Chapter 7

Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications

Amit Kumar Tyagi
https://orcid.org/0000-0003-2657-8700
National Institute of Fashion Technology, New Delhi, India

ABSTRACT

As the internet of things (IoT) and industrial internet of things (IIoT) continue to expand, the need for robust cyber security solutions becomes increasingly critical. The convergence of blockchain technology and artificial intelligence (AI) offers promising opportunities to address the security challenges posed by IoT and IIoT applications. This chapter provides an overview of the potential synergies between blockchain and AI in the context of cyber security for IoT and IIoT. Blockchain technology, with its decentralized and immutable nature, can provide enhanced security and trust in IoT and IIoT networks. It offers features such as data integrity, transparency, and tamper resistance, making it well-suited for securing critical data and transactions. Additionally, blockchain can facilitate secure device identity management, access control, and secure communication among IoT and IIoT devices.

DOI: 10.4018/979-8-3693-0659-8.ch007

1. INTRODUCTION

The rapid proliferation of IoT and IIoT devices has introduced new challenges in ensuring the security and privacy of connected systems. The interconnected nature of these devices, along with the vast amounts of data they generate, has created a complex cyber security landscape. In response to these challenges, the integration of Blockchain technology and AI has emerged as a potential solution (Gupta & Sehgal, 2019). Note that Blockchain, originally developed for cryptocurrency applications, is a decentralized and distributed ledger technology that ensures the transparency, integrity, and immutability of data. It provides a secure and tamper-resistant platform for recording and verifying transactions. The decentralized nature of Blockchain eliminates the need for a central authority, making it suitable for securing IoT and IIoT networks. Artificial Intelligence, on the other hand, leverages advanced algorithms and machine learning techniques to enable systems to analyze, learn, and make intelligent decisions (Xu et al., 2018). AI has the potential to enhance cyber security by detecting anomalies, identifying patterns, and predicting and mitigating cyber threats. It can adapt and improve its defense mechanisms based on continuous learning from data patterns and user behavior. The integration of Blockchain and AI in the context of cyber security for IoT and IIoT applications offers several advantages. Blockchain provides a secure and transparent infrastructure for recording and sharing security-related information, such as device identities and access permissions. It enhances trust and accountability in IoT and IIoT networks. AI, on the other hand, can leverage the data stored on the Blockchain to analyze and detect potential threats in real-time. By combining the strengths of both technologies, organizations can achieve a higher level of security and resilience in their connected systems.

However, there are challenges and issues to be addressed in the implementation of Blockchain and AI for cyber security. Scalability and interoperability issues need to be overcome to handle the increasing volume of IoT and IIoT data. The computational overhead of Blockchain and the complexity of AI models pose additional challenges. Moreover, the explainability, privacy, and ethical aspects of AI algorithms need careful attention. In summary, the integration of Blockchain and AI presents a promising approach to address the cyber security challenges in the era of IoT and IIoT applications. By leveraging the strengths of Blockchain's decentralized and immutable nature and AI's advanced analytics and decision-making capabilities, organizations can enhance the security, trust, and resilience of their connected systems. In last, this work has been discussed in 11 sections.

2. INTERNET OF THINGS (IoT) AND INDUSTRIAL INTERNET OF THINGS (IIoT)

2.1 Overview of IoT and IIoT

IoT and IIoT are two interconnected concepts that involve the integration of smart devices, sensors, and networks to enable communication and data exchange between physical objects and digital systems (Aljawarneh et al., 2020). The IoT refers to a network of interconnected devices, objects, and systems that are embedded with sensors, software, and connectivity capabilities. These devices can collect and exchange data with each other and with cloud-based platforms, enabling various applications and services. IoT devices can range from everyday consumer products like smart thermostats and wearable devices to industrial equipment and infrastructure. The IIoT, on the other hand, focuses specifically on the application of IoT technologies in industrial sectors such as manufacturing, energy, transportation, and agriculture. IIoT systems are designed to improve operational efficiency, optimize resource utilization, and enable data-driven decision-making in industrial processes. It involves the integration of sensors, automation, and data analytics in industrial equipment and infrastructure.

Note that both IoT and IIoT share common characteristics such as connectivity, data exchange, and the ability to remotely monitor and control devices. They enable real-time data collection, analysis, and interaction between physical objects and digital systems, creating new opportunities for efficiency, automation, and innovation. Hence, few key components of IoT and IIoT include:

- Devices and Sensors: These are physical objects equipped with sensors and actuators to collect and transmit data.
- Connectivity: IoT and IIoT devices rely on various communication technologies such as Wi-Fi, Bluetooth, cellular networks, or low-power wide-area networks (LPWAN) to connect and exchange data.
- Cloud Computing: Data collected from IoT and IIoT devices is often processed and stored in cloud-based platforms, providing scalability and accessibility for data analysis and application development.
- Data Analytics: IoT and IIoT generate large volumes of data, which can be analyzed using advanced analytics techniques such as machine learning and artificial intelligence to derive valuable insights and make informed decisions.
- Applications and Services: IoT and IIoT enable a wide range of applications and services across various industries, including smart home automation, predictive maintenance, remote monitoring, supply chain optimization, and energy management.

Hence, the growth of IoT and IIoT has the potential to revolutionize industries, improve efficiency, and create new business opportunities (Raza et al., 2017). However, it also poses challenges related to data privacy, security, interoperability, and scalability. Addressing these challenges requires a holistic approach that considers technical, regulatory, and ethical issues to ensure the successful implementation and adoption of IoT and IIoT technologies.

2.2 Applications and Use Cases of IoT and IIoT

The applications and use cases of the IoT and IIoT span across various industries and sectors. Here are some prominent examples:

- Smart Home Automation: IoT enables homeowners to control and automate various devices in their homes, such as lighting, temperature, security systems, and appliances. It enhances convenience, energy efficiency, and security.
- Smart Cities: IoT technologies can be used to optimize urban infrastructure and services, including smart parking, intelligent traffic management, waste management, air quality monitoring, and efficient energy distribution.
- Industrial Automation: IIoT facilitates the automation and optimization of industrial processes, such as manufacturing, supply chain management, and logistics. It enables real-time monitoring, predictive maintenance, and improved operational efficiency.

- Agriculture: IoT is utilized in precision farming to monitor and optimize crop conditions, irrigation, and livestock management. It helps farmers make data-driven decisions, reduce resource wastage, and enhance productivity.
- Energy Management: IoT and IIoT enable smart grid systems that monitor and manage energy distribution, consumption, and renewable energy sources. They promote energy efficiency, grid stability, and demand response programs.
- Healthcare: IoT devices are used for remote patient monitoring, wearable health trackers, and smart medical devices. They enable real-time health data collection, early detection of medical conditions, and personalized healthcare.
- Environmental Monitoring: IoT sensors and networks are deployed for monitoring and managing environmental conditions, such as air quality, water quality, and weather patterns. They aid in pollution control and natural resource management.
- Transportation and Logistics: IoT is applied to track and manage fleet vehicles, optimize routes and logistics operations, and improve supply chain visibility. It enhances efficiency, safety, and asset management.
- Smart Retail: IoT is utilized in retail environments for inventory management, personalized customer experiences, smart shelves, and automated checkout systems. It enhances customer satisfaction and operational efficiency.

Hence these are few examples, and the potential applications of IoT and IIoT continue to expand across industries. The ability to collect and analyze data from connected devices enables organizations to gain valuable insights, optimize processes, and create innovative solutions that improve efficiency, sustainability, and quality of life.

