper-resistant designs, and physical security controls like locks and access cards. Privacy - IoT devices should respect user privacy by only gathering information that is required and handling it securely. Users should be clearly informed by devices about the types of data being gathered and how they are being used. Network security - IoT devices should be built to function safely on both public and private networks, among other network environments. This may involve taking precautions like installing firewalls, installing intrusion detection and prevention systems, or using secure communication protocols like VPNs. In order to stay abreast of the most recent security threats and vulnerabilities, a solid security strategy for the IoT ecosystem should be multi-layered, proactive, and constantly developing.

B. Avenues of Cyber Attacks in IoT

The connection between IoT devices offer several opportunities for cyber criminals to find flaws and launch assaults. Here are a few typical IoT ecosystem cyber-attack vectors. Poor authentication methods - IoT devices are susceptible to assaults like brute force attacks, dictionary attacks, and password cracking attacks if they employ weak or default passwords or have no authentication mechanisms at all. Unsecured communication protocols: IoT devices that employ these protocols are susceptible to replay, eavesdropping, and man-in-the-middle attacks. IoT devices that run out-of-date or unpatched software may contain vulnerabilities that attackers can take advantage of[49]. Buffer overflows, SQL injections, and cross-site scripting attacks are some examples of these flaws. IoT devices are susceptible to malware and ransomware infections, which might jeopardize the ecosystem's overall security. DDoS assaults, botnet attacks, and other malicious activities can all be carried out via malware on a system. Physical tampering: IoT devices that lack physical security are susceptible to physical tampering, which gives hackers access to the system without authorization, gives them the chance to steal data, or modifies the device's behaviour [50]. Social engineering - Social engineering attacks, such as phishing assaults or pretexting, which deceive users into disclosing sensitive information or installing malware, can be used to target IoT devices. Fig. 4 depicts research trend in the domains of Blockchain, AI, IoT and Cyber security

TABLE V. RELATED SURVEYS ON IOT SECURITY

Reference	Year	Description
[53]	2014	Three layers of IoT security are examined, as well as the appropriate fix.
[54]	2016	The proposed design is built on IoT middleware, and each layer's specifics are detailed. The authors also discussed the IoT middleware system's adaptability and security challenges.
[55]	2016	Presented the reference model and the edge-side security threads. The countermeasure to the potential solutions was also discussed in the study.
[56]	2017	Outlined the merging of the IoT with Cyber-Physical Systems. Detailed examination of the privacy and security issues. The integration of edge/fog computing with IoT is considered.
[57]	2017	The study surveyed participants about their privacy and security concerns with IoT applications and devices. The authors looked at the authentication process for the IoT system.IoT applications built on a four-layer architecture provide difficult security challenges that are thoroughly explained.
[58]	2017	The authors of this study looked into modern security concerns in IoT applications. IThe risks and vulnerabilities of the system are thoroughly investigated in terms of communications, architecture, and applications.The paper's conclusion offers a strategy for resolving several security problems.
[59]	2018	The paper offers a thorough analysis of IoT security layer-by-layer. Suitable countermeasures and a model of probable dangers are thoroughly examined.
[60]	2018	Look at the danger and security model for IoT applications. The article discussed a few IoT system problems, including access control, trust management, and authentication.
[61]	2018	IoT systems' many standardized architectures have been reviewed, and the current solution strategy for security and interoperability is described.
[62]	2019	Examined the hazard and security in IoT applications. The use of Blockchain, edge computing, fog computing, and alternative solution approaches was suggested.
[63]	2020	There is a newly emerging technology that can address IoT security concerns. During a thorough investigation, the authors discovered that artificial intelligence, blockchain technology, and machine learning are the current approaches being used to address the IoT security problem.
[64]	2021	Security, trust, and faultless communication issues affecting the integration of IoT with blockchain are examined. Described in detail the study process used to examine the problems with the integration of blockchain, AI, and IoT.
[65]	2022	The IoT, blockchain and AI-based authentication in cybersecurity are all combined in this paper to give researchers a full, high-quality study on authentication and session keys.

