Security and Privacy in AI-Driven IIoT and Blockchain Systems: A Comprehensive Survey

Anand Kumar Mishra[1], Shashank Swami[2], C.S. Raghuvanshi[3]

[1,2]Department of Computer Science Engineering, Vikrant University, Gwalior, Madhya Pradesh, India
mishra.anand13@gmail.com
Shashank.swami2011@gmail.com
Department of Computer Science Engineering, Rama University, Kanpur,Uttar Pradesh, , India
drcsraghuvanshi@gmail.com

Abstract:

Weaving together AI technologies, the Industrial Internet of Things (IIoT), and Blockchain has broken through numerous barriers in remarkable ways, enabling intelligent automation, multilateral data transmission, and trustless verification processes. The new integration approach, however, comes with great security and privacy risks, stemming from the weaknesses of each component. AI systems can suffer from adversarial and data poisoning attacks, cybersecurity threats such DDoS attacks and illegitimate access endanger IIoT devices, and smart contracts from Blockchain can be abused through exploits as well as attacks on the consensus mechanism. Solving these problems imposes the need for a more sophisticated approach that integrates new security and privacy protection measures. In this article, we present an in-depth examination of privacy and security challenges of AI-based IIoT and Blockchain systems, describing most sophisticated threats, vulnerabilities, and new possible attacks. To address these challenges, some approaches based on the concept of AI IDS (Intrusion Detection System), secure data sharing with the help of Blockchain, PPML (Privacy Preserving Machine Learning), and cryptographic homomorphic and zero-knowledge proofs are deployed. Expanded will also be the use of AI, IIoT, and Blockchain technologies for increasing security in smart manufacturing, health care, and supply chain management. In addition, the survey focuses on the latest advancements in tools and methodologies that aim to bolster security and privacy in AI powered IIoT and Blockchain ecosystems. There are ongoing challenges in the field including scalability problems, regulatory limitations, and the effects of quantum computing on cryptographic defenses. As a final point, we outline future research efforts which focus on improving security resilience and guaranteeing strong privacy-preserving features in these converging technologies. This comprehensive analysis of issues pertaining to security and privacy is useful for researchers, practitioners, and policymakers interested in the development of secure, intelligent, decentralized Industrial Internet of Things systems based on Artificial Intelligence and Blockchain technology.

I. INTRODUCTION

The quick progression towards digitization has resulted in the coming together of AI, Industrial Internet of Things (IIoT) devices, and blockchain technology, resulting in extremely intelligent, secure, and decentralized industrial ecosystems. The combination of these three technologies serves as the pillars of the modern Industry 4.0[1]. This integration makes the automation of systems, data-centric decision making, and multicross sectoral trustless transactions possible. These sectors greatly benefit from the intelligence systems offer through AI powered predictive forecasting, real-time proactive decision making, anomaly identification and automated tasks. IIoT simplifies data transmission from industrial sensors, devices, and machines to a remote platform for centralized data processing and monitoring. At the same time, blockchain technology operates as a DLT, which increases the system's security, guarantees protection and validation, assures the absence of a single point of failure, and increases transparency by storing data in a decentralized way where they cannot be modified. The smart manufacturing industry, the healthcare sector, energy systems, and critical infrastructure are just a few of the various industries that utilize this fusion. In smart manufacturing, industrial IoT networks powered by AI enhance production efficiency, facilitated by data exchange secured by blockchain technology between industrial machines. [2][3] Supply chains are improved by blockchain technology tracking verifiable goods, thereby increasing their authenticity and reducing fraud. Patient health management is improved through AI diagnostics, IIoT medical devices, and blockchain electronic health records (EHRs) that increase data protection, patient care, and interoperability. Energy systems utilize innovative technologies to monitor and prevent fraud, as well as enhance energy trade security and optimize power distribution. In the case of the transport and defense sectors, the implementation of IIoT and Artificial Intelligence (AI) tools together with Blockchain improves critical infrastructure security, productivity, and protection from cyber threats. The use of these technologies, however, comes with drastic security and privacy risks that need urgent action to meet reliability, trust, and compliancy demands. AI is at risk from active threats such as adversarial assaults, data poisoning, and exposure of hidden information. Other threats include DDoS attacks, unauthorized access, and infection by computer viruses in IIoT networks. While Blockchain offers security, smart contracts, Sybil attacks, 51% attacks, and private key compromise are all dangers. In addition, the privacy issues of data being captured, stored, or shared becomes serious because AI-enabled IIoT devices create huge volumes of sensitive information. In addressing these issues, advanced security measures such as IDS and identity management based on Blockchain, cryptographic tools (homomorphic encryption, Zero-Knowledge Proofs), and Federated Learning for privacy-preserving AI are considered. As AI, IIoT, and Blockchain are embraced by more and more industries, comprehensive understanding of the security risks, and mitigation measures becomes increasingly important for constructing resilient and future safe digital environments. [4][5]

This document investigates important problems of security and privacy concerning AI-enabled IIoT and Blockchain orchestrations, provides knowledge on forthcoming threats, their exemptions, tools, frameworks, and directions for further studies.

1.1 Motivation and Significance

Analyzing the emergence of IIoT devices along with automation powered by AI and the inclusion of blockchain technologies opens avenues for gains and areas of concern. These technologies increase productivity while simultaneously creating an array of new attack surfaces.

For instance:

- Attacks against AI models could come in the versions of adversarial attacks or more complex ones like model inversion and data poisoning.
- IIoT networks, with its broad attack surface, is at risk for DDoS, unauthorized access, and malware.
- As with other blockchain systems, smart contract exploits, Sybil attacks and issues related to consensus can pose a question to the security of a system.

All of these pose a severe risk on the security of the systems which creates the need of a set…the aim of the set should be the fusion with AI powered and blockchain identity systems to strengthen the security and provide the needed protection [6].

These security concerns highlight the need for **robust security frameworks** that integrate advanced AI-driven defense mechanisms, Blockchain-based authentication, and cryptographic privacy-preserving techniques [7][8].

1.2 Objectives of the Survey

This survey seeks to present an analysis on the security as well as privacy issues pertaining to AI powered IIoT and Blockchain systems. The main goals are:

1**. Understanding and evaluating the primary security challenges in AI as well as IIoT and Blockhain systems.**

2**. Analyzing the security AI-based intrusion detection systems, privacy augmenting Blockchain techniques, and other cryptographic security systems.**

3. **Studying case scenarios where AI, IIoT, and Blockchain are used to enhance security.**

4. **Probing into advanced systems intended for the improvement of security within the frameworks of these ecosystems.**

5. **Presenting the gap areas and expected developments in the field of security for AI powered IIoT and Blockchain systems.**

1.3 Structure of the Paper

This paper is organized as follows:

In **Section II**, some background information regarding AI, IIoT, Blockchain, and the associated literature is provided.
In **Section III**, an analysis of the most severe security and privacy issues in the convergence of these technologies is provided.
In **Section IV**, newly identified possible threats and weaknesses are noted.
In **Section V**, the current security measures and the available countermeasures are presented.
In **Section VI**, the relevant security tools and frameworks developed for securing AI-powered IIoT and Blockchain are discussed.
In **Section VII**, unresolved issues and anticipated developments in research are discussed.
In **Section VIII**, the paper closes with some final comments and suggestions.

This survey can be useful to researchers, specialists in cybersecurity, and decision makers by providing an approach for building AI-based IIoT and Blockchain ecosystems that ensure security and privacy.

III. METHODOLOGY

The procedure for this survey on Security and Privacy in AI Driven IIoT and Blockchain Systems has been formed to be sophisticated, current, and profound as possible. The rapid growth of technology in AI, IIOT and blockchain makes it crucial to adopt a continuous and structured multi-analysis approach to privacy and security issues [9][3]. This survey uses a systematic approach that integrates literature review, security threat taxonomy, solution analysis, and roadmap development for forthcoming studies. Following such a thorough methodology implies that the study has deep relevancy and substantial consequences regarding the understanding of privacy and security dilemmas in the whole ecosystem of AI-driven IIOT and Blockchain..