3. CYBERSECURITY IN THE IoT AND IIoT LANDSCAPE

3.1 Threat Landscape in IoT and IIoT

The threat landscape in IoT and IIoT is constantly evolving, with various types of threats targeting the connected devices and systems. Here are some key threats in the IoT and IIoT landscape:

- Unauthorized Access: Attackers may attempt to gain unauthorized access to IoT devices or networks to exploit vulnerabilities, steal sensitive data, or take control of devices for malicious purposes. Weak or default passwords, insecure communication protocols, and outdated software are common entry points for unauthorized access.
- Data Breaches: IoT devices collect and transmit vast amounts of sensitive data, including personal information and operational data. Data breaches can occur if security measures, such as encryption, access controls, and secure data storage, are not implemented properly. Stolen or compromised data can be used for identity theft, financial fraud, or other malicious activities.
- Botnets and DDoS Attacks: IoT devices can be compromised and recruited into botnets, which are networks of compromised devices controlled by a remote attacker. Botnets can be used to launch Distributed Denial of Service (DDoS) attacks, overwhelming targeted systems or networks with a flood of traffic and causing service disruptions.

- Device Tampering and Physical Attacks: Physical access to IoT devices can enable attackers to tamper with their functionality or extract sensitive information. This includes physically altering devices, manipulating sensors or actuators, or extracting cryptographic keys. Physical attacks can also target the infrastructure supporting IoT deployments, such as communication networks or data centers.
- Malware and Ransomware: IoT devices are susceptible to malware infections and ransomware attacks, where malicious software encrypts or locks down devices until a ransom is paid. Malware can spread through vulnerable devices or compromised networks, leading to system disruption, data loss, or unauthorized access.
- Supply Chain Attacks: IoT devices often rely on a complex supply chain involving multiple vendors and components. Attackers may exploit vulnerabilities in the supply chain to introduce malicious software or hardware, compromising the security and integrity of the devices.
- Privacy Violations: IoT devices constantly collect and transmit data, raising concerns about user privacy. Unauthorized access to personal information, unauthorized monitoring, or data leakage can result in privacy violations and compromise user trust.
- Insider Threats: Insider threats involve malicious actions or negligence from employees, contractors, or individuals with authorized access to IoT systems. Insider threats can result in data breaches, system manipulation, or theft of sensitive information.
- Lack of Security Updates and Patching: IoT devices often have long lifecycles and limited resources, making them vulnerable to security vulnerabilities that may go unpatched. Failure to regularly update and patch IoT devices can leave them susceptible to known security vulnerabilities.
- Lack of Standardization: The lack of standardized security protocols and practices across IoT devices and platforms can create inconsistencies and vulnerabilities. Lack of interoperability and standardization hinders the implementation of robust security measures.

Hence, addressing the IoT and IIoT threat landscape requires a comprehensive approach that includes implementing strong authentication mechanisms, encryption, access controls, regular security updates, and monitoring mechanisms. User awareness, industry collaboration, and regulatory frameworks are essential in mitigating the evolving threats in the IoT and IIoT ecosystem.

3.2 Security Challenges and Vulnerabilities in IoT and IIoT

The widespread adoption of IoT and IIoT brings about various security challenges and vulnerabilities (Biswas & Koo, 2020; Puthal et al., 2019). Here are some key security challenges and vulnerabilities in IoT and IIoT:

- Weak Authentication and Authorization: Many IoT devices and systems suffer from weak or default authentication mechanisms, making them susceptible to unauthorized access. Lack of strong authentication and authorization mechanisms can allow attackers to compromise devices, gain unauthorized control, or access sensitive data.
- Insecure Communication: IoT devices often rely on communication protocols that lack encryption or use weak encryption methods. This vulnerability can enable attackers to intercept and tamper with data during transmission, leading to data breaches or unauthorized control of devices.

- Lack of Device Management: IoT devices often have limited security features and lack robust device management capabilities. This makes it challenging to enforce security policies, apply security updates, and detect and respond to security incidents in a timely manner.
- Firmware and Software Vulnerabilities: IoT devices often run on firmware and software that may have security vulnerabilities. Manufacturers may not regularly provide security patches or updates for these devices, leaving them exposed to known vulnerabilities that can be exploited by attackers.
- Physical Security Risks: Physical access to IoT devices can lead to tampering, reverse engineering, or extraction of sensitive information. Physical security measures, such as tamper-proof packaging, secure boot processes, and device hardening, are essential to protect against physical attacks.
- Privacy issues: IoT devices collect vast amounts of data, often including personal and sensitive information. Inadequate privacy protections, such as improper data handling, lack of user consent, or unauthorized data sharing, can result in privacy breaches and compromise user trust (Ding et al., 2019).
- Scalability and Interoperability Challenges: As IoT deployments scale, managing security becomes more challenging. Ensuring interoperability and security across diverse devices, platforms, and networks requires standardized security protocols, secure APIs, and consistent security practices.
- Lack of Security Awareness: Users and organizations may lack awareness of IoT security best practices, making them more susceptible to social engineering attacks, such as phishing or credential theft. Security training and awareness programs are necessary to educate users about the risks and promote secure behaviors.
- Legacy System Integration: Integrating IoT devices with existing legacy systems introduces security challenges. Incompatibilities, lack of security measures in legacy systems, and potential vulnerabilities in integration points can expose the entire system to security risks.

In summary, addressing these security challenges and vulnerabilities requires a holistic approach that includes robust authentication and encryption mechanisms, secure communication protocols, regular security updates, strong access controls, and user awareness. Collaboration between manufacturers, service providers, policymakers, and users is important to ensuring the security and resilience of IoT and IIoT deployments.

3.3 Importance of Cybersecurity in IoT and IIoT

Cybersecurity is of paramount importance in the context of IoT and IIoT due to the increasing interconnectedness of devices, networks, and systems. Here are some key reasons why cybersecurity is important in IoT and IIoT:

- Protection of Sensitive Data: IoT and IIoT systems collect and transmit vast amounts of sensitive data, including personal information, operational data, and industrial trade secrets. Ensuring robust cybersecurity measures protects this data from unauthorized access, theft, tampering, or disclosure, preserving privacy and maintaining the integrity of critical information.
- Safeguarding Operational Continuity: Many IoT and IIoT deployments are used in critical infrastructure and industrial settings where disruptions can have severe consequences. Cybersecurity

safeguards prevent unauthorized access, manipulation, or disruption of IoT devices and systems, ensuring uninterrupted operations and maintaining the stability and reliability of critical services.

- Mitigating Financial Losses: Cyberattacks on IoT and IIoT deployments can lead to significant financial losses for individuals, businesses, and organizations. These losses may arise from theft of intellectual property, financial fraud, system downtime, or regulatory fines due to non-compliance. Implementing robust cybersecurity measures helps mitigate the financial impact of cyber threats.
- Protecting User Privacy: IoT devices often gather sensitive information about individuals, such as personal habits, health data, and location information (Samaniego & Yang, 2020; Yang et al., 2019). Cybersecurity measures, including encryption, secure data storage, and user authentication, are important for protecting user privacy and ensuring that personal information remains confidential.
- Preserving Trust and Reputation: Cybersecurity incidents in IoT and IIoT can undermine trust in the technology and the organizations deploying it. Demonstrating a strong commitment to cybersecurity builds trust with users, customers, and partners, enhancing reputation and ensuring continued adoption and success of IoT and IIoT solutions.
- Ensuring Safety: In certain IoT and IIoT applications, such as autonomous vehicles, healthcare devices, or industrial control systems, cybersecurity is critical for ensuring the safety of users and the public. Cybersecurity vulnerabilities in these systems can lead to physical harm, accidents, or loss of life. Robust security measures help prevent such risks and ensure the safety of individuals and communities.
- Addressing Evolving Threat Landscape: The threat landscape in the cybersecurity domain is constantly evolving, with new attack vectors, vulnerabilities, and sophisticated techniques emerging regularly. Proactive cybersecurity measures, including continuous monitoring, threat intelligence, and timely updates, are important for staying ahead of emerging threats and minimizing risks.

Hene, by giving the interconnected and complex nature of IoT and IIoT systems, we need to ensure cybersecurity requires a multi-layered approach that encompasses secure device design, strong authentication and encryption mechanisms, network security, regular updates and patching, user awareness, and industry collaboration.