TABLE VI. SOLUTIONS TO IOT SECURITY ATTACKS/CHALLENGES

Reference	Technique Used	Security Attack/Challenge	Measure Taken	Description
[66]	Edge computing using permission based blockchain for Smart Grid Network	The use of viability and the allocation of funds are under attack	transparent agreements updated on the blockchain	Solves the problems of intelligent systems, information security, and viability security by combining square chain and limit registration approaches.
[67]	Distributed security model using blockchain, edge cloud, and software-defined networking	Security attacks at edge layer of IoT network	SDN based gateway to hinder the doubtful flows.	By computing suspicious network traffic flows and preventing suspicious flows, the SDN-based gateway's dynamic network traffic flow management aids in the detection of security assaults and lowers their frequency.
[68]	Privacy protection of location data mining	Protection of location data records	Differential privacy mechanism	Using a multi-level query tree's structure and a different privacy method, you can query and publish location data on databases.
[69]	Privacy protection technique for location data	Privacy protection for location data	L ocation sensitivity for location recommendation	It uses check-in frequencies and location trajectories to determine a threshold for categorizing the sensitivity level of the places.
[70]	Privacy protection is integrated to machine learning	Classification process for local differential privacy protection	Logistic regression is applied for noise addition and feature selection	To achieve classification utilizing noise addition and feature selection, local differential privacy protection is created.

C. Related Work

Some study has already been done by researchers on the topic of how AI and IoT may work together to improve computation and decision-making in IoT systems. The work employs an master attack in the IoT to enable AI-based smart city applications [51]. In Zou et al. [52], similar explanations of fog and edge computing in IoT may be found. The Blockchain network employs a number of consensus techniques to reach consensus among the nodes. The design and potential uses of the Blockchain are thoroughly explained in the authors' essay [71]. In their study [72], the authors examined the concept, relevant research on IoT security and a possible approach to a solution using blockchain. The authors proposed a secure architecture for internet of things applications built on a distributed Blockchain system [73].

The authors' paper [74] briefly discusses how Blockchain technology is used in the Internet of Things. In paper [75], the authors assess the several Blockchain options for IoT security challenges as well as their implementation issues. To analyse and calculate the massive data collection using a machine learning technique, an effective framework [76] is needed. The authors of paper [77] examine the security concerns raised by using machine learning to a smart grid application. The authors of article [78] discuss intrusion detection in Internet of Things applications. Table V summarizes the related survey works in the area of IoT security.

IoT issues were divided into four groups in Kshetri et al. research's [79]: (i) Cost and Capacity Limitations (ii) Deficient Architecture (iii) Downtime and Unavailability of Services on Cloud Servers (iv) Susceptibility to Manipulation. Their research covered the significance of blockchain in enhancing general security in supply chain networks as well as potential Blockchain solutions to each IoT concern. IoT datasets, which are used by the academic and expert communities, are one of the issues Banerjee et al. [80] examined when researching IoT security solutions. A standard for communicating IoT data values among research and expert communities, other pertinent partners, and vendors is necessary given the potentially conscious character of IoT datasets. In the future, blockchain technology should be made accessible to secure the security of IoT applications. Li et al. [81] offered a thorough analysis of the security risks to blockchain technology and talked about analogous actual attacks by extending well-liked Blockchain systems. They examined the blockchain technology security augmentation options. Table VI summarizes the techniques and countermeasures to address security attacks in IoT.