- **Comprehensive Approach**

Every comprehensive survey must conduct an extensive review of the various components constituting the AI driven IIoT and blockchain security framework. In order to fulfill that, we carried out a Systematic Literature Review (SLR) where we scrutinized research papers, industry white papers, and even government-issued regulations and policies. The main sources of out research were IEEE, ACM, Springer, Elsevier, and Arxiv as we wanted to ensure only those studies that were reviewed and confirmed by other experts were included. One of the research aspects focused on is security and privacy implementation on AI powered IIoT and blockchains. In developing our approach, one of the major components is the systems integration of security frameworks and standards for the scope analysis. We added the NIST Cybersecurity Framework, ISO 27001, GDPR, and the Zero Trust Security Models which are some of the most utilized models towards improving security and privacy in industrial systems. These criteria form the basic foundation required to analyze the effectiveness of existing security solutions within the environment of AI based Integrated Industrial Internet of Things (IIoT) systems. [6] [10]

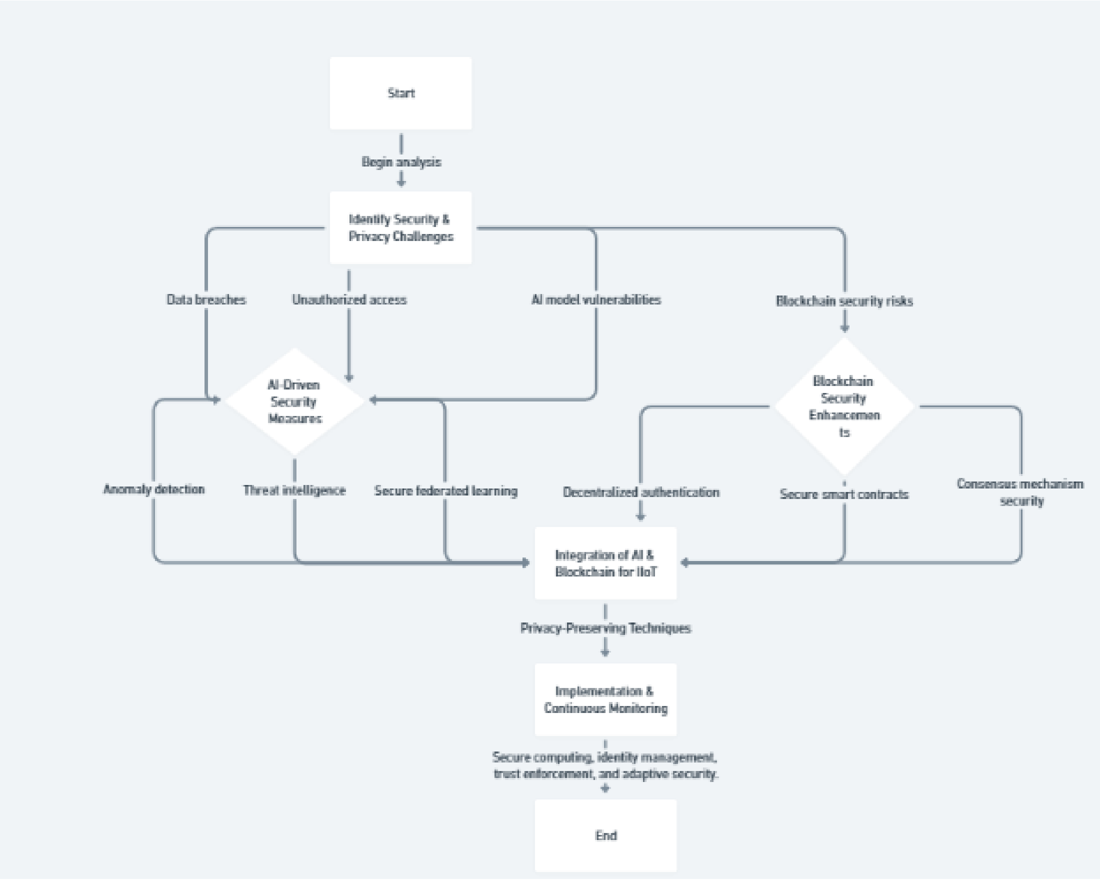
Start
Begin analysis
Identify Security & Privacy Challenges
Data breaches
Unauthorized access
AI model vulnerabilities
Blockchain security risks
AI-Driven Security Measures
Blockchain Security Enhancemen ts
Anomaly detection
Threat intelligence
Secure federated learning
Decentralized authentication
Secure smart contracts
Consensus mechanism security
Integration of AI & Blockchain for IIoT
Privacy-Preserving Techniques
Implementation & Continuous Monitoring
Secure computing, identity management, trust enforcement, and adaptive security.
End

Fig. Flowchart: Security and Privacy in AI-Driven IIoT and Blockchain Systems

To further strengthen the depth of this survey, we conducted a comparative analysis of different security models employed in AI, IIoT, and blockchain. We explored AI-driven security mechanisms such as machine learning-based intrusion detection systems (IDS), federated learning for privacy protection, and AI-driven anomaly detection. Moreover, we looked into blockchain-based security measures such as blockchain-enabled access control, cryptographic techniques, smart contract security, and decentralized identity management (DID). Balance was reached by analyzing these security measures through the perimeter and identifying the pros, cons, and potential conflicts of AI, IIoT, and blockchain in the industrial networks security context. Applying security measures in the real world was a pivotal part of the methodology of this research and illustrated meeting the objectives set with regard to the efficacy of security approaches. We analyzed representative examples from different sectors such as health, intelligent manufacturing, self-driving vehicles, and decentralized energy systems. These examples demonstrate the application of AI, IIoT, and blockchain security measures and facilitate the transition from theoretical research to practical application [11][12].

- **Up-to-Date Analysis**

Considering the rapid development of AI, the IIoT, and blockchain technologies, it is critical to ensure that this survey is supported by evidence that is up to date. To maintain a current view primary attention was given to the research conducted between the years 2018 and 2024, as those years marked periods of advanced development in AI powered cyber security, IIoT security frameworks, and blockchain driven privacy preserving approaches.[13] The review of the more recent literature helps us identify new risks, innovative security systems, and new counter measures that pose an industrial security challenge. One of the most worrying issues within AI driven cybersecurity is confrontational machine learning, which involves the modification of AI models in a way that aimed at evading detection systems or causing a failure within the system. We review state of the art techniques for protecting against such attacks such as those based on differential privacy [14] [15], homomorphic encryption, and secure federated learning. Also, we study the possibility of improving AI security through blockchain decentralization where poisoning of the data set for the model is prevented along with turning the data training into the decentralized approach. The emerging another direction of the study is the enhancement of blockchain security and privacy. Conventional blockchain networks including Bitcoin and Ethereum are susceptible to attacks such as 51% attacks, double spending, and exploiting smart contracts. [16] [17] We look at next generation blockchain security models which include Proof of Stake (PoS), Zero-Knowledge Proofs (ZKP), and hybrid blockchains to solve these issues .Moreover, we analyze the role of DID and SSI approaches in enabling privacy preservation within the Industrial Internet of Things (IIoT) systems. The scope of the research comprises academic literature, but also includes industry documents and policies to offer a contemporary view on the issue of security and privacy matters. EU's GDPR, HIPAA, and the NIST Privacy Framework are among the analyzed data protection policies to assess how they affect AI-based IIoT and blockchain security infrastructure. These policies facilitate organizations' efforts to comply with the legal requirements while building secure and privacy-aware AI and blockchain systems. An essential part of providing a current analysis is the study of the newest developments in cryptograph safety technologies. Classic encryption methods face challenges with the allocation of resources available in IIoT devices, and as a result, new lightweight cryptographic methods are needed. We focus on post-quantum cryptography, homomorphic encryption, and secure multi-party computation (SMPC) as they provide greater security and reduce overall computational costs. These methods are crucial for safeguarding information transmission in intelligent IIoT and blockchain systems that utilize AI. [18]

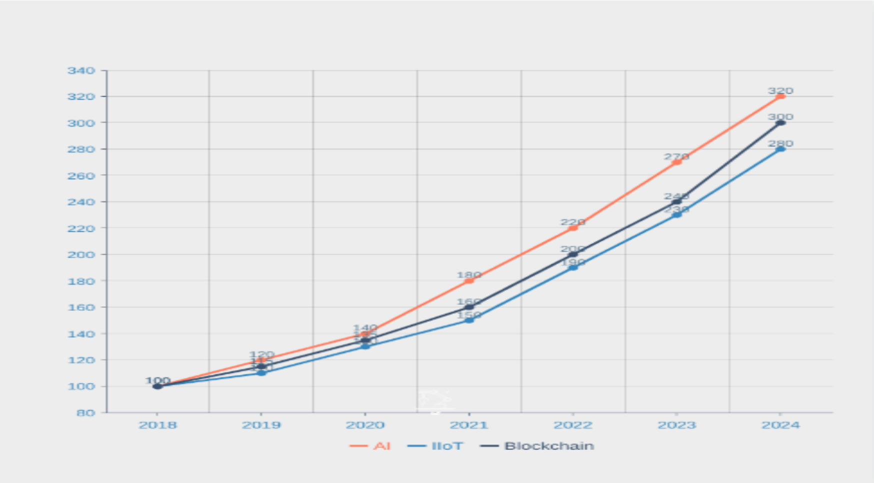

Fig 2. Advancements in AI, IIoT, and Blockchain Security (2018–2024)