4. ARTIFICIAL INTELLIGENCE (AI) IN CYBERSECURITY

4.1 Introduction to AI and Machine Learning in Cybersecurity

AI and machine learning have emerged as powerful technologies in the field of cybersecurity. They offer innovative approaches to detecting, preventing, and responding to cyber threats (Yang et al., 2019; Ylianttila & Vasilakos, 2017). Here is an introduction to AI and machine learning in cybersecurity:

- Artificial Intelligence: Artificial Intelligence refers to the development of computer systems that can perform tasks that typically require human intelligence. It involves the simulation of human intelligence processes such as learning, reasoning, problem-solving, and decision-making.
- Machine Learning: Machine Learning is a subset of AI that focuses on developing algorithms and models that enable computers to learn from data and make predictions or take actions without

explicit programming. Machine learning algorithms can automatically analyze and detect patterns in data to generate insights and make informed decisions.

- Application of AI and Machine Learning in Cybersecurity: AI and machine learning have found various applications in cybersecurity due to their ability to process large volumes of data, identify patterns, and make real-time decisions. Here are some key applications:
- Threat Detection and Prevention: Machine learning algorithms can analyze vast amounts of data to identify patterns indicative of cyber threats, such as malware, phishing attacks, or network intrusions. By learning from historical data, machine learning models can detect and prevent potential security breaches, enabling early intervention and proactive defense mechanisms.
- Anomaly Detection: AI and machine learning techniques can identify anomalous behavior or deviations from normal patterns in network traffic, user activities, or system behavior. This helps in detecting insider threats, zero-day attacks, or unusual system behavior that may indicate a security breach.
- Behavioral Analysis: Machine learning algorithms can learn and analyze user behavior to establish baseline profiles and detect deviations. This allows for the identification of suspicious activities or unauthorized access attempts, enhancing the accuracy of intrusion detection systems.
- Malware Detection: AI and machine learning techniques can be applied to identify and classify malware based on its behavior, code analysis, or signature detection. Machine learning models can continually learn from new malware samples to improve detection rates and stay updated against emerging threats.
- Vulnerability Management: AI and machine learning can assist in vulnerability management by automatically scanning and analyzing systems and applications for potential vulnerabilities. This helps in prioritizing and patching vulnerabilities, reducing the risk of exploitation by attackers.
- Security Analytics: AI and machine learning enable advanced security analytics by correlating data from multiple sources, detecting complex attack patterns, and generating actionable insights. This helps in identifying advanced persistent threats (APTs), conducting threat hunting, and improving incident response capabilities.
- Automated Response and Orchestration: AI can automate incident response by integrating with security orchestration platforms. Machine learning models can make real-time decisions, initiate automated remediation actions, or provide recommendations to security analysts, thereby accelerating incident response and reducing response times.

Note that the integration of AI and machine learning in cybersecurity brings several benefits, including enhanced threat detection capabilities, improved accuracy, faster response times, and proactive defense mechanisms. However, it is essential to address challenges such as the potential for adversarial attacks, data privacy concerns, and the need for interpretability and explainability in AI models to ensure the effective and responsible use of these technologies in cybersecurity.

4.2 AI-Based Threat Detection and Prevention

AI-based threat detection and prevention refers to the use of artificial intelligence techniques, such as machine learning, to identify and mitigate cybersecurity threats in real-time (Nair & Tyagi, 2023; Sk et al., 2022). These advanced systems analyze vast amounts of data, learn from patterns, and make intelligent decisions to detect and prevent various types of cyber-attacks. Here is an overview of AI-based threat detection and prevention:

Machine Learning Algorithms: Machine learning algorithms are trained on large datasets to learn patterns and characteristics of normal network behavior. These algorithms can then identify anomalies and deviations from normal behavior, indicating potential security threats. Examples of machine learning algorithms used in threat detection include decision trees, random forests, support vector machines, and neural networks.

- Anomaly Detection: Anomaly detection is a common approach in AI-based threat detection. Machine learning models are trained on historical data to establish a baseline of normal behavior. Any deviation from this baseline is flagged as an anomaly and investigated further. Anomaly detection can help identify various attacks, including network intrusions, insider threats, and unauthorized access attempts.
- Behavioral Analysis: AI-based systems can analyze user behavior to identify unusual or suspicious activities. By learning from user patterns, these systems can detect anomalies in user behavior, such as abnormal login times, excessive data access, or unauthorized privilege escalation. Behavioral analysis helps in identifying potential insider threats and detecting account compromise or misuse.
- Malware Detection: AI techniques are used for malware detection by analyzing characteristics, behaviors, or code patterns of known malware samples. Machine learning models can be trained on large datasets of malware samples to identify common features and signatures. This allows for the detection of new and previously unseen malware based on learned patterns, even if specific signatures are not available.
- Threat Intelligence and Data Analysis: AI-based systems can leverage threat intelligence feeds, vulnerability databases, and security-related news to gather information on the latest threats and attack vectors. By analyzing this data, AI models can identify emerging threats, correlate events, and provide timely alerts or recommendations to security teams.
- Automated Response and Remediation: AI-based systems can automate response and remediation actions to counter detected threats. These systems can integrate with security orchestration platforms to initiate automated actions, such as isolating compromised systems, blocking malicious IP addresses, or updating firewall rules. Automated response capabilities help in reducing response times and mitigating the impact of cyber-attacks.

Hence, AI-based threat detection and prevention systems offer the advantage of real-time monitoring, proactive defense, and the ability to handle large volumes of data. However, it is important to regularly evaluate and update these systems, as cyber threats are constantly evolving. Collaboration between AI systems and human experts is also important to ensure accurate threat identification, response prioritization, and decision-making in complex cybersecurity environments.

4.3 AI-Driven Anomaly Detection in IoT and IIoT

AI-driven anomaly detection plays a critical role in securing IoT and IIoT environments. It helps in identifying abnormal behaviors or events that could indicate potential security breaches, equipment malfunctions, or operational anomalies. Here’s an overview of AI-driven anomaly detection in IoT and IIoT:

- Data Collection and Preprocessing: Anomaly detection starts with the collection of data from IoT and IIoT devices, which can include sensor readings, network traffic, device logs, and operational data. The collected data is preprocessed to remove noise, handle missing values, and normalize the data for further analysis.
- Feature Extraction: Relevant features are extracted from the preprocessed data to capture meaningful patterns and characteristics. These features can include statistical measures, time-series properties, frequency components, or other domain-specific metrics.
- Unsupervised Learning Techniques: AI-driven anomaly detection often utilizes unsupervised learning techniques. Unsupervised learning algorithms, such as clustering or density estimation algorithms, are applied to the feature space to identify groups or clusters of normal behavior. Instances that fall outside these clusters are flagged as potential anomalies.
- Supervised Learning Techniques: In some cases, labeled data may be available, where anomalies are already identified. Supervised learning algorithms, such as classification or regression algorithms, can be used to train models on labeled data and then apply them to detect anomalies in new, unlabeled data.
- Time-Series Analysis: IoT and IIoT data often exhibit time-dependent patterns. Time-series analysis techniques, such as autoregressive models, moving averages, or Fourier transforms, can be employed to capture temporal dependencies and identify anomalies based on deviations from expected patterns.
- Deep Learning Approaches: Deep learning, particularly recurrent neural networks (RNNs) and long short-term memory (LSTM) networks, are effective for anomaly detection in sequential data. These models can learn complex temporal patterns and detect anomalies based on deviations from learned sequences.
- Online and Real-Time Detection: Anomaly detection in IoT and IIoT requires real-time or near real-time processing to enable timely response. AI-driven approaches should be capable of analyzing streaming data, detecting anomalies in real-time, and triggering immediate alerts or automated actions.

Hence, AI-driven anomaly detection in IoT and IIoT brings several benefits, including early detection of security breaches, proactive maintenance, improved operational efficiency, and reduced downtime. However, challenges such as high-dimensional data, data quality issues, scalability, and interpretability of AI models need to be addressed to ensure the effectiveness and reliability of anomaly detection systems in IoT and IIoT environments.