TABLE VII. INNOVATIONS THROUGH THE CONVERGENCE OF BLOCKCHAIN, AI AND IOT

Reference	Enablers	Innovation Domain	Use case	Description
[82]	Big data, 5G, Cloud Computing	Software Engineering	Blockchain-as-a- service (BaaS)	Cloud-based infrastructure and management provided by a third party for businesses developing and running blockchain applications. BaaS performs the back-end management for a platform or app built on blockchain in a manner similar to that of a web host.
[83]	Digital Twin	Data analytics	Intelligent money transaction - own profit centers (Autonomous agent)	IoT-based digital twins that can send and receive money via blockchain technology and act independently as economic agents can all do this.
[83]	Deep Reinforcement Learning	Block producers, consensus algorithm, block size, and block interval	Blockchain enabled IoT System	Framework for performance tuning to increase throughput.
[84]	Decentralization, AI algorithms	Digitally signed hash values, Data validation	Secure banking system	Reduces difficulties with accuracy, latency, privacy and security, and centralization.
[85]	Open source software	Bitcoin Protocol	Trust Management	It increases confidence in the system when a miner completes Proof of Work (PoW) without the aid of a bank or other centralised authority. Blockchain technology makes consumers think that no one can be trusted and that no one can make a claim to be one as a result.
[86]	Edge computing	Control and manage computation workload distribution	Data integrity and ensuring its availability and user accountability	Giving dispersed IoT hardware a reliable way to distribute computation-workload control and management across a large number of nodes.

D. Blockchain for AI in Addressing IoT Security

The AI can complete all tasks without outside influence with the aid of the Blockchain. Hence, all analysis and decision-making may be done on a private and secure platform. A decentralized AI platform also prevents data manipulation. Although AI and machine learning are two distinct methodologies, they are somewhat interconnected. The AI program employs a method called machine learning to respond to the tasks that are put in front of it. Unsupervised learning and supervised learning are the two types of learning that can be employed when creating and training an AI. Blockchain can be used in the context of AI to protect data produced by IoT devices, which is frequently utilized to train AI models. Blockchain can aid in preventing data tampering, manipulation, and unauthorized access by building a secure, decentralized record of this data. This can safeguard users' privacy while enhancing the accuracy and dependability of AI models. Securing device communication is another potential use for blockchain-based AI in IoT security. Without a centralized authority or middleman, devices can establish safe communication channels by using blockchain-based smart contracts to verify one other's identities. Attacks like man-in-the-middle attacks, which are frequent in IoT environments, could be avoided as a result of this.

E. AI for Blockchain for Addressing IoT Security

AI can help blockchain technology overcome some of its drawbacks, such as consensus procedures. Nodes can validate transactions rapidly and effectively in Proof of Work (PoW) or Proof of Stake (PoS) by using AI. Also, as the mining process uses a lot of energy, AI can help blockchains use less energy. This is possible by implementing AI technologies that have proven successful in reducing energy consumption. Using federated learning, for instance, which can offer a decentralized learning system, can help alleviate the scalability problems of blockchain. Also, while blockchain offers greater security than current technologies, AI can add an extra layer of security. IoT device data is analysed by AI algorithms to spot patterns and anomalies that can point to security lapses or other risks. AI can assist in preventing and reducing security concerns by continuously monitoring the data produced by IoT devices and using machine learning algorithms to spot anomalous activity. Digital signatures are used by blockchain-based systems to verify transactions. These signatures can be examined by AI systems to find patterns that might point to fraud or other sorts of harmful behaviour. This could aid in limiting illegal access to IoT networks or devices. IoT devices produce a lot of data that can be used to forecast when a gadget is most likely to break down. This might lessen security threats that might be brought on by a corrupted or broken device. Strong authentication procedures are needed for blockchain-based systems to make sure that only authorized users can access devices and networks. To identify individuals and prevent illegal access, AI algorithms can be employed to examine biometric data such as facial recognition or voice recognition.In summary, the blockchain and AI work together to enhance the security of the IoT ecosystem. As outlined in Table VII, the blockchain and AI work together to pave the road for innovations in the IoT space.

IV. PROPOSED ARCHITECTURAL FRAMEWORK

Security, privacy, and scalability concerns can be addressed by designing a new framework for a Blockchain-based AI-enhanced IoT system. Fig. 5 depicts the proposed layered architectural framework for secured IoT. The layers of proposed architecture are as follows:

1) Perception layer:: IoT devices that gather and send data to the system are part of the perception layer. The system's core elements are IoT devices. They are in charge of gathering (sensing), storing, acting upon, and sending information to the system. They gather information from a variety of sensors, including temperature, humidity, and motion sensors.