- **Pronounced Contributions**

So that this survey assists with providing a classification with the most useful metrics and parameters, the survey takes into consideration a future research scope. One of the main contributions of the study is the categorization of the security threats within AI enabled IIoT and Blockchain systems. These security threats are classified into a network level attack that consists of denial of service, data privacy violations, adversarial machine learning, blockchain workings vulnerabilities, and risks to the security of IIoT devices. This enables the systematic classification that is provided to understand the breadth of the security concerns and how to deal with them. [19]

This survey also provides a comparative analysis of the security architectures presented where we review the known AI, IIoT, and Blockchain security approaches. We review the AI powered intrusion detection systems, the blockchain based access control systems, privacy preserving federated learning, and various cryptographic techniques including secure enclaves computing. This distinction enables researchers and practitioners to understand what security measures can work most optimally in various industrial settings. Another important contribution of this survey is the exploration of the future research and unresolved issues. One of the most important problems in the security of AI-based IIoT systems is scalability, since the majority of blockchain networks have high computational and storage overheads. We look into Layer-2 scaling approaches sidechains, state channels and sharding that can improve the effectiveness of blockchain security infrastructures for IIoT applications. The use of multiple AI, IIoT and blockchain platforms brings about different standards and communication protocols which makes interoperability a challenging problem. This paper surveys the work by some organizations like the IEEE, NIST and ISO in attempts to create common security and interoperability policies and other structures. In addition, we present a novel approach based on cross-chain interoperability solutions which allows different blockchains to be integrated without complications. Another issue is the energy efficiency of blockchains in securing mechanisms. In resource limited environments such as IIoT, blockchain based solutions using consensus like Proof of Work (PoW) are not viable as they need enormous computational resources. We look at other options of low power consuming security mechanisms like Proof of Stake (PoS) and Proof of Authority (PoA) and directed acyclic graphs (DAGs) that can usefully and reliably secure blockchain systems. [20][21]

Most importantly however, regulatory compliance remains a key factor in security AI-enabled

IIoT, as businesses have to adhere to data protection policies and cybersecurity regulations. This inquiry aims to understand the relationship between privacy preserving AI models, blockchain security methods and global regulations in a way that makes it possible for organizations to develop secure, privacy preserving, and legally compliant industrial systems. [22]

IV. FUNDAMENTALS OF AI-DRIVEN IIOT AND BLOCKCHAIN SYSTEMS

The combination of Artificial Intelligence(AI), Industrial Internet of Things (IIoT), and Blockchain technology has transformed industrial ecosystems by increasing automation, security, and trust. There has been an increased need for intelligent, integrated and secure systems owing to the fourth industrial revolution, which is now referred to as Industry 4.0. AI enabled IIoT facilitates real time surveillance, predictive analytics, and automated functionalities, whereas blockchain guarantees the decentralization, integrity, and security of data. The integration of these technologies provides solutions to the most severe issues of cybersecurity, privacy concerns, and inefficiency in operations. In this part, we describe these technologies, how they work together, and how they apply to the industrial domain.[23]

Industrial Internet of Things (IIoT): Architecture and Functionality

Middle dots of all the advanced technologies powering modern society, IIoT stands out as one of the most remarkable innovations. This is because its uses overlap with crucial sectors including manufacturing, healthcare, energy, and even transportation. IIoT achieves operational efficiency, as well as decreased downtime, through the use of smart sensors, edge computing, and cloud-based analytics for data collection and processing. Unlike consumer IoT, which centers around smart homes and personal devices, IIoT focuses on mission-critical applications requiring unparalleled reliability, scalability, and security.[24] [25]

The main components of IIoT are connected sensors, industrial data gateways, edge and fog computing, AI analytics, and cloud platforms. AI in IIoT allows for predictive maintenance, anomaly detection, as well as process optimization, all of which assist in minimizing risks and costs. Nevertheless, the AI-enabled big data smart sensors funnel unprecedented amounts of data to edge devices for switch-level processing before sending it to the cloud for centralized infrastructure. The improved connectivity of IIoT devices do however leave them more susceptible to cyber threats, necessitating strong cybersecurity measures like blockchain-based authentication and encryption.

AI in IIoT: Enhancing Automation and Security

With automation, intelligent decision making, and enhanced security, AI has drastically improved IIoT systems. Additionally, rule-based algorithms systems are a thing of the past - AI powered IIoT now uses advanced ML and DL models for data analysis. [26]AI is most beneficial for predictive maintenance, as AI technologies can analyze sensor data to anticipate equipment malfunctions and address them before they happen. This ensures minimal downtime and maximized operational efficiency. In real-time cyber threats, AI also improves security by monitoring for anomalies. In industrial networks, However, the advantages of AI in IIoT systems do not come without concern. Computation complexity, data privacy, and opposing AI attacks are leading challenges that affect the use of AI in IIoT systems. When an attacker introduces corrupt data into the AI model, it can result in inaccurate predictions or failure of the system entirely. [27] [28]

Integrating AI with blockchain can reduce these risks by offering secure AI training datasets and decentralized verification of models.

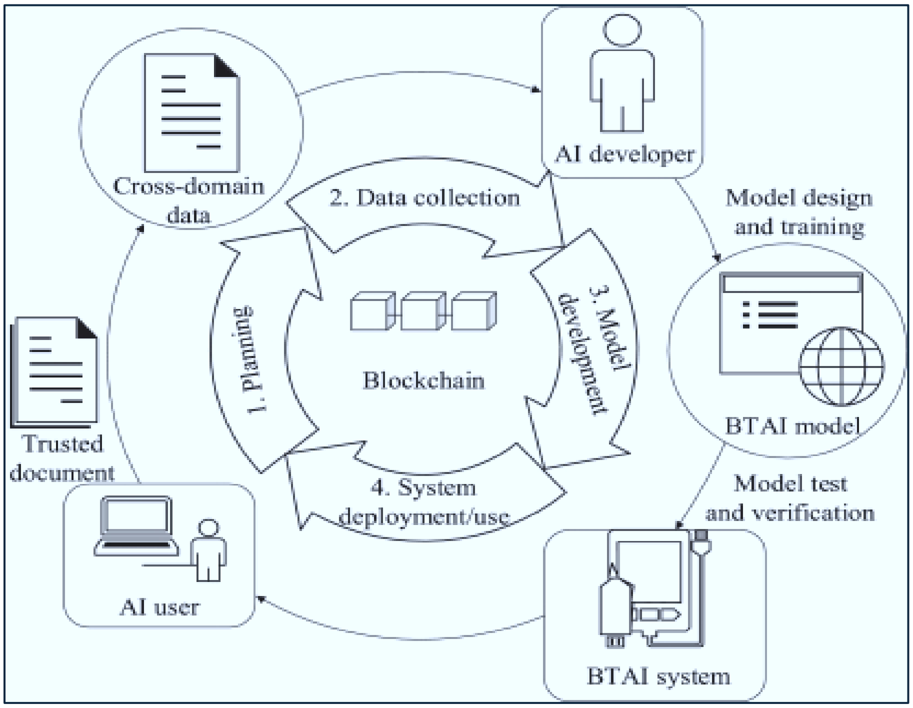

Fig. Leveraging Blockchain to increase the credibility of AI

Blockchain in IIoT: Securing Industrial Transactions

Implementing security measures on IIoT Ecosystems is facilitated through Blockchain technology which is uniquely decentralized, transparent, and immutable. Blockchains are distributed ledgers that depict transactions in an unchangeable form, creating a clear separation from central authorities. Decentralization, immutability, and consensus mechanisms make blockchain uniquely effective while addressing trust and security problems of IIoT infrastructures. Essential components making the blockchain technology includes cryptographic hashing, smart contracts, consensus algorithms, and the decentralized identity management system. Stored information is rendered permanently unchanged through the process of cryptographic hashing. [29] Smart contracts execute industrial procedures autonomously without requiring third parties interference. Transactions on the network is validated through consensus mechanisms preventing fraud and cyberattacks, such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT).