5. BLOCKCHAIN TECHNOLOGY IN CYBERSECURITY

5.1 Fundamentals of Blockchain Technology and Blockchain Applications in Cybersecurity

Blockchain technology is a decentralized and distributed ledger system that enables secure and transparent record-keeping of transactions or data across multiple participants (). Understanding the fundamentals of blockchain technology is essential to explore its potential applications and implications in various industries, including cybersecurity, finance, logistics, and governance. Blockchain technology offers several applications in the field of cybersecurity, providing enhanced security, transparency, and integrity. Here are some key applications of blockchain in cybersecurity:

- Immutable Audit Trails: Blockchain provides an immutable and tamper-proof ledger, making it ideal for creating audit trails. Security events, such as system changes, access attempts, or data breaches, can be recorded on the blockchain, ensuring transparency and enabling forensic analysis.
- Secure Identity Management: Blockchain can be used for identity management, eliminating the need for centralized identity providers. By storing encrypted identity information on the blockchain, users can maintain control over their personal data, reducing the risk of identity theft and unauthorized access.
- Secure Data Storage: Blockchain can be used to securely store sensitive data. Instead of storing data on centralized servers, data can be encrypted, distributed across the blockchain network, and accessed only by authorized parties. This enhances data security and mitigates the risk of data breaches.
- Distributed Threat Intelligence: Blockchain enables the sharing of threat intelligence across multiple organizations securely. By storing and sharing threat information on the blockchain, organizations can collaborate in real-time, enhancing their ability to detect and respond to emerging threats.
- Secure Supply Chain Management: Blockchain can be utilized to enhance the security and transparency of supply chains. It enables the tracking and verification of products and components throughout the supply chain, ensuring authenticity and preventing counterfeiting or tampering.
- Decentralized DNS: Blockchain can be used to create a decentralized domain name system (DNS), reducing the risk of domain hijacking and DNS attacks. By storing domain ownership information on the blockchain, it becomes more resilient to malicious manipulation.
- Zero-Trust Networks: Blockchain can facilitate the creation of decentralized, trustless networks. By using blockchain technology, organizations can establish peer-to-peer connections and verify the integrity and authenticity of network participants without relying on a central authority.
- Secure Smart Contracts: Blockchain-based smart contracts can enhance the security of contractual agreements. Smart contracts are self-executing and self-enforcing, reducing the risk of fraud or tampering. The decentralized nature of blockchain ensures the reliability and integrity of smart contract execution.
- Incident Response and Forensics: Blockchain technology can aid in incident response and forensic investigations. By storing security event logs and digital evidence on the blockchain, investigators can ensure the integrity and non-repudiation of collected evidence.
- Threat Detection and Analytics: Blockchain can be leveraged for detecting and analyzing cyber threats. By aggregating and analyzing security-related data from multiple sources on the blockchain, patterns and anomalies can be identified, enabling proactive threat detection and response.

Note that these applications highlight the potential of blockchain technology in enhancing cybersecurity practices. However, it's important to consider the limitations of blockchain, such as scalability, privacy, and regulatory challenges, while exploring its applications in the cybersecurity domain.

5.2 Security and Privacy Concerns of Blockchain Based Cybersecurity

While blockchain technology offers enhanced security features, it is not without its security and privacy concerns (Jayaprakash & Tyagi, 2022; Tyagi, Agarwal, & Sreenath, 2022). Here are some of the key concerns related to blockchain-based cybersecurity:

- 51% Attack: In public blockchains that rely on consensus mechanisms like Proof of Work (PoW), there is a risk of a 51% attack. If a single entity or group controls more than 50% of the network's computing power, they can manipulate the blockchain by rewriting transaction history or excluding certain transactions from being added to the chain.
- Smart Contract Vulnerabilities: Smart contracts deployed on blockchain platforms can be vulnerable to coding errors or vulnerabilities, leading to security breaches. Exploiting these vulnerabilities can result in financial losses, unauthorized access to data, or disruption of services.
- Privacy Risks: While blockchain provides transparency, it also poses challenges to privacy. The decentralized and immutable nature of blockchain means that once data is recorded, it cannot be easily modified or erased. This can be a concern when dealing with sensitive or personally identifiable information.
- Key Management: Blockchain-based systems rely on cryptographic keys for authentication and data encryption. Poor key management practices, such as weak passwords or improper storage of keys, can lead to unauthorized access and compromise the security of the blockchain.
- Scalability and Performance: Public blockchains, like Bitcoin and Ethereum, face scalability and performance limitations. As the number of transactions increases, the network can become congested, resulting in slower transaction processing times and increased costs. These limitations can impact the overall security and effectiveness of blockchain-based systems.
- Regulatory Compliance: Blockchain-based systems may face challenges in meeting regulatory requirements, particularly in industries with strict data protection and privacy regulations. Compliance with regulations like the General Data Protection Regulation (GDPR) can be complex, considering the decentralized nature and immutability of blockchain data.
- Insider Threats: While blockchain provides security against external tampering, it may not address insider threats. Malicious actors with authorized access to the blockchain network can manipulate data or disrupt the system from within, posing a significant security risk.
- Lack of Standardization: The absence of standardized protocols and frameworks for blockchain security can lead to inconsistencies in security practices across different blockchain platforms. This lack of standardization may make it challenging to ensure consistent security measures and interoperability between blockchain networks.

Note that to address these issues, it is essential to implement additional security measures, such as secure key management practices, code audits for smart contracts, encryption of sensitive data, and access control mechanisms. It is also important to continuously monitor and update the security protocols of blockchain-based systems to mitigate emerging threats and vulnerabilities.

6. INTEGRATION OF BLOCKCHAIN AND AI FOR CYBERSECURITY IN IoT AND IIoT

6.1 Blockchain-Based Secure Communication in IoT and IIoT

Blockchain technology can be leveraged to provide secure communication in IoT and IIoT environments (Dagher et al., 2018; Fernández-Caramés & Fraga-Lamas, 2020; Jayaprakash & Tyagi, 2022; Varsha, 2022). Here's how blockchain can enhance communication security in these contexts:

- Data Integrity: Blockchain ensures the integrity of data transmitted within IoT and IIoT systems. Each data transaction is recorded as a block on the blockchain, and once added, it becomes immutable. This guarantees that the data cannot be tampered with or altered during transmission, ensuring the integrity of the information exchanged.
- Trust and Authentication: Blockchain enables trust and authentication in IoT and IIoT communication. By leveraging cryptographic algorithms, devices can securely identify and authenticate themselves on the blockchain network. This eliminates the need for a centralized authority for authentication, reducing the risk of unauthorized access or impersonation.
- Distributed and Decentralized Network: Blockchain operates as a distributed and decentralized network, making it resilient against single points of failure or attacks. IoT and IIoT devices can connect to the blockchain network, ensuring that communication occurs in a peer-to-peer manner. This decentralized architecture enhances security by minimizing the potential for a single point of vulnerability.
- Secure Device Registration: Blockchain can facilitate secure device registration and onboarding in IoT and IIoT networks. By storing device identity and registration information on the blockchain, it becomes easier to verify the authenticity and integrity of the devices joining the network. This prevents unauthorized devices from gaining access and compromising the network.
- Encrypted Communication Channels: Blockchain-based systems can leverage encryption techniques to establish secure communication channels between IoT and IIoT devices. Encryption ensures that the data transmitted between devices is protected from eavesdropping or interception, safeguarding the confidentiality of the communication.
- Consensus Mechanisms: Blockchain consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), can be used to validate and verify IoT and IIoT transactions. Consensus ensures that only legitimate and valid transactions are added to the blockchain, preventing malicious actors from injecting fraudulent or malicious data into the communication stream.
- Auditability and Traceability: Blockchain provides auditability and traceability of communication transactions. Each communication event or transaction is recorded on the blockchain, creating an immutable audit trail. This enables forensic analysis and facilitates the identification and mitigation of any security breaches or unauthorized activities within the IoT and IIoT network.

Hence, by integrating blockchain technology into IoT and IIoT communication, organizations can enhance the security and trustworthiness of their systems. Blockchain-based secure communication ensures data integrity, authentication, decentralized network architecture, and encrypted channels, addressing the security concerns associated with IoT and IIoT environments.