2) Network layer:: This layer includes communication network that links the IoT devices to the system. To protect against any unauthorized access or data tampering, the network needs to be trustworthy and secure. VPNs and cryptographic protocols like SSL/TLS can be used to increase network security.

3) Security layer:: This layer contains the security defenses against cyber-attacks, including access control, encryption, and authentication. It guarantees the system's availability, integrity,

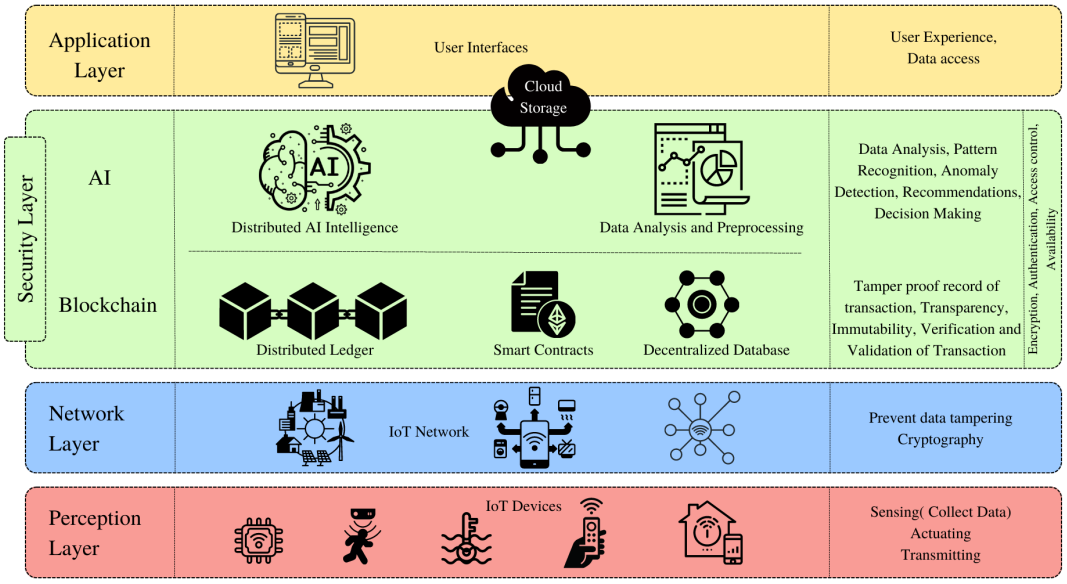

Fig. 5. Architectural Framework Integrating Blockchain and AI for Secured IoT.

and secrecy. The data gathered from the IoT devices is stored in the cloud and on the Blockchain. A distributed ledger in the Blockchain keeps a tamper-proof record of all transactions. It guarantees the system's immutability, transparency, and security. Blockchain offers a secure, distributed database for storing all of the transactions. Large volumes of data are stored in the cloud storage, which also gives the system scalability. Smart contracts are self-executing agreements that uphold the system's laws and regulations. They aid in the automation of the transactions' validation and verification processes. The data gathered from IoT devices is stored and processed using cloud computing. It gives the system flexibility, scalability, and affordability. The distributed ledger of the blockchain offers a new way to store data in a more efficient manner. Blockchain and AI working together has implications for a variety of fields, including Security: AI and blockchain may combine to provide an additional line of defense against online dangers. Uncovering suspicious events is one of the most challenging issues facing upcoming businesses. Some, however, are already utilizing machine learning technologies that help in instantly spotting them. Speed – Combining the two technologies may speed up the delivery of information and data, improving the efficiency and speed of consumer interactions with enterprises. Service customization will increase over the coming years, and large companies' or businesses' recommendation systems will become widely used.

The artificial intelligence algorithms used to analyze the data gathered from IoT devices are included in this layer. AI assists in spotting trends, patterns, and abnormalities in the data. Additionally, it offers suggestions and forecasts based on the data analysis. AI offers insightful information that aids in decision-making. The data gathered from IoT devices is processed using data analytics. It assists with spotting trends, patterns, and abnormalities in the data.