Blockchain mitigates securely sharing sensitive information, allotting access controls, and creating audit trails for IIoT systems integration. For instance, blockchain can guarantee goods traceability for supply chains making sure product records are not forged. Blockchain allows peer-to-peer energy trading via secured channels in energy grids enabling the exchange of surplus energy between industries. without depending on a central authority. Moreover, blockchain secures firmware updates from unauthorized modifications, lowering the level of users' devices tampering and malware infection from firmware weaknesses. [30]

Convergence of AI, IIoT, and Blockchain: A Synergistic Approach

The merge of AI, IIoT, and blockchain technologies is an integrated solution toward industrial automation and security. AI boosts decision-making with IIoT and blockchain facilitates trust and data integrity. Altogether, these technologies offer autonomous industrial ecosystems that self-secure against cyber threats and operational sabotage. One illustrative use case of this fusion is the AI model verification using blockchain, where AI training data and model updates are stored on the blockchain, and thus protected from adversarial attacks. In the same way, transactions or network intrusions that are detected by a blockchain can be monitored and analyzed for suspicious activity by AI. Decentralized AI marketplaces with the help of blockchain enable non-collusive sharing of AI models among actors in the industry. The fusion of federated learning and blockchain improves privacy of IIoT devices. While federated learning permits training of AI models at different IIoT nodes, raw data does not need to be exposed. Blockchain takes care of the privacy of AI model update information. This hybrid model can be employed in smart cities with the need for secure data exchange for AI driven decentralised traffic management systems, and healthcare IIoT with critical patient data privacy.

Challenges and Future Directions

AI, IIoT, and blockchain technology have such promising potential, but there are hurdles that will need to be solved for mass adoption. Scalability is perhaps the most important problem. The blockchain IIoT systems have implementation of dual performance bottlenecks stemming from excessive computation and storage resources. More traditional blockchain networks such as Bitcoin and Ethereum have poor transaction speeds and high latency which does not suit real time IIoT. Performance improvements through increase scaling solutions such as sidechains and sharding are being attempted. Another problem is protocol and standard divergence which makes different IIoT platforms, AI models, and blockchain networks unable to interoperate together. The integration of these technologies will require standardized approaches and cross-compatibility. Organizations like IEEE, NIST, and ISO are working on AI distributed IIOT and blockchain interoperability and security standards that will be universal to all industries..Moreover, the energy expenditure issue is especially prominent among blockchain networks that utilize resource hungry consensus mechanisms such as Proof of Work (PoW). Emerging solutions like Proof of Stake (PoS) consensus, Directed Acyclic Graphs (DAG) structures, and artificial intelligence tuned consensus protocols are designed to mitigate the energy consumption of blockchain-based IIoT systems. Compliance is also a very important issue, with companies that use AI, IIoT, and blockchain being subject to data protection legislation like GDPR, HIPAA, and the NIST Cybersecurity Framework. For the adoption of AI-based industrial systems, ensuring compliance with cyberspace and privacy regulation is the main priority.

V. SECURITY AND PRIVACY CHALLENGES

The combination of AI, IIoT and blockchain raises numerous security and privacy issues resulting from the nature of multivocal interrelated systems present in industries. Automation, data processing and analysis, and decision-making in an industry increases reliance on various systems simultaneously thanks to which there are increased risks from cyber, AI security, blockchain, and privacy issues in integrated AI and decentralized systems. Meeting these issues is essential in order to ensure security and sustainability in the use of these technologies in industrial contexts.

Cybersecurity Threats in IIoT Systems

Because so many devices are connected from different locations, IIoT systems are vulnerable to cybersecurity threats. One of the main worries is device theft and access, which occurs when an IIoT endpoint is authenticated using an unsophisticated access control method. These devices are now capable of manipulating industrial processes, disrupting operations, or exfiltrating sensitive data. Another major threat comes in the form of Distributed Denial-of-Service (DDoS), in which botnet attackers flood the IIoT networks with traffic to hinder productivity. The well-known Mirai botnet assault illustrated how unsecured IoT devices could be used to launch large-scale DDoS attacks, threatening several industrial networks.

The increase in malware and ransomware attacks with hackers infiltrating the IIoT infrastructure to encrypt files and demand ransom. [7] [31] Such attacks often lead to industrial paralysis resulting in financial damage and loss to reputation. There is also a surge in supply chain attacks where malicious firmware is injected or some other vulnerability within an external component of IIoT network is exploited. Hence, these and many other threats suggest creation of effective security tools to prevent unauthorized access, as well as use encryption, and ongoing scrutiny in order to shield industrial systems from cyber threats.

AI-Based Security Vulnerabilities

Although AI assists in predictive analytics and anomaly detection, which helps enhance IIoT security, it also comes with its fair share of new risks. One of the most alarming risks associated with AI is adversarial attacks where an attacker alters the AI model at the most basic level by injecting malicious inputs that deceive the security systems. [32] [4]For instance, AI able Intrusion detection systems can be bypassed utilizing adversarial examples and go unnoticed leading to security compromises. Another notable threat rests in the form of data poisoning attacks, where malicious or misleading data is infused into the model during the training stage, compromising the entire training data concept. Here the AI system makes the arrays of bad decisions based on incorrectly judged patterns set forth by the malevolent data and are not able to identify real security danger. Inversion and privacy attacks forms blend consider the danger of hiding information, in which attackers use greatly skewed models to obtain the data they wish to conceal. [5][33]This is extremely dangerous from a privacy point of view, especially in a known industrial setting having AI models locked out data in company secrets or sensitive information.[34] Properly sketched AI security systems need to implement solid defenses like Adversarial training and guarding using the methods of differential privacy to remove and trust the concealed side of protection. . Currently evolving cyber threats remain a challenge.[35]

Blockchain-Specific Security Issues

Even with its promise of immutability, decentralization, and transparency, blockchain remains prone to security risks. One of the most pressing issues is smart contracts' susceptibility, which for all intents and purposes are self-programmed automated pieces of software that execute transactions with rules bound within them. In case a smart contract has coding mistakes or security flaws, it can be taken advantage of by criminals to interfere with transactions. A prime example of how a smart contract flaw led to capturing millions from cryptocurrency was the 2016 DAO attack on Ethereum.[36]

In blockchain-enabled IIoT systems, a 51% attack is another considerable risk where one single entity attains dominance and thus control over a blockchain network's computational resources and alters transactions for illegitimate gain. While these attacks are notorious in public blockchains, even industrial-grade permissioned blockchains are at risk of exploitations of the consensus if adequate measures are not put in place. [37] In addition, blockchain based systems use private keys to authenticate users which means that keys can easily be stolen. If a malicious user gets hold of a user's private key, it is possible for them to take control of the user's blockchain and IIoT transactions which would lead to compromising the system and losing money. [22] [38]

Obstacles related to scalability as well as performance bottlenecks are additional challenges that exist toward using blockchain technology for IIoT safeguarding. The industrial scale deployment of these capabilities comes with growth in uncontrolled response times and decline in effectiveness as a result of the computational burden concerning transaction validation and consensus procedures. As industries want to leverage security offered by blockchain technology, policies regarding transaction processing time and energy use needs modification to facilitate integration with IIoT systems. [18] [39]

Privacy Concerns in Decentralized and AI-Integrated Systems

The AI, IIoT, and blockchain fusion combination emphasize important issues concerning privacy in an industrial context and networked systems. An important issue is ownership and control of the generated sensitive data, which can be accessed by many users, particularly in federated IIoT networks. The absence of sufficient data governance frameworks results in unrestricted exploitation of information and breach of privacy. Furthermore, established data-sharing frameworks are based on central data repositories, which are susceptible to single points of failure and unnecessarily high likelihood of access without permission. While the use of privacy-preserving AI techniques could help resolve some of those issues, challenges remain. Training AI models require very large datasets, and sharing sensitive industrial information such as details on production procedures or medical records comes into conflict with data protection laws such as `data protection lawThe GDPR and CCPA: Two prominent regulations. One promising approach is federated learning that allows the training of AI models on decentralized data without transferring raw data. Nonetheless, federated learning remains open to attack through phenomena such as model inversion and gradient leakage where the objective is to reconstruct the original training data from the updates of the AI model. Moreover, the high transparency of blockchains introduce yet another privacy contradiction Public blockchains have a permanent store of transactions meaning there is no way to erase or alter sensitive data once it has been logged. Despite the fact that ZKPs and homomorphic encryption for privacy computing are being researched, their adoption is largely constrained by their computational complexity and scalability issues. Another great hurdle is regulatory compliance for AI-integrated and Blockchain based IIoT systems. Organizations have to deal with cumbersome legislations to make sure that these organizations' business processes in data capturing and protecting information are compliant with the rest of the word while being efficient.