6.2 AI-Enhanced Threat Intelligence Using Blockchain

AI-enhanced threat intelligence refers to the use of artificial intelligence techniques to enhance the process of collecting, analyzing, and responding to cybersecurity threats. Blockchain technology can be integrated with AI to further enhance the effectiveness and trustworthiness of threat intelligence systems. Here's how AI and blockchain can be combined to provide AI-enhanced threat intelligence:

- Immutable Data Storage: Blockchain provides a tamper-resistant and immutable ledger to store threat intelligence data. By storing threat data on the blockchain, it becomes difficult for attackers to modify or manipulate the information. This ensures the integrity and trustworthiness of the data used by AI systems for threat analysis.
- Data Sharing and Collaboration: Blockchain allows for secure and transparent data sharing among different entities within the cybersecurity ecosystem. AI algorithms can leverage blockchain to access a shared pool of threat intelligence data from various sources, including threat feeds, security vendors, and security researchers. This enables AI systems to have a broader and more comprehensive view of the threat landscape.
- Trust and Authenticity: Blockchain's decentralized and consensus-driven nature helps establish trust and authenticity in the threat intelligence data. AI algorithms can rely on the consensus mechanism of the blockchain to validate the accuracy and reliability of the data before utilizing it for analysis. This reduces the risk of relying on inaccurate or manipulated threat data.
- Enhanced Data Privacy: Blockchain can be used to implement privacy-preserving techniques, such as zero-knowledge proofs or differential privacy, to protect sensitive threat intelligence data. AI systems can leverage these privacy-enhancing features to ensure the confidentiality of the data while still benefiting from its insights.
- Smart Contracts for Threat Sharing: Smart contracts, which are self-executing contracts with predefined conditions, can be utilized on the blockchain to automate the sharing and distribution of threat intelligence. AI systems can interact with these smart contracts to retrieve relevant threat data, ensuring a seamless and secure sharing process.
- Real-time Threat Detection and Response: AI algorithms can be trained on real-time threat intelligence data stored on the blockchain, enabling faster and more accurate threat detection and response. By leveraging AI's capabilities in pattern recognition, anomaly detection, and behavioral analysis, organizations can proactively identify and mitigate emerging threats.
- Auditable and Transparent Analysis: The transparent nature of blockchain allows for auditable and transparent analysis of AI-driven threat intelligence systems. Security auditors and regulatory bodies can examine the blockchain to verify the integrity and fairness of the AI algorithms used for threat analysis.

Hence, by combining AI and blockchain, organizations can enhance their threat intelligence capabilities with improved data integrity, enhanced collaboration, trustworthiness, and privacy protection. AI algorithms can leverage the secure and transparent nature of blockchain to provide more effective and reliable threat intelligence for proactive cybersecurity defense.

6.3 Privacy and Data Protection With Blockchain and AI

Privacy and data protection are essential issues when implementing blockchain and AI technologies. Here are some key aspects to consider:

- Data Encryption: Utilize encryption techniques to protect sensitive data stored on the blockchain or usedby AI systems. Encryption ensures that only authorized parties with the appropriate decryption keys can access and interpret the data, adding an extra layer of protection.
- Pseudonymization: Apply pseudonymization techniques to replace personally identifiable information (PII) with pseudonyms or identifiers. This helps protect the privacy of individuals while still allowing for data analysis and processing.
- Access Control: Implement robust access control mechanisms to restrict data access to authorized users or AI algorithms. This includes authentication and authorization protocols to ensure that only approved entities can access and interact with the data.
- Consent Management: Establish clear processes for obtaining and managing user consent regarding data collection, processing, and sharing. Blockchain can be utilized to store and enforce consent records, providing a transparent and auditable system for managing user consent preferences.
- Privacy by Design: Incorporate privacy issues into the design and development of blockchain and AI systems from the outset. By integrating privacy features and principles during the design phase, organizations can ensure that privacy is prioritized throughout the technology implementation.
- Data Minimization: Only collect and store the minimum amount of data necessary for the intended purpose. Avoid unnecessary or excessive data collection to minimize privacy risks and potential data breaches.
- Transparent Data Management: Blockchain's transparent and immutable nature can provide individuals with greater visibility and control over their data. Use blockchain to enable individuals to track and manage their data, including the ability to revoke access permissions or request data deletion.
- Privacy Policies and Documentation: Clearly communicate privacy policies and practices to users, stakeholders, and employees. Provide easily accessible documentation that outlines how personal data is collected, used, stored, and protected within the blockchain and AI systems.
- Compliance with Regulations: Ensure compliance with relevant data protection regulations such as GDPR (General Data Protection Regulation) or CCPA (California Consumer Privacy Act). Understand the legal requirements for handling personal data and implement measures to meet those requirements.
- Regular Assessments and Audits: Conduct regular privacy assessments and audits to identify any vulnerabilities or risks related to privacy and data protection. This includes assessing the security of the blockchain infrastructure, evaluating AI algorithms for potential biases or privacy implications, and reviewing data handling practices.

Hence, by integrating privacy and data protection measures into the design and implementation of blockchain and AI systems, organizations can maintain a high level of privacy assurance while benefiting from the advantages of these technologies. It is important to adopt a privacy-conscious approach and ensure ongoing monitoring and compliance with privacy regulations and best practices.

7. SECURE IDENTITY AND ACCESS MANAGEMENT IN IoT AND IIoT

7.1 Authentication and Authorization in IoT and IIoT Based Environment

Authentication and authorization are essential components of security in IoT and IIoT environments. They help ensure that only authorized devices and entities can access and interact with IoT systems. Here's an overview of authentication and authorization in IoT and IIoT:

A. Authentication:
   - Authentication verifies the identity of devices or entities attempting to access the IoT or IIoT network. It ensures that only trusted and authorized devices are granted access. Common authentication mechanisms used in IoT and IIoT include:
   - Digital Certificates: Devices are issued digital certificates that contain their unique identifiers and cryptographic keys. These certificates are used to authenticate and establish trust between devices and the IoT network.
   - Passwords and Tokens: Devices may be assigned passwords or tokens that they must provide during the authentication process. These credentials are verified against a database of authorized devices or an authentication server.
   - Biometrics: Biometric authentication, such as fingerprint or facial recognition, can be used to authenticate users or devices. Biometric data is compared against stored templates to verify identity.
   - Public/Private Key Encryption: Devices can use asymmetric encryption with public and private keys. During authentication, a device presents its public key, and the network verifies the corresponding private key to establish device identity.

B. Authorization:
   - Authorization determines the level of access and privileges granted to authenticated devices or entities within the IoT or IIoT network. It ensures that devices can only perform authorized actions based on their roles and permissions. Common authorization mechanisms used in IoT and IIoT include:
   - Role-Based Access Control (RBAC): Devices are assigned specific roles that define their access rights and privileges. Access control policies are enforced based on these roles.
   - Attribute-Based Access Control (ABAC): Access control decisions are based on specific attributes associated with devices or entities, such as their location, time of access, or environmental conditions.
   - Access Control Lists (ACL): A list of authorized devices or entities and the actions they are allowed to perform is maintained. Access requests are evaluated against this list to determine whether access should be granted or denied.
   - Policy-Based Access Control (PBAC): Access control policies define the rules and conditions for granting access. Policies may consider factors such as device type, user identity, or the state of the network.

C. Combining Authentication and Authorization:
   - Authentication and authorization work together to ensure secure access to IoT and IIoT systems. After successful authentication, devices are granted appropriate authorization based

on their identity and assigned privileges. This combination helps prevent unauthorized access, malicious activities, and data breaches within the IoT and IIoT environments.

Note that we need to implement robust authentication and authorization mechanisms that align with the specific security requirements and constraints of the IoT and IIoT applications. This includes considering factors such as device constraints, network scalability, and the need for secure communication protocols.