4) Application layer:: User interface, data analytics, and other programs that enable the system's functionality are all included in the application layer. The system's data and analytics are accessed through the user interface, which is also used to interact with the system. IoT device data is processed using data analytics, which offers insightful information.

The proposed framework offers a safe, scalable, and effective solution to manage IoT devices, gather data, and use AI and data analytics to make wise decisions. While the use of AI and data analytics provide useful insights and aids in making decisions, the usage of Blockchain protects the security, transparency, and immutability of the system. An additional layer of defense against cyber-attacks is offered by the security layer.

V. Conclusion

Blockchain and AI coming together is a promising way to secure the IoT ecosystem. IoT devices are prone to cyber-attacks, and a decentralized architecture supported by blockchain and AI can offer a practical solution to improve the security of these devices. The purpose of this suggested framework is to investigate the potential benefits of this convergence for secure IoT. The framework can improve the data acquired by IoT devices in terms of security, transparency, and privacy. Additionally, it can lessen the need on centralized middlemen and offer a decentralized platform for data transfer and communication amongst IoT devices. The IoT ecosystem's security and the development of the digital future may both benefit from the integration of blockchain and AI. Several theories and tests have been conducted in an effort to connect AI, IoT, and Blockchain; nevertheless, more research will be needed to build a digital strategy that might effectively combine the three for a reliable and useful digital component. Unlike any previous period in history, cloud computing is incredibly important today and enables online connections. The

massive amount of data handled by this computing system emphasizes the necessity for automated systems with (QoS) standards. Identification of essential technologies is necessary to meet this demand, and it currently looks that Blockchain, AI, and IoT are these convergent technologies.

ACKNOWLEDGMENT

Authors acknowledge the support from REVA University for the facilities provided to carry out the research.

REFERENCES

[1] Schwab, Klaus. The fourth industrial revolution. Currency, 2017.

[2] Akhtar, Muhammad Waseem, et al. "The shift to 6G communications: vision and requirements." Human-centric Computing and Information Sciences 10 (2020): 1-27.

[3] Nguyen, Quoc Khanh, and Quang Vang Dang. "Blockchain Technology for the Advancement of the Future." 2018 4th international conference on green technology and sustainable development (GTSD). IEEE, 2018.

[4] Li, Zhi, Ali Vatankhah Barenji, and George Q. Huang. "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform." Robotics and computer-integrated manufacturing 54 (2018): 133-144.

[5] Zhu, Qingyi, et al. "Applications of distributed ledger technologies to the internet of things: A survey." ACM computing surveys (CSUR) 52.6 (2019): 1-34.

[6] Gulati, Prerna, et al. "Approaches of blockchain with ai: Challenges & future direction." Proceedings of the International Conference on Innovative Computing & Communications (ICICC). 2020.

[7] Statista, I. H. S. "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)." URL: https://www. statista. com/statistics/471264/iot-number-of-connecteddevicesworldwide/(Consulté 17/05/2020) (2018).

[8] Hugoson, Mats-Åke. "Centralized versus decentralized information systems: A historical flashback." History of Nordic Computing 2: Second IFIP WG 9.7 Conference, HiNC2, Turku, Finland, August 21-23, 2007, Revised Selected Papers 2. Springer Berlin Heidelberg, 2009.

[9] Atlam, Hany F., and Gary B. Wills. "IoT security, privacy, safety and ethics." Digital twin technologies and smart cities (2020): 123-149.

[10] Atlam, Hany F., and Gary B. Wills. "Technical aspects of blockchain and IoT." Advances in computers. Vol. 115. Elsevier, 2019. 1-39.

[11] Uddin, Md Ashraf, et al. "A survey on the adoption of blockchain in iot: Challenges and solutions." Blockchain: Research and Applications 2.2 (2021): 100006.

[12] Da Xu, Li, and Wattana Viriyasitavat. "Application of blockchain in collaborative internet-of-things services." IEEE Transactions on Computational Social Systems 6.6 (2019): 1295-1305.

[13] Xiong, Zuobin, et al. "Privacy threat and defense for federated learning with non-iid data in AIoT." IEEE Transactions on Industrial Informatics 18.2 (2021): 1310-1321.