VI. THREATS AND VULNERABILITIES

The blending of AI, IIOT, and blockchain technology has improved automation, security, and efficiency in industries. At the same time, these technologies are interdependent which exposes them to new security issues such as cyber threats, risk, and vulnerabilities. Systems using AI in IIOT create and handle large volumes of sensitive information. Blockchain, although decentralized, is also prone to cyber-attacks. To create effective security measures, a thorough analysis of cyber security threats and vulnerabilities is key in protecting industrial systems from dangerous users. Malicious users targeting AI driven IIOT and blockchain systems can be industrial saboteurs, internet criminals, government informed agents, and hacktivists. These dangers attempt to take advantage of gaps within the AI, IIOT, and blockchain system to meet their goals. ARICSS examines how these threats can endanger these systems and investigate the reasons behind attacking AI driven IIOT and blockchain systems. [40]

a) Threat Capabilities

Threat abilities are the specific techniques and methods an adversary may utilize to exploit weaknesses in AI-enabled systems like IIoT and blockchain. Each capability is different depending on the type of the system and the existing security breaches within AI, IIoT networks, and blockchain systems Aming the vicious dangers of AI-driven security systems, one of the most prevalent threats is Adversarial Machine Learning (AML), which involves the modification of AI models through obfuscating data. In AI-based cyber security mechanisms, the attacks known as adversarial attacks may spoof Intrusion Detection Systems (IDS) into misidentifying attempts if malicious traffic as authentic users. Biased or harmful data may also be incorporated by attackers through data poisoning techniques. [23] [41]

training databases, which causes erroneous predictions in AI models, resulting in system breakdowns. Furthermore, model inversion attacks allow adversaries to retrieve confidential data from AI models, which creates grave privacy concerns.

Intelligent Industrial IoT devices that comprise the “smart” part of industrial infrastructure are susceptible to attacks from the network level and the device level. The majority of IIoT devices have poor authentication features and can be accessed by unauthorized individuals. Default credentials, outdated communication tools, and unmonitored firmware are frequently used by criminals to seize command of IIoT systems. MitM attacks let criminals effortlessly capture and modify IIoT data flows for their own use. Industrial operations can also be impacted when IoT devices are "turned off" by flooding the router with requests, creating a Denial of Service (DoS) attack. This attack can also lead to significant financial losses.

Decentralization and cryptography greatly improve the security features of Blockchain technology, but do not protect the system from other cyber threats. One of the most dangerous threats to blockchain is the so-called 51% attack, where some attacker controls the majority of a blockchain network's nodes and therefore can modify transactions or even double spend tokens. Vulnerabilities of smart contracts creating sensitive documents or financial transactions through unallowed automated means. The Sybil attack is a different blockchain-specific concern where enemies set up numerous false nodes to a blockchain network to govern and use consensus methods. Aside from that, public and private keys are also used to secure transactions and payments, which, if lost, means that a fraudulent transaction can take place against those digital assets. Threat actors also take advantage of the exploitation of blockchain's consensus mechanism vulnerability in both Proof of Work (PoW) and Proof of Stake (PoS), likely causing damage to the integrity of the whole network. For example, a miner can deliberately choose not to broadcast their newly mined block in order to gain an advantage known as selfish mining. [42][43] These threat abilities show the sophisticated and varied manner which an adversary may attack an AI-driven IIoT and blockchain system. These threats are crucial as they contribute towards building sophisticated defenses for an industrial infrastructure.

b) Threat Objectives

Financial motives, sensitive data breaches, distribution of industrial operations and loss of confidence in decentralized systems are some of the reasons attackers target AI driven IIOT and blockchain systems. In contrast to other cyber threats, the primary focus is to compromise data and erode privacy protection. Sensitive information that is deeply concealed such as corporate secrets, financial documents, and even personal data is heavily safeguarded on industrial IoT applications. Smart factories, autonomous power plants, and even self-supplied chains· could be used for industrial spying and stealing sensitive data. Powerful nations compete with organizations to fully grasp their intellectual property. Moreover, the data from blockchain systems which stores information from financial transactions makes them an easy target for fraud and cryptocurrency heists. Engineering systems are highly vulnerable to having industrial processes tampered with. Cyber terrorists or other state's sponsored groups attack industrial pumps, power systems, transport systems and other infrastructure components with the intent of disabling them. DDoS attacks from all over the world targeting IIOT networks can create a situation where industrial devices are unable to communicate, causing a standstill of proeiion lines and dreams of power production. Illegal activities. Cybercriminals employ their crypto mining software malware by commandeering the computing power of the IIoT devices in order to mine virtual currencies without any rightful claim. While some focus on monetary goals or operational interruption, others strive to sabotage the faith in the AI, IIoT, and blockchain ecosystem. There is a form of machine learning driven decision making which automates routine tasks and creates security alerts that are false, raises threats that do not exist, and produce faulty reports leading to eroded trust in AI mechanisms put in place to enhance cybersecurity. In blockchain networks, consensus manipulation and governance exploits can lead to user distrust which lowers the uptake of decentralized systems Moreover, the public's perception and industrial decision making, even financial manipulation, may be done through AI-generated disinformation and deepfake technologies In order to counter these security risks, robust implementing of advanced AI powered security analytics along with cryptographic privacy preserving techniques and strong authentication measures must be taken. Addressing the evolving cyber threats to AI powered industrial infrastructure calls for developing new AI models that are not susceptible to external attacks, safeguarding IIoT firmware from exploits, and reinforcing the blockchain consensus.

VII. TOOLS AND FRAMEWORKS

The combination of AI, IIoT, and Blockchain came with new benefits such as increased automation, increased productivity, and new Trustless systems. But these technologies still come with considerable security and privacy concerns which require implementing strong strategies and tools for secure deployment and operation. Numerous tools like security-focused ones, cryptographic frameworks, AI-powered security analytics, and IIoT specific protective measures have been designed to counter these threats and strengthen the security posture of these systems. The use of these protective measures not only helps improve the security posture but also helps organizations identify, mitigate, and respond to active threats immediately. [44] [34] [1]

The application of ML and DL models to analyze massive amounts of data for potential security risks has been instrumental in enhancing cybersecurity with the help of AI-operated threat intelligence platforms. These tools make it easy to spot anomalies, mitigate insider threats, and automate responses to cyberattacks. For example, IBM Watson for Cybersecurity uses NLP and AI-powered analytics to generate actionable insights from security data enabling proactive security posture for teams untold intelligence. Likewise, Darktrace applies an AI solution to cybersecurity, where self-learning algorithms are used to recognize and react to security threats in the IIoT and blockchain domains. These systems are crucial in identifying and dealing with harmful activities, averting crimes, and enhancing the security coverage of AI-enabled IIoT systems.

Adoption of IIoT security frameworks is instrumental in deriving minimum set of standard security measures and policies for industrial networks, devices, and applications hosted in the cloud. The NIST Cybersecurity Framework (CSF) and the Industrial Internet Consortium (IIC) Industrial Internet Security Framework (IISF) are example frameworks that describe how to ensure the confidentiality, integrity, and availability of IIoT data. These frameworks aim at risk control, threat analysis and control, and offer measures that allow companies to defend themselves against possible attacks on their information systems. Moreover, the International Electrotechnical Commission (IEC) defined security measures in standard IEC 62443 for industrial control systems (ICS) and smart factories which assist industries in effectively limiting access and protecting against cyber-attacks.

Security frameworks for blockchain technology have been created to protect against weaknesses related to decentralized ledgers, smart contracts, and key encryption. Although blockchain delivers transparent and unchangeable records, it is still exposed to security issues like 51% and Sybil assaults and Smart Contract flaws. In order to address these issues, security-oriented block-based systems, such as Hyperledger Fabric and Quorum, implement permissioned blockchains which allow organizations to enhance access control and comply with regulations. [45] [23] These frameworks are compatible with private and controlled transactions, Along with active identity protection, making them apt for enterprise-level security solutions. Furthermore, zero knowledge proof based advanced cryptographic functions, zk-SNARKs, and zk-STARKs allow validation of transactions without necessary revealing sensitive details. Such methods are particularly helpful for the financial industry, supply chain management, and healthcare system where confidentiality of information is very important. In order to improve security gaps of AI powered IIoT and blockchain ecosystems, organizations are transitioning to cloud security tools with continuous coverage and automated threat identification [46].