7.2 Blockchain-Based Identity Management Solutions for IoT and IIoT Based Environment

Blockchain-based identity management solutions have emerged as a promising approach to address the challenges of identity and access management in IoT and IIoT environments. These solutions leverage the decentralized and immutable nature of blockchain to enhance security, privacy, and trust in managing identities of IoT devices and entities. Here's how blockchain can be used for identity management in IoT and IIoT:

- Decentralized Identity: Blockchain enables the creation of decentralized identities for IoT devices and entities. Each device can have its unique identifier stored on the blockchain, ensuring that identity information is not controlled by a single central authority. This eliminates the need for a centralized identity management system and reduces the risk of a single point of failure.
- Immutable Identity Records: Identity information and credentials can be stored on the blockchain as immutable records. This ensures the integrity and tamper-proof nature of identity data, making it difficult for malicious actors to alter or manipulate device identities.
- Trust and Verification: Blockchain provides a trust layer for identity verification. Device identities and associated attributes can be verified through consensus mechanisms, such as proof-of-work or proof-of-stake, ensuring the authenticity and validity of the identity information.
- Self-Sovereign Identity: Blockchain allows for self-sovereign identity, where devices have control over their own identity data. Devices can selectively share identity attributes and credentials with other parties while maintaining control over their personal information. This enhances privacy and gives devices the ability to manage their own identity without relying on a centralized authority.
- Secure Authentication: Blockchain-based identity management solutions can facilitate secure authentication mechanisms for IoT devices. Digital signatures and cryptographic protocols can be used to authenticate device identities and ensure secure communication between devices and the IoT network.
- Auditability and Transparency: Blockchain's transparent and auditable nature enables the tracking and auditing of identity-related transactions. This enhances accountability and allows for the traceability of identity management activities.
- Interoperability: Blockchain-based identity management solutions can facilitate interoperability between different IoT systems and platforms. Devices from different manufacturers or ecosystems can use a common blockchain-based identity framework, simplifying the integration and interoperability of diverse IoT devices.
- Revocation and Deletion: Blockchain can provide mechanisms for revoking or deleting device identities when necessary. For example, if a device is compromised or decommissioned, its identity can be revoked, preventing further access to the network.

Hence, implementing blockchain-based identity management solutions in IoT and IIoT environments offers several benefits, including enhanced security, privacy, trust, and interoperability. However, challenges such as scalability, performance, and energy efficiency need to be considered and addressed when designing and deploying blockchain-based identity management systems for IoT and IIoT applications.

8. DATA INTEGRITY AND PRIVACY IN IoT AND IIoT

8.1 Challenges of Data Integrity and Privacy in IoT and IIoT Based Environment

Data integrity and privacy in IoT and IIoT environments present significant challenges due to the massive volume of data generated, diverse sources of data, and the distributed nature of IoT systems. Here are some key challenges related to data integrity and privacy in IoT and IIoT:

- Data Verification and Trustworthiness: Ensuring the integrity and authenticity of IoT data is challenging, as data can be tampered with or manipulated during transmission or storage. Verifying the trustworthiness of data becomes useful/ important to prevent malicious activities and maintain data integrity.
- Data Encryption and Security: IoT devices generate and transmit sensitive data, including personal information, financial data, and operational details. Protecting this data from unauthorized access requires robust encryption techniques and security measures to safeguard against data breaches and cyber-attacks.
- Data Aggregation and Fusion: IoT systems often involve multiple devices and sensors that generate vast amounts of data. Aggregating and fusing data from diverse sources while preserving data integrity and privacy is a complex task. Ensuring that data from different devices is combined accurately and securely is a challenge in maintaining data integrity.
- Data Lifecycle Management: Managing the lifecycle of IoT data, from collection to storage and disposal, presents challenges. Data must be properly handled, stored securely, and disposed of appropriately to prevent unauthorized access, data leakage, or unintended exposure.
- Consent and User Privacy: IoT devices collect data from users, and ensuring user consent and privacy becomes essential. Consent mechanisms should be transparent and allow users to have control over the data collected from them. Respecting user privacy rights while maintaining the functionality of IoT systems is a challenge.
- Data Governance and Compliance: IoT and IIoT environments may be subject to various data protection regulations and compliance requirements. Ensuring compliance with regulations such as the General Data Protection Regulation (GDPR) or industry-specific standards is a challenge due to the distributed nature of IoT systems and the complexity of data handling.
- Data Sharing and Collaboration: IoT systems often require data sharing and collaboration between different stakeholders. Balancing the need for data sharing while protecting privacy and maintaining data integrity is a challenge. Establishing secure and privacy-preserving data sharing frameworks and protocols is important.
- Edge Computing and Data Processing: With the proliferation of edge computing in IoT and IIoT, data is processed closer to the source. Ensuring data integrity and privacy during edge processing

becomes challenging due to resource-constrained devices and the need for secure communication and computation.

Hence, addressing these challenges requires a detailed approach that includes robust encryption techniques, secure data transmission protocols, privacy-preserving data management practices, and compliance with relevant regulations. Additionally, implementing secure authentication mechanisms, data access controls, and transparency in data handling can help mitigate data integrity and privacy risks in IoT and IIoT environments.

8.2 Blockchain-Enabled Data Integrity and Auditing in IoT and IIoT Based Environment

Blockchain technology offers a promising solution for ensuring data integrity and auditing in IoT and IIoT environments. By leveraging the decentralized and immutable nature of blockchain, it provides a transparent and tamper-proof framework for data verification and auditing. Here's how blockchain enables data integrity and auditing in IoT and IIoT:

- Immutable Data Storage: Blockchain serves as a distributed ledger where data can be stored in a decentralized manner. Each data transaction is recorded as a block, which is linked to the previous blocks using cryptographic hashes, forming a chain. Once a block is added to the blockchain, it becomes immutable, making it highly resistant to data tampering or unauthorized modifications.
- Data Integrity Verification: With blockchain, data integrity can be ensured through cryptographic techniques. IoT devices can generate digital signatures or hashes of their data, which are then stored on the blockchain. Any subsequent changes or tampering with the data can be detected by comparing the original digital signature or hash with the one stored on the blockchain.
- Consensus Mechanisms: Blockchain relies on consensus mechanisms to validate and verify data transactions. In a public blockchain, multiple nodes in the network participate in the consensus process to agree on the validity of transactions. This consensus mechanism ensures that only valid and authorized data is added to the blockchain, enhancing data integrity.
- Auditing and Traceability: Blockchain's transparent and immutable nature facilitates auditing and traceability of data in IoT and IIoT systems. Each data transaction recorded on the blockchain can be traced back to its origin, providing an auditable trail of data events. This capability enables organizations to track data flow, verify data authenticity, and ensure compliance with regulatory requirements.
- Smart Contracts for Data Validation: Smart contracts, which are self-executing agreements running on the blockchain, can be used to automate data validation and auditing processes. Smart contracts can define rules and conditions for data transactions, automatically verifying the integrity of incoming data and triggering actions based on predefined criteria.
- Data Provenance and Ownership: Blockchain can establish a clear record of data provenance and ownership. By storing transaction details on the blockchain, organizations can track the origin of data, its ownership, and any subsequent transfers or modifications. This feature enhances data transparency and accountability in IoT and IIoT environments.
- Data Access Controls: Blockchain enables fine-grained access controls to data stored on the blockchain. Access to data can be managed through cryptographic keys and permissioned blockchain

networks, ensuring that only authorized entities can view or modify data. This helps protect data privacy and prevent unauthorized access.

Note that by leveraging blockchain technology, IoT and IIoT systems can benefit from enhanced data integrity, transparency, and auditability. The decentralized and tamper-proof nature of blockchain provides a robust framework for securing and verifying data in IoT and IIoT environments, addressing the challenges of data integrity and auditing.