[14] Chen, Yinong. "IoT, cloud, big data and AI in interdisciplinary domains." Simulation Modelling Practice and Theory 102 (2020): 102070.

[15] Nawaz, Anum, et al. "Edge AI and blockchain for privacy-critical and data-sensitive applications." 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU). IEEE, 2019.

[16] Bertino, Elisa, Ahish Kundu, and Zehra Sura. "Data transparency with blockchain and AI ethics." Journal of Data and Information Quality (JDIQ) 11.4 (2019): 1-8.

[17] Zhang, Guozhen, et al. "Blockchain-based data sharing system for ai-powered network operations." Journal of Communications and Information Networks 3 (2018): 1-8.

[18] Parker, Brian, and Christian Bach. "The synthesis of blockchain, artificial intelligence and internet of things." European Journal of Engineering and Technology Research 5.5 (2020): 588-593.

[19] Lai, Ying-Hsun, et al. "Cognitive optimal-setting control of AIoT industrial applications with deep reinforcement learning." IEEE Transactions on Industrial Informatics 17.3 (2020): 2116-2123.

[20] Nebula Ai (NBAI) Decentralized ai blockchain whitepaper, Nebula AI Team, Montreal, QC, Canada; 2018.

[21] Dinh TN, Thai MT. Ai and blockchain: a disruptive integration. Computer. 2018;51(9):48-53.

[22] McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." Artificial intelligence and statistics. PMLR, 2017.

[23] Falco, Gregory, Carlos Caldera, and Howard Shrobe. "IIoT cybersecurity risk modeling for SCADA systems." IEEE Internet of Things Journal 5.6 (2018): 4486-4495.

[24] Yu, Tianlong, et al. "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things." Proceedings of the 14th ACM Workshop on Hot Topics in Networks. 2015.

[25] Nawari, Nawari O., and Shriraam Ravindran. "Blockchain technology and BIM process: review and potential applications." J. Inf. Technol. Constr. 24.12 (2019): 209-238.

[26] Vocke, Christian, Carmen Constantinescu, and Daniela Popescu. "Application potentials of artificial intelligence for the design of innovation processes." Procedia CIRP 84 (2019): 810-813.

[27] Jesus, Emanuel Ferreira, et al. "A survey of how to use blockchain to secure internet of things and the stalker attack." Security and communication networks 2018 (2018).

[28] Figueroa, Santiago, Javier Añorga, and Saioa Arrizabalaga. "An attribute-based access control model in RFID systems based on blockchain decentralized applications for healthcare environments." Computers 8.3 (2019): 57.

[29] Dinh, Thang N., and My T. Thai. "AI and blockchain: A disruptive integration." Computer 51.9 (2018): 48-53.

[30] Lv, Chen, et al. "Hybrid-learning-based classification and quantitative inference of driver braking intensity of an electrified vehicle." IEEE Transactions on vehicular technology 67.7 (2018): 5718-5729.

[31] Panarello, Alfonso, et al. "Blockchain and iot integration: A systematic survey." Sensors 18.8 (2018): 2575.

[32] Miraz, Mahdi H., and Maaruf Ali. "Blockchain enabled enhanced IoT ecosystem security." Emerging Technologies in Computing: First International Conference, iCETiC 2018, London, UK, August 23–24, 2018, Proceedings 1. Springer International Publishing, 2018.

[33] Sharma, Pradip Kumar, Mu-Yen Chen, and Jong Hyuk Park. "A software defined fog node based distributed blockchain cloud architecture for IoT." Ieee Access 6 (2017): 115-124.

[34] Zhang, Yu, and Jiangtao Wen. "The IoT electric business model: Using blockchain technology for the internet of things." Peer-to-Peer Networking and Applications 10 (2017): 983-994.

[35] Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." IEEE internet of things journal 5.2 (2018): 1184-1195.

[36] Ozyilmaz, Kazim Rifat, and Arda Yurdakul. "Designing a Blockchain-based IoT with Ethereum, swarm, and LoRa: the software solution to create high availability with minimal security risks." IEEE Consumer Electronics Magazine 8.2 (2019): 28-34.