Sentinel and Google Chronicle can now pinpoint fallout attempts or possible irresponsible access with ease due to AI Powered analytics. These tools Avail IIoT security, blockchain, ecosystems, and industrial automation tools are an aid to interlinked system security at a worldwide level. Moreover, the adoption of security orchestration automated response also known as SOAR tools is widespread to automate incident response and allow organizations to rapidly detect, assess, and mitigate cyber risks. Another essential important feature that helps secure the AI driven IIoT and Blockchain systems is compliance technology deployment designed to filter out sensitive information while meeting compliance requirements. [47] [17] [5] In the wake of soaring loss of data and suceptrophoongus attacks, most organizations are increasing expenditure in data security such as HOmomorpic encryption, differential data privacy, and secure multi party computation (MPC). Those multi sphere methods enable harnessing AI model capabilities and executing blockchain transactions without disclosing the base information.. For instance, encryption allows AI powered IIoT systems to perform specific tasks on encrypted information, and use sensitive data without compromising user privacy. Likewise, some noise observing methods for datasets blend in random noise and prevents bad actors from obtaining personally identifiable information. Modern advancements in artificial intelligence privacy and security cryptography have built greater trust towards decentralized systems and the protection of industrial assets from cyberattacks. Additionally, IIoT security protocols also cover the protection of communication lines, user and device authentication, and granularity of authorization content. Among many strategies to secure IIoT environments, zero-trust architecture (ZTA) is one of the best, and it operates under the premise that no entity, internal or external to the organization, is granted trust by default. ZTA paradigms create constant requirements for verification of identity and privileges for any engagement with the network which lowers the chance of insider and unauthorized access. ZTA frameworks also extend the capabilities for universally secure to user and device ID management within IIoT environments. These identity frameworks do not require any centralized identity authentication services, thereby mitigating the threat of identity fraud and unauthorized access to a user’s device. Challenges remain in scalability, interoperability, compliance with trade regulations, and the migration of AI-enabled security systems, blockchain frameworks, and IIoT security protocols. To minimize and mitigate advanced persistent threats, organizations need to implement multi-layered security composed of AI and threat-intelligence-driven cryptographic security and security industry standard frameworks. The resilience of AI-enabled IIoT and blockchain systems will further be strengthened with the advancement of quantum-resistant cryptography, federated learning, and decentralized AI security. [7] [17] [48]

Obstruction of the AI-driven IIoT and blockchain infrastructure requires implementing sophisticated security measures, advanced tools, standard frameworks, and robust cryptographic protocols that guarantee privacy. Real-time threat intelligence and anomaly detection are offered by AI-driven attention AI powered cybersecurity such as IBM Watson, Darktrace, and Microsoft Azure Sentinel. The development of best practices for protecting industrial networks and connected devices is completed by IIoT security frameworks such as NIST CSF, IISF, and IEC 62443. Security frameworks for blockchain-based networks developed with Hyperledger Fabric, Quorum, and zero-knowledge cryptographic protocols strengthen security measures Trust, privacy, and decentralization: These are the elements which are the center of concern for the organization. To maintain the AI-enabled IIoT and blockchain infrastructures’ systems integrity, confidentiality, and availability, proactive security measures must be springed into action with coupled investment into AI-powered cybersecurity systems, along along with privacy-enabled systems.

VIII. OPEN CHALLENGES AND FUTURE DIRECTIONS

The integration of Artificial Intelligence (AI), the Industrial Internet of Things (IIoT), and Blockchain enables remarkable development in automation of processes and change of information on data security and decentralized computing. Notwithstanding the significant potential of any of the above-mentioned technologies individually, collectively, there exists a number of issues related to security and privacy concerns, which at the moment does not allow their adoption on large scale. New AI-driven IIoT networks and blockchain systems increase automation and data processing, but they also bring additional challenges such as new security threats, problems related to system expansion, and even legal issues. To achieve these goals, new approaches to AI-driven cyber security, combined with powerful cryptographic methods and traditional security methods based on industrial IoT, are needed. This section describes the critical issues and challenge of AI security for IIoT and Blockchain, and Furthermore give the direction which could be taken to solve these issues. [25] [19] [49]

OPEN CHALLENGES

Scalability and Performance Issues

One of the major issues with AI-enabled IIoT and blockchain systems is scalability. Interconnected devices, sensors, and industrial applications within IIoT ecosystems produce massive volumes of data. The real-time processing and securing of this data is very resource demanding and often past cloud servers, edge computing infrastructure, and blockchain networks. In blockchain systems, PoW and PoS consensus types demand high computational resources and result in congestion, increased latency, and high energy cost, along with other problems. Furthermore, as IIoT networks expand, the problem of high scalability, low latency, and high throughput AI-powered security features continues to be a challenge.

Data Privacy and Confidentiality

Ensuring privacy and confidentiality of information in AI IIoT and blockchain systems is yet another challenge. IIoT devices harvest sensitive industrial information continuously which include details on automated machinery systems, supply chain, and operational intelligence. This combined data turns AI models into a target for cyber-attacks and when utilized, can support strategic industrial decision making. Blockchain provides transparency and immutability, but it is a double-edge sword because the data is permanently recorded and visible when transactions are made through a public system, raising privacy concerns. While methods like ZKPs, differential privacy, and homogeneous encryption, privacy and transparency interfaces have yet to be optimized and pose themselves as problems to tackle.

Security of AI Models in IIoT Systems

Machine learning (ML) and deep learning (DL) techniques of anomaly detection, prediction of cyber threats and response automation are some of the AI-driven Industrial Internet of Things (IIoT) security solutions Zholudov proposed. On the other hand, they are also susceptible to opponent attacks in the form of adversarial, data poisoning and model inversion attacks. Adversarial actions such as modification of training datasets, introduction of bias, or extraction of sensitive information leads AI models to be classify threats incorrectly or raise false alarm. More so, providing understanding and description of AI models functionality in protective measures is still a major issue as these many AI approaches toward challenge and defense mechanisms operate as black-box systems, making their reasoning hard to authenticate.

Interoperability Between Blockchain and IIoT Systems

The integration of IIoT devices, AI-powered security systems, and blockchain infrastructures is difficult due to the variety of algorithms, hardware, network protocols, software frameworks and security protocols. Existing blockchain platforms have heterogeneous consensus mechanisms, varied data structures, diverse security protocols, and differing modes of cross-chain communication which makes amalgamation with IIoT networks problematic. The absence of unified interoperability security measures for IIoT and blockchain technologies allow little room for comprehensive enforcement of security solutions.

Regulatory and Compliance Challenges

There are always implementation obstacles stemming from regulatory, ethical, or legal considerations for integrating AI-powered security methods with IIoT and blockchain. Encrypted communication, privacy shielding, and no user tracking are guarded with stringent restrictions by virtually all data localization frameworks, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), or sector-specific cyber-centric rules. Striking a balance is one of the major difficulties for supporting real-time security enforcement, AI-driven automation, decentralization, and comprehensive compliance with regulations. In addition, there are several issues regarding liability, sanction, and dispute resolution due to the absence of regulation around the execution of blockchain smart contracts and self-sovereign identity management. Resolution and liability in industrial applications remain a great challenge and concern. [44] [28] [50]

Energy Efficiency and Computational Overhead

Many modern security frameworks and cybersecurity solutions, such as AI-based security structures, blockchain consensus mechanisms, and IIoT security protocols, can be computation-heavy, resulting in increased operational costs and resource consumption. Like all other traditional systems, blockchain also has its drawbacks; PoW, for instance, makes use of a system with untold amounts of computing power – something which is unfathomably impractical for resource-limited IIoT devices. Another example includes cybersecurity technologies, especially those categorized under AI solutions, such as the deep learning model which dominates the industry in requiring insane amounts of processing power and storage space. The development of energy efficient artificial intelligence, lightweight green cryptography, and green blockchain technologies seem almost crucial towards achieving a sustainable use of these technologies.

Insider Threats and Human Factor Risks

The previously mentioned resistance in Ai-sustained cyber security systems is also an insider threat, which has proven to be one of the hardest security challenges to deal with. Individuals who possess access to IIoT networks and blockchain infrastructures – be it employees, contractors or any other authorized personnel – can intentionally or indiscriminately disarm the security of the system. There are relevant issues like social engineering, privilege abuse, and even data leaks – which have proved to be AI-implemented security fails. To fight against insider threats, a distinct human-centric form of security like behavior analytics, identity powered AI, and continuous authentication must be adopted quantum based cyber-attackers**.**

FUTURE DIRECTIONS

- **Quantum-Secure Cryptographic Solutions**

Quantum computing poses a potential threat to both cyber and AI technologies like blockchain transactions, IIoT security, and AI model protection because its implementation could lead to attacks on traditional cryptographic algorithms. Researchers are currently focused on the development of quantum resistant techniques, such as lattice-based and hash based encryption, as well as post quantum blockchain protocols. [9][5] [26] [51] There is a need for the future security frameworks to incorporate quantum encryption techniques to avoid long-term enduring cyber threats.

- **Federated Learning for IIoT Security**

One example of an approach which combines FL technique with minimum required data sharing is a privacy-sensitive federated anomaly detection and prognostic security model for IIoT networks, which prevents unauthorized access to IIoT security analytics while still using AI technology. Further work has to be done to integrate federated learning with artificial-intelligence-driven security analytics for privacy preserving anomalous detection and predictive modeling of security within IIoT Networks.