8.3 AI-Based Data Privacy Protection Techniques for IoT and IIoT Based Environment

AI-based data privacy protection techniques play an important role in safeguarding sensitive information in IoT and IIoT environments. Here are some AI-driven techniques used for data privacy protection:

- Differential Privacy: Differential privacy is a technique that adds noise or randomness to data before it is shared or analyzed. AI algorithms can apply differential privacy mechanisms to IoT and IIoT data, ensuring that individual data points cannot be re-identified, thus protecting privacy while allowing for meaningful analysis.
- Homomorphic Encryption: Homomorphic encryption allows computation on encrypted data without decrypting it. AI algorithms can be designed to perform operations on encrypted IoT data, preserving privacy throughout the data processing pipeline. This technique enables data analysis while keeping sensitive information encrypted.
- Privacy-Preserving Machine Learning: AI algorithms can be used to develop privacy-preserving machine learning models. These models are trained on decentralized or encrypted data, protecting individual data points while still providing accurate predictions. Techniques such as federated learning and secure multiparty computation enable collaborative model training without exposing raw data.
- Anonymization and Pseudonymization: AI techniques can be applied to anonymize or pseudonymize sensitive data in IoT and IIoT environments. This involves removing or obfuscating personally identifiable information (PII) to protect individual privacy. AI algorithms can be used to ensure that anonymization techniques maintain data utility while minimizing the risk of re-identification.
- Contextual Privacy Preservation: AI can be utilized to analyze the context and sensitivity of IoT data to determine appropriate privacy protection measures. By understanding the context in which data is collected and used, AI algorithms can dynamically adjust privacy settings and access controls to protect sensitive information.
- Privacy-Preserving Data Sharing: AI algorithms can facilitate secure and privacy-preserving data sharing in IoT and IIoT environments. Techniques such as secure multi-party computation and secure data federations enable collaboration while maintaining data privacy. AI can also enforce data usage policies, ensuring that shared data is only used for authorized purposes.
- Adversarial Robustness: AI techniques can be employed to enhance the robustness of IoT and IIoT systems against adversarial attacks. By training models to detect and mitigate adversarial attacks on IoT data, privacy breaches can be prevented, and the overall security of the system can be improved.

- User-Centric Privacy Control: AI-driven privacy control mechanisms can empower individuals to have more control over their IoT and IIoT data. AI algorithms can enable personalized privacy settings, allowing users to specify their privacy preferences and consent to data collection and usage. This puts individuals in control of their data and ensures compliance with privacy regulations.

Note that by leveraging AI-based data privacy protection techniques, IoT and IIoT systems can achieve a balance between data utility and privacy preservation. These techniques enable organizations to extract valuable insights from IoT data while ensuring the confidentiality and integrity of sensitive information.

9. BLOCKCHAIN AND AI FOR INCIDENT RESPONSE AND FORENSICS

9.1 Blockchain and AI Based Incident Detection and Response for IoT and IIoT based Environment

Blockchain and AI can be combined to enhance incident detection and response in IoT and IIoT environments. Here's how blockchain and AI can be leveraged for incident detection and response:

- Immutable Event Logging: Blockchain's immutable nature can be used to create a tamper-proof and transparent log of IoT and IIoT events. Each event or data transaction can be recorded on the blockchain, providing an audit trail that cannot be altered. This ensures the integrity of incident-related data and allows for reliable incident detection.
- Anomaly Detection: AI algorithms can analyze IoT and IIoT data to detect anomalies or deviations from normal behavior. By training machine learning models on historical data, AI can learn patterns and identify abnormal activities or events. This enables the early detection of potential incidents or security breaches in real-time.
- Threat Intelligence Sharing: Blockchain provides a decentralized and secure platform for sharing threat intelligence data among IoT and IIoT devices and systems. AI algorithms can analyze and correlate threat intelligence from various sources to identify emerging threats and vulnerabilities. This shared intelligence can help prevent incidents and enhance response capabilities.
- Real-time Monitoring and Alerts: AI can continuously monitor IoT and IIoT systems, analyzing data in real-time to identify potential incidents. By leveraging machine learning algorithms, AI can detect anomalies, suspicious patterns, or unauthorized activities and generate timely alerts to enable quick incident response.
- Incident Response Automation: AI can automate incident response processes in IoT and IIoT environments. Machine learning algorithms can be trained to classify and prioritize incidents based on their severity, enabling automated response actions. This can include isolating affected devices, applying security patches, or triggering alerts to security teams for further investigation.
- Decentralized Incident Management: Blockchain's decentralized nature allows for distributed incident management in IoT and IIoT environments. Incident-related information, such as event logs, response actions, and remediation steps, can be securely stored and shared across the blockchain network. This ensures that incident information is accessible to authorized parties and prevents single points of failure.

- Forensic Analysis: Blockchain's immutable and transparent nature can facilitate forensic analysis in the event of a security incident. The recorded data on the blockchain can serve as a reliable source for post-incident investigations and forensics. AI algorithms can analyze this data to reconstruct the sequence of events, identify the root cause, and gather evidence for remediation and legal purposes.

Note that by combining the strengths of blockchain and AI, IoT and IIoT environments can benefit from improved incident detection, faster response times, and enhanced overall security. The tamper-proof and decentralized nature of blockchain, along with the intelligence of AI algorithms, provides a robust framework for incident detection and response in the IoT and IIoT domain.

9.2 Forensic Analysis Using Blockchain and AI for IoT and IIoT Based Environment

Forensic analysis using blockchain and AI in IoT and IIoT environments can help investigate security incidents, gather evidence, and reconstruct the sequence of events. Here's how blockchain and AI can be leveraged for forensic analysis:

- Immutable and Transparent Data Storage: Blockchain's immutable nature ensures that once data is recorded on the blockchain, it cannot be altered or tampered with. This characteristic is important for preserving the integrity of forensic evidence. IoT and IIoT data, such as device logs, sensor readings, or transaction records, can be stored on the blockchain, providing a trustworthy source of evidence for forensic analysis.
- Chain of Custody: Blockchain can establish a chain of custody for forensic evidence in IoT and IIoT environments. Each transaction or event recorded on the blockchain includes a timestamp, cryptographic hash, and information about the parties involved. This creates an auditable trail of custody, ensuring the integrity and authenticity of the evidence throughout the investigation process.
- Data Attribution and Ownership: Blockchain can assist in identifying the source and ownership of IoT and IIoT data. By leveraging blockchain's decentralized architecture, AI algorithms can analyze the blockchain to trace the origin of data, identify the devices or systems responsible for generating it, and determine the ownership of the data. This information is essential for forensic investigations and establishing accountability.
- Reconstruction of Events: AI algorithms can analyze the data recorded on the blockchain to reconstruct the sequence of events leading up to a security incident. By correlating various data points, such as device logs, sensor readings, and transaction records, AI can identify the activities and interactions that occurred before, during, and after the incident. This helps investigators understand the timeline, identify potential causes, and uncover the tactics used by malicious actors.
- Pattern Recognition and Anomaly Detection: AI algorithms can leverage machine learning techniques to analyze patterns and detect anomalies in IoT and IIoT data. By comparing the current data with historical records, AI can identify abnormal behaviors, suspicious patterns, or deviations from normal operations. This aids in identifying potential security incidents and understanding the impact and scope of the incident.

- Collaborative Investigation: Blockchain's decentralized and transparent nature enables collaborative forensic analysis in IoT and IIoT environments. Multiple parties, such as investigators, analysts, or legal authorities, can access the blockchain to review and contribute to the investigation. This fosters transparency, information sharing, and coordination among stakeholders, enhancing the effectiveness of the forensic analysis process.
- Privacy-Preserving Analysis: AI algorithms can be designed to perform forensic analysis while preserving the privacy of individuals or sensitive information. Techniques such as federated learning or secure multi-party computation allow AI models to be trained on decentralized or encrypted data, ensuring that privacy is maintained during the analysis process.

Hence, by combining the immutability of blockchain with the intelligence of AI algorithms, forensic analysis in IoT and IIoT environments can become more reliable, transparent, and efficient. The integration of blockchain and AI ensures the integrity of evidence, enables thorough reconstruction of events, and supports collaborative investigation efforts, leading to effective forensic analysis in IoT and IIoT-based environments.

10. FUTURE DIRECTIONS AND CHALLENGES

10.1 Emerging Trends and Technologies for Blockchain: AI – IoT-IIoT Based Environment

The convergence of blockchain, AI, IoT, and IIoT is driving several emerging trends and technologies that hold great potential for enhancing security, efficiency, and scalability in various domains. Here are some notable trends and technologies in the blockchain-AI-IoT-IIoT-based environment:

A. Edge Computing:
   - Edge AI: Edge computing combined with AI allows for real-time data processing and decision-making at the edge devices, reducing latency and improving efficiency.
   - Edge Blockchain: Deploying blockchain technology at the edge devices enables distributed consensus and local data storage, enhancing security and privacy in IoT and IIoT applications.