[37] Wu, Chung Kit, et al. "The IDex case study on the safety measures of AIoT-based railway infrastructures." 2020 IEEE International Symposium on Product Compliance Engineering-Asia (ISPCE-CN). IEEE, 2020.

[38] Xiong, Zuobin, et al. "Privacy threat and defense for federated learning with non-iid data in AIoT." IEEE Transactions on Industrial Informatics 18.2 (2021): 1310-1321.

[39] Lai, Ying-Hsun, et al. "Cognitive optimal-setting control of AIoT industrial applications with deep reinforcement learning." IEEE Transactions on Industrial Informatics 17.3 (2020): 2116-2123.

[40] Rathore, Shailendra, Pradip Kumar Sharma, and Jong Hyuk Park. "XSSClassifier: an efficient XSS attack detection approach based on machine learning classifier on SNSs." Journal of Information Processing Systems 13.4 (2017): 1014-1028.

[41] Jeong, Young-Sik, and Jong Hyuk Park. "IoT and smart city technology: challenges, opportunities, and solutions." Journal of Information Processing Systems 15.2 (2019): 233-238.

[42] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." International journal of web and grid services 14.4 (2018): 352-375.

[43] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[44] Li, Daming, et al. "Blockchain as a service models in the Internet of Things management: Systematic review." Transactions on Emerging Telecommunications Technologies 33.4 (2022): e4139.

[45] McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." Artificial intelligence and statistics. PMLR, 2017.

[46] Tanwar, Sudeep, et al. "Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward." IEEE Access 8 (2019): 474-488.

[47] Tyagi, Amit Kumar, Gillala Rekha, and N. Sreenath. "Beyond the hype: Internet of things concepts, security and privacy concerns." Advances in Decision Sciences, Image Processing, Security and Computer Vision: International Conference on Emerging Trends in Engineering (ICETE), Vol. 1. Springer International Publishing, 2020.

[48] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." 2015 ieee world congress on services. IEEE, 2015.

[49] Abdullah, T. A., et al. "A review of cyber security challenges attacks and solutions for Internet of Things based smart home." Int. J. Comput. Sci. Netw. Secur 19.9 (2019): 139.

[50] Varga, Pal, et al. "Security threats and issues in automation IoT." 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). IEEE, 2017.

[51] Falco, Gregory, et al. "A master attack methodology for an AI-based automated attack planner for smart cities." IEEE Access 6 (2018): 48360-48373.

[52] Zou, Zhuo, et al. "Edge and fog computing enabled AI for IoT-an overview." 2019 IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS). IEEE, 2019.

[53] Jing, Qi, et al. "Security of the Internet of Things: perspectives and challenges." Wireless Networks 20 (2014): 2481-2501.

[54] Ngu, Anne H., et al. "IoT middleware: A survey on issues and enabling technologies." IEEE Internet of Things Journal 4.1 (2016): 1-20.

[55] Mosenia, Arsalan, and Niraj K. Jha. "A comprehensive study of security of internet-of-things." IEEE Transactions on emerging topics in computing 5.4 (2016): 586-602.

[56] Lin, Jie, et al. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE internet of things journal 4.5 (2017): 1125-1142.

[57] Yang, Yuchen, et al. "A survey on security and privacy issues in Internet-of-Things." IEEE Internet of things Journal 4.5 (2017): 1250-1258.

[58] Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." Journal of Network and Computer Applications 88 (2017): 10-28.

[59] Grammatikis, Panagiotis I. Radoglou, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios. "Securing the Internet of Things: Challenges, threats and solutions." Internet of Things 5 (2019): 41-70.

[60] Das, Ashok Kumar, Sherali Zeadally, and Debiao He. "Taxonomy and analysis of security protocols for Internet of Things." Future Generation Computer Systems 89 (2018): 110-125.

[61] Di Martino, Beniamino, et al. "Internet of things reference architectures, security and interoperability: A survey." Internet of Things 1 (2018): 99-112.