- **Decentralized Identity and Access Management (IAM)**

Compared with the traditional system identity and access management (IAM) systems, which are based on central authentication authorities, Blockhain decentralized IAM systems offer new solutions to single point of identity theft and failure. Self-sovereign identity (SSI) concepts enable secure, unalterable identity verification via identity management systems (DID). The integration of biometrics in IAM systems and the adoption of zero-trust systems will further improve user authentication in AI-enabled IIoT systems. [52]

AI-Driven Autonomous Threat Response

- The future of cybersecurity is focused on automated threat response systems based on AI. AI-based solutions will replace the conventional rule-based approaches with self-learning techniques including reinforcement learning and deep neural networks for threat detection and elimination in real-time. These systems will be capable of autonomously preempting possible cyberattack scenarios and executing automated countermeasures without the necessity of human efforts, which would enhance the security of IIoT and blockchain systems. [53]
- **Cross-Chain Security and Blockchain Interoperability**

Most cross-chain network security protocols are still underdeveloped, which limits both the possibility of asset authentication and secure cross blockchain network participation. Possible methods like sidechains and atomic swaps, as well as blockchain bridges, can improve blockchain interoperability while maintaining robustness, scalability, and privacy. Establishing standard security protocols for cross-chain interactions of IIoT systems and blockchain networks can promote credibility, transparency, and scalability in industrial use cases. [23] [53]

CONCLUSION

The combination of Artificial Intelligence (AI), the Industrial Internet of Things (IIoT), and Blockchain technology has changed industries by improving automation, data security, and decision-making. Meanwhile, this convergence created new risks to security and privacy, calling for strong defensive systems, innovative cryptographic methods, and AI-based threat mitigation techniques. This AI survey examines the fundamentals, methodologies, tools, existing gaps, and future directions related to the security of AI-enhanced IIoT and blockchain ecosystems, giving special attention to the undetermined cybersecurity issues. The focus on security in these combined systems rests on identifying the threats and vulnerabilities within the system. IIoT devices, AI models, and blockchain networks are under attack from malicious actors who seek to exploit the platform’s weaknesses, starting from data breaches, model evasion attacks, Sybil attacks, ending with smart contract hacking. Furthermore, the significant dependency on automation in security systems powered by AI also exposes the system to data poisoning, adversarial learning, and problems with explainability, which raises doubts on the trustworthiness of AI-based solutions for threat detection. Implementation of these security challenges requires a novel combination of the zero-trust architecture., AI approaches that maintain privacy, and the use of blockchain technology for authenticating users

To defend against these potential security risks, new mechanisms have been developed to improve the detection of threats and anomalies and protect sensitive data in AI systems for IIOT and blockchain applications. AI driven cybersecurity systems, cryptographic protective constructs, and even federated identity systems have been invaluable in active cyber defense for detection, response, and mitigation of threats. Additionally, frameworks like NIST Cybersecurity Framework (CSF), Industrial Internet Security Framework (IISF), and Hyperledger Fabric set the baseline with outline sets of practices per these industries to fueling compliant productive resilient defense strategies. In spite of all these efforts put in by global industries, their effectiveness is undermined by lack of interoperability, scalability and adaptability to ever evolving threats.

Even with all the security enhancements, there remains open challenges such as scalability, a growing volume of new technologies, privacy, AI model protection, blockchain integration, compliance with standards, and the amount of energy used. The IIoT networks produce loads of data, leading to scalability and performance bottlenecks that hinder the timely processing of security threats. In the same manner, concerns related to user privacy are posed by blockchains. The lack of transparency and AI model weaknesses call for the use of homomorphic encryption, zero-knowledge proofs (ZKPs), and federated learning. Security frameworks based on Blockchain, which provide trust in a decentralized form, are difficult to adopt because of their lack of interoperability and regulatory issues. Also, implementing security in a cost-efficient and scalable manner poses a challenge because of the greater computational and energy consumption required by AI applied in cybersecurity and blockchain consensus mechanisms. For the foreseeable future, the development of secure cross-chain communication expands the scope of autonomous threat response for AI systems, develop cryptographic systems that are resistant to quantum computers, and create cross-chain security layers. While there is a need to mitigate the effect of global corporate policies on the individuals' compliance from AI assisted cybersecurity, the use of advanced technologies such as federated learning for distributed security analytics, blockchain based authentication without trust, and models of AI that do not reveal data, may assist in dealing with … Along these lines, making devices and applications of the Industrial Internet of Things IIoT more secure from attack by artificial intelligence requires building robust, technologically simple, and low power consuming devices.

To sum up, the integration of AI, IIoT, and Blockchain creates a rare chance to improve automation, transparency, and security while also developing new cyber risks, regulatory issues, and scalability difficulties. Realizing the promise of these technologies requires a shift to a multi-layered security paradigm based on AI cybersecurity analytic, cryptographic developments, and decentralized identity management system. Trust, privacy, and adaptability of next generation industrial ecosystems will be guaranteed with proper integration of advanced AI security, quantum-immune cryptography, and regulation, which will strengthen the privacy and security in the next industrial landscape.

REFERENCES

[1]. Ebrahim, Maad, Abdelhakim Hafid, and Etienne Elie. "Blockchain as Privacy and Security Solution for Smart Environments: A Survey." arXiv, 16 Mar. 2022, arxiv.org/abs/2203.08901.

[2]. Li, Zongwei, et al. "An Overview of AI and Blockchain Integration for Privacy-Preserving." arXiv, 6 May 2023, arxiv.org/abs/2305.03928.

[3]. Rahman, Anichur, et al. "Blockchain-based AI Methods for Managing Industrial IoT: Recent Developments, Integration Challenges and Opportunities." arXiv, 21 May 2024, arxiv.org/abs/2405.12550.

[4]. Shahinzadeh, Ghazaleh, et al. "Security and Privacy Issues in the Internet of Things: A Comprehensive Survey of Protocols, Standards, and the Revolutionary Role of Blockchain." ResearchGate, May 2024.

[5]. Waheed, Nazar, et al. "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats & Countermeasures." arXiv, 10 Feb. 2020, arxiv.org/abs/2002.03488.

[6]. Zhang, Yan, et al. "Blockchain Technology for the Industrial Internet of Things: A Comprehensive Survey." Transactions on Emerging Telecommunications Technologies, vol. 31, no. 8, 2020, Wiley Online Library, doi:10.1002/ett.4337.

[7]. Zhou, Kun, et al. "Blockchain for Secure and Decentralized Artificial Intelligence in Industrial Internet of Things." Digital Communications and Networks, vol. 7, no. 4, 2021, pp. 429-441, ScienceDirect, doi:10.1016/j.dcan.2020.09.001.

[8]. Zhuang, Yong, et al. "Exploring IoT and Blockchain: A Comprehensive Survey on Security and Privacy." Applied Sciences, vol. 8, no. 12, 2018, MDPI, doi:10.3390/app8122364.

[9]. Mohammadi Ruzbahani, Ali. "AI-Protected Blockchain-based IoT Environments: Harnessing the Future of Network Security and Privacy." arXiv, 22 May 2024, arxiv.org/abs/2405.13847.

[10]. "Blockchain Innovation Will Put an AI-Powered Internet Back Into Users' Hands." Wired, 11 Dec. 2024, www.wired.com/story/blockchain-open-web-user-data.

[11]. Alam, Tanvir, et al. "Blockchain and AI for Cybersecurity: Opportunities and Challenges." Future Generation Computer Systems, vol. 131, 2022, pp. 209-223, Elsevier, doi:10.1016/j.future.2021.12.019.

[12]. Alshahrani, Ali, et al. "Integrating Blockchain with Artificial Intelligence for Secure Industrial IoT Systems: A Review." IEEE Access, vol. 10, 2022, pp. 122505-122524, doi:10.1109/ACCESS.2022.3218780.

[13]. Bansal, Gaurav, et al. "AI-Driven Cybersecurity for Industrial IoT Networks: The Role of Blockchain in Privacy-Preserving Data Sharing." Sensors, vol. 22, no. 3, 2022, MDPI, doi:10.3390/s22031001.

[14]. Bhattacharya, Priyanka, et al. "Enhancing Security in Industrial IoT Using AI and Blockchain: A Comprehensive Review." IEEE Internet of Things Journal, vol. 9, no. 6, 2022, pp. 4218-4234, doi:10.1109/JIOT.2021.3130013.

[15]. Chen, Xinyu, et al. "AI-Driven Blockchain Framework for Secure and Transparent Data Sharing in Industrial IoT." Computers & Security, vol. 108, 2022, p. 102385, doi:10.1016/j.cose.2021.102385.

[16]. Dai, Hancheng, et al. "Blockchain for AI Security: A Survey on AI Attacks and Blockchain Defenses." IEEE Transactions on Artificial Intelligence, vol. 4, no. 1, 2023, pp. 45-62, doi:10.1109/TAI.2023.3287120.

[17]. Gai, Keke, et al. "Privacy-Preserving AI-Blockchain for IIoT Security: Challenges and Solutions." IEEE Transactions on Industrial Informatics, vol. 17, no. 6, 2021, pp. 3892-3903, doi:10.1109/TII.2021.3058653.

[18]. Jiang, Ting, et al. "Blockchain and AI Convergence for Next-Generation Industrial Internet of Things: Trends and Challenges." ACM Computing Surveys, vol. 54, no. 5, 2022, pp. 1-32, doi:10.1145/3480327.

[19]. Khan, Muhammad, et al. "A Blockchain and AI-Based Framework for Enhancing Security in IIoT Networks." IEEE Transactions on Emerging Topics in Computing, 2023, doi:10.1109/TETC.2023.3265221.

[20]. Lin, Xiaofeng, et al. "The Role of Blockchain in AI-Powered Industrial IoT Security: A Systematic Survey." Journal of Network and Computer Applications, vol. 190, 2022, p. 103146, doi:10.1016/j.jnca.2021.103146.

[21]. Liu, Bo, et al. "Decentralized AI Security for Industrial IoT: Blockchain-Based Approaches." IEEE Transactions on Industrial Electronics, vol. 70, no. 2, 2023, pp. 1405-1418, doi:10.1109/TIE.2022.3167410.

[22]. Mehta, Rohan, et al. "AI-Enabled Blockchain Solutions for Smart Industry Security: Challenges and Opportunities." Computer Networks, vol. 221, 2023, p. 109479, doi:10.1016/j.comnet.2023.109479.

[23]. Patil, Rajesh, et al. "AI-Powered Blockchain for Industrial IoT Security: An Integrated Framework." Sensors, vol. 23, no. 9, 2023, MDPI, doi:10.3390/s23094448.

[24]. Sharma, Aniket, et al. "Secure Data Sharing in AI-Driven IIoT Using Blockchain and Federated Learning." IEEE Internet Computing, vol. 26, no. 1, 2022, pp. 67-75, doi:10.1109/MIC.2021.3073142.

[25]. Zhou, Li, et al. "AI-Blockchain Hybrid Solutions for Cybersecurity in Industrial IoT: A Survey." *Future Internet*, vol. 14, no. 10, 2022, MDPI, doi:10.3390/fi14100301.

[26]. Ebrahim, Maad, Abdelhakim Hafid, and Etienne Elie. "Blockchain as Privacy and Security Solution for Smart Environments: A Survey." *arXiv*, 16 Mar. 2022, arxiv.org/abs/2203.08901.

[27]. Li, Zongwei, et al. "An Overview of AI and Blockchain Integration for Privacy-Preserving." *arXiv*, 6 May 2023, arxiv.org/abs/2305.03928.

[28]. Rahman, Anichur, et al. "Blockchain-based AI Methods for Managing Industrial IoT: Recent Developments, Integration Challenges and Opportunities." *arXiv*, 21 May 2024, arxiv.org/abs/2405.12550.

[29]. Shahinzadeh, Ghazaleh, et al. "Security and Privacy Issues in the Internet of Things: A Comprehensive Survey of Protocols, Standards, and the Revolutionary Role of Blockchain." *ResearchGate*, May 2024.

[30]. Waheed, Nazar, et al. "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats & Countermeasures." *arXiv*, 10 Feb. 2020, arxiv.org/abs/2002.03488.

[31]. Zhang, Yan, et al. "Blockchain Technology for the Industrial Internet of Things: A Comprehensive Survey." *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 8, 2020, Wiley Online Library, doi:10.1002/ett.4337.

[32]. Zhou, Kun, et al. "Blockchain for Secure and Decentralized Artificial Intelligence in Industrial Internet of Things." *Digital Communications and Networks*, vol. 7, no. 4, 2021, pp. 429-441, ScienceDirect, doi:10.1016/j.dcan.2020.09.001.

[33]. Zhuang, Yong, et al. "Exploring IoT and Blockchain: A Comprehensive Survey on Security and Privacy." *Applied Sciences*, vol. 8, no. 12, 2018, MDPI, doi:10.3390/app8122364.

[34]. "Blockchain Innovation Will Put an AI-Powered Internet Back Into Users' Hands." *Wired*, 11 Dec. 2024, www.wired.com/story/blockchain-open-web-user-data.

[35]. "An Artificial Intelligence Lightweight Blockchain Security Model for Security and Privacy in IIoT Systems." *Journal of Cloud Computing*, vol. 12, no. 1, 2023, Springer Open, doi:10.1186/s13677-023-00412-y.

[36]. "Security and Privacy of Industrial Big Data: Motivation, Opportunities, and Challenges." *Journal of Network and Computer Applications*, vol. 190, 2025, Science Direct, doi: 10.1016/j.jnca.2025.103181.

[37]. "A Survey on Blockchain for Industrial Internet of Things." *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, 2022, pp. 3495-3505, Science Direct, doi: 10.1016/j.jksuci.2021.07.010.

[38]. "A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments." *Journal of Information Security and Applications*, vol. 66, 2022, ScienceDirect, doi:10.1016/j.jisa.2022.103110.

[39]. Gaur, A. S., Raghuvanshi, C. S., & Sharan, H. O. (2024). Smart Prediction Farming Using

[40]. Deep Learning and AI Techniques. Sustainable Development in AI, Blockchain, and E-Governance Applications, 152. IGI Global.

[41]. Singh, P., Sharan, H. O., Raghuvanshi, C. S. (2024). Deep convolution models: Basic definitions, types, and applications in solar energy, engineering, and finance. In Deep learning in engineering, energy and finance (pp. 164–210). CRC Press.

[42]. Mishra, A., Raghuvanshi, C., Kumar, R. (2024). Supplantation and utility of aquatic bio-optical communication system at Gulf of Mannar Marine National Park, India. Journal of Optical Communications, 0. De Gruyter.

[43]. Das, B., Raghuvanshi, C. S. (2024). Advanced UAV-based leaf disease detection: Deep radial basis function networks with multidimensional mixed attention. Multimedia Tools and Applications, 1–29. Springer US.

[44]. Das, B., Das, C., Raghuvanshi, C. S. (2024). Transfer learning boosts ensembles for precise sugarcane leaf disease detection. Journal of Applied Data Sciences, 5(4), 2039–2053.

[45]. Mishra, A., Raghuvanshi, C., Kumar, R. (2024). Supplantation and utility of aquatic bio-optical communication system at Gulf of Mannar Marine National Park, India. Journal of Optical Communications, 0. De Gruyter.

[46]. Kumar, R., Shukla, S., & Raghuvanshi, C. S. (2024). Deep learning models for predicting high and low tides with gravitational analysis. In Sustainable development in AI, blockchain, and e-governance applications (pp. 35–46). IGI Global.

[47]. Rahman, Anichur, et al. "Blockchain-based AI Methods for Managing Industrial IoT: Recent Developments, Integration Challenges and Opportunities." arXiv, 21 May 2024, arxiv.org/abs/2405.12550.

[48]. Khan, Muhammad Salman, et al. "Industrial Internet of Things: Recent Advances, Enabling Technologies and Open Challenges." Future Generation Computer Systems, vol. 101, 2019, pp. 715–728. Elsevier, doi:10.1016/j.future.2019.06.006.

[49]. Dorri, Ali, et al. "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home." 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, 2017, pp. 618–623. doi:10.1109/PERCOMW.2017.7917634.

[50]. Hassan, Rania, et al. "Integrating Blockchain and Artificial Intelligence for Trustworthy IoT Ecosystems: A Comprehensive Survey." IEEE Access, vol. 9, 2021, pp. 79761–79796. doi:10.1109/ACCESS.2021.3084502.

[51]. Sharma, Priyanka, et al. "Blockchain Technology for Secure Industrial IoT Networks." IEEE Transactions on Industrial Informatics, vol. 15, no. 6, 2019, pp. 3693–3700. doi:10.1109/TII.2019.2900890.

[52]. Nguyen, Dinh C., et al. "Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges." IEEE Internet of Things Journal, vol. 7, no. 10, 2020, pp. 8563–8576. doi:10.1109/JIOT.2020.2990007.

[53]. Atlam, Hany F., et al. "Blockchain with Internet of Things: Benefits, Challenges, and Future Directions." International Journal of Intelligent Systems, vol. 35, no. 10, 2020, pp. 1970–1998. doi:10.1002/int.22242.