[62] Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

[63] Mohanta, Bhabendu Kumar, et al. "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology." Internet of Things 11 (2020): 100227.

[64] Guergov, Sasho, and Neyara Radwan. "Blockchain Convergence: Analysis of Issues Affecting IoT, AI and Blockchain." International Journal of Computations, Information and Manufacturing (IJCIM) 1.1 (2021).

[65] Attkan, Ankit, and Virender Ranga. "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security." Complex & Intelligent Systems 8.4 (2022): 3559-3591.

[66] Gai, Keke, et al. "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks." IEEE Internet of Things Journal 6.5 (2019): 7992-8004.

[67] Medhane, Darshan Vishwasrao, et al. "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach." IEEE Internet of Things Journal 7.7 (2020): 6143-6149.

[68] Gu, Ke, Lihao Yang, and Bo Yin. "Location data record privacy protection based on differential privacy mechanism." Information Technology and Control 47.4 (2018): 639-654.

[69] Yin, Chunyong, et al. "Location recommendation privacy protection method based on location sensitivity division." EURASIP Journal on Wireless Communications and Networking 2019.1 (2019): 1-13.

[70] Yin, Chunyong, et al. "Local privacy protection classification based on human-centric computing." Human-centric Computing and Information Sciences 9 (2019): 1-14.

[71] Mohanta, Bhabendu Kumar, et al. "Blockchain technology: A survey on applications and security privacy challenges." Internet of Things 8 (2019): 100107.

[72] Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo. "A blockchain future for internet of things security: a position paper." Digital Communications and Networks 4.3 (2018): 149-160.

[73] Satapathy, Utkalika, et al. "A secure framework for communication in internet of things application using hyperledger based blockchain." 2019 10th international conference on computing, communication and networking technologies (ICCCNT). IEEE, 2019.

[74] Fernández-Caramés, Tiago M., and Paula Fraga-Lamas. "A Review on the Use of Blockchain for the Internet of Things." Ieee Access 6 (2018): 32979-33001.

[75] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future generation computer systems 82 (2018): 395-411.

[76] I. Kotenko , I. Saenko , A. Branitskiy , Framework for mobile internet of things security monitoring based on big data processing and machine learning, IEEE Access 6 (2018) 72714–72723 .

[77] Hossain, Eklas, et al. "Application of big data and machine learning in smart grid, and associated security concerns: A review." Ieee Access 7 (2019): 13960-13988.

[78] N. Chaabouni , M. Mosbah , A. Zemmari , C. Sauvignac , P. Faruki , Network intrusion detection for IoT security based on learning techniques, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2671–2701 .

[79] Rathore, Shailendra, Pradip Kumar Sharma, and Jong Hyuk Park. "XSSClassifier: an efficient XSS attack detection approach based on machine learning classifier on SNSs." Journal of Information Processing Systems 13.4 (2017): 1014-1028.

[80] Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo. "A blockchain future for internet of things security: a position paper." Digital Communications and Networks 4.3 (2018): 149-160.

[81] Banerjee, M.; Lee, J.; Choo, K.-K.R. A blockchain future for internet of things security: A position paper. Digit. Commun. Netw. 2018, 4, 149–160.

[82] Parker, Brian, and Christian Bach. "The synthesis of blockchain, artificial intelligence and internet of things." European Journal of Engineering and Technology Research 5.5 (2020): 588-593.

[83] Sandner, Philipp, Jonas Gross, and Robert Richter. "Convergence of blockchain, IoT, and AI." Frontiers in Blockchain 3 (2020): 522600.

[84] Singh, Sushil Kumar, Shailendra Rathore, and Jong Hyuk Park. "Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence." Future Generation Computer Systems 110 (2020): 721-743.

[85] Uddin, Md Ashraf, et al. "A survey on the adoption of blockchain in iot: Challenges and solutions." Blockchain: Research and Applications 2.2 (2021): 100006.

[86] Alrubei, Subhi M., Edward Ball, and Jonathan M. Rigelsford. "A secure blockchain platform for supporting AI-enabled IoT applications at the Edge layer." IEEE Access 10 (2022): 18583-18595.