B. Federated Learning:
   - Federated AI: Federated learning enables training AI models across multiple edge devices while preserving data privacy. It facilitates collaborative and decentralized AI training in IoT and IIoT environments.
   - Interoperability and Standardization:
   - Blockchain Interoperability: Efforts are underway to establish interoperability protocols and standards to enable seamless communication and data exchange between different blockchain networks.
   - IoT Standardization: Organizations are working towards developing common standards and protocols to ensure interoperability among IoT devices and platforms.

C. Hybrid Blockchain:

- ◦ Public-Private Hybrid Blockchain: Hybrid blockchain architectures combine the benefits of both public and private blockchains, offering scalability, privacy, and decentralized governance for IoT and IIoT applications.

D. Secure Hardware:
- ◦ Trusted Execution Environment (TEE): TEEs provide secure hardware environments for executing sensitive operations and protecting cryptographic keys, enhancing the security of IoT and IIoT devices.
- ◦ Hardware Security Modules (HSMs): HSMs offer secure key storage and cryptographic operations, ensuring the integrity and confidentiality of data in IoT and IIoT deployments.

E. Data Marketplace:
- ◦ Blockchain-based Data Marketplace: Decentralized data marketplaces built on blockchain enable secure and transparent data exchange, allowing individuals and organizations to monetize and trade their IoT and IIoT data.

F. AI-powered Blockchain Analytics:
- ◦ AI-driven Blockchain Analytics: AI techniques, such as machine learning and natural language processing, are employed to analyze blockchain data and detect patterns, anomalies, and potential security threats.

G. Self-Sovereign Identity (SSI):
- ◦ SSI on Blockchain: Self-sovereign identity solutions leverage blockchain to enable individuals to have control over their digital identities, enhancing privacy and security in IoT and IIoT ecosystems.

H. Quantum-Resistant Cryptography:
- ◦ Post-Quantum Cryptography: With the advent of quantum computing, post-quantum cryptography algorithms are being explored to ensure long-term security for blockchain and IoT systems against quantum attacks.

I. Energy Efficiency:
- ◦ Green Blockchain: Efforts are being made to develop energy-efficient consensus algorithms and sustainable blockchain infrastructure to minimize the environmental impact of blockchain-based systems.

These emerging trends and technologies demonstrate the continuous evolution and integration of blockchain, AI, IoT, and IIoT, creating new opportunities and addressing existing challenges in various industries. As these technologies mature, they have the potential to revolutionize multiple domains, including healthcare, supply chain, finance, energy, and smart cities, leading to increased efficiency, transparency, and security in the digital era.

10.2 Research Opportunities and Open Challenges for Blockchain: AI – IoT-IIoT Based Environment

The intersection of blockchain, AI, IoT, and IIoT presents numerous research opportunities and open challenges. Here are some areas where further exploration and innovation are needed:

A. Scalability and Performance:
   ◦ Scalable Blockchain Solutions: Developing scalable blockchain architectures and consensus mechanisms to handle the increasing volume of IoT and IIoT data and transactions.
   ◦ Efficient AI and ML Algorithms: Designing lightweight and resource-efficient AI and ML algorithms that can run on resource-constrained IoT and IIoT devices without compromising performance.

B. Privacy and Data Protection:
   ◦ Privacy-Preserving Techniques: Investigating techniques for preserving the privacy of IoT and IIoT data while still enabling secure and efficient data sharing and analysis.
   ◦ Differential Privacy: Exploring the application of differential privacy mechanisms to protect sensitive information in IoT and IIoT environments.

C. Trust and Security:
   ◦ Trust Management Systems: Developing trust management frameworks and reputation systems to establish trustworthiness among IoT and IIoT devices and participants.
   ◦ Security Auditing and Certification: Investigating mechanisms to audit and certify the security of blockchain, AI, and IoT systems to ensure their resilience against cyber threats.
   ◦ Interoperability and Standardization:
   ◦ Cross-Platform Interoperability: Developing standards and protocols to enable seamless integration and interoperability between different blockchain networks, AI systems, and IoT platforms.
   ◦ Data and Device Interoperability: Addressing challenges related to data format, semantic interoperability, and device heterogeneity in IoT and IIoT environments.

D. Energy Efficiency:
   ◦ Green Blockchain Solutions: Exploring energy-efficient consensus algorithms and sustainable blockchain infrastructures to minimize the energy consumption of blockchain-based systems.
   ◦ AI for Energy Optimization: Utilizing AI techniques to optimize energy usage in IoT and IIoT deployments, leading to more energy-efficient operations.

E. Governance and Legal issues:
   ◦ Legal and Regulatory Frameworks: Examining the legal implications and regulatory requirements associated with the use of blockchain, AI, IoT, and IIoT technologies, especially in sensitive domains.
   ◦ Governance Models: Designing governance models and frameworks to ensure transparency, accountability, and fair participation in blockchain-based ecosystems.

Hence, these research opportunities and challenges highlight the multidisciplinary nature of blockchain-AI-IoT-IIoT-based environments and call for collaboration between researchers, industry practitioners, policymakers, and other stakeholders. By addressing these open issues, researchers can contribute to the advancement of these technologies and drive innovation that enables secure, efficient, and responsible applications in various domains.

11. CONCLUSION

The combination of blockchain, AI, IoT, and IIoT offers tremendous potential for enhancing cybersecurity in today's interconnected world. This convergence of technologies provides innovative solutions to address the complex security challenges associated with IoT and IIoT applications. Blockchain technology offers decentralized and immutable data storage, enhancing the security and integrity of IoT and IIoT data. It enables secure transactions, data sharing, and identity management, reducing vulnerabilities and ensuring trust among participants. The transparency and auditability of blockchain also facilitate incident detection, response, and forensic analysis. AI, with its advanced algorithms and machine learning capabilities, plays an essential role in cybersecurity. It enables efficient threat detection, anomaly detection, and predictive analytics, enhancing the detection and prevention of cyberattacks in real-time. AI-driven algorithms can identify patterns and anomalies in large-scale IoT and IIoT data, enabling proactive measures to mitigate potential security risks.

Hence, this chapter provides the detail explanation of the integration of blockchain, AI, and IoT/IIoT applications, with introducing a new paradigm of cybersecurity for future researchers/ scientific community. It strengthens the protection of sensitive data, safeguards critical infrastructures, and enhances the resilience of IoT and IIoT ecosystems against cyber threats. By leveraging the power of distributed ledger technology and intelligent algorithms, organizations can achieve secure and reliable communication, data integrity, access control, and incident response.

REFERENCES

Agrawal, D., Bansal, R., Fernandez, T. F., & Tyagi, A. K. (2022). Blockchain Integrated Machine Learning for Training Autonomous Cars. In Lecture Notes in Networks and Systems, (vol 420). Springer, Cham. doi:10.1007/978-3-030-96305-7_4

Aljawarneh, S., Aldwairi, M., & Jararweh, Y. (2020). Blockchain-based Framework for Securing IoT Applications. *Journal of Ambient Intelligence and Humanized Computing*, *11*(4), 1629–1641.

Aswathy, S. U. (2021). The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities and Challenges. Recent Trends in Blockchain for Information Systems Security and Privacy. CRC Press.

Biswas, K., & Koo, S. (2020). Blockchain-Based Security Framework for Industrial IoT Systems. *Future Generation Computer Systems*, *104*, 962–975.

Dagher, G. G., Mohler, J., Milojkovic, M., Marella, P. B., & Ancile, C. (2018). Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. *Sustainable Cities and Society*, *39*, 283–297. doi:10.1016/j.scs.2018.02.014

Deshmukh, A., Patil, D., & Tyagi, A. K. (2022). Recent Trends on Blockchain for Internet of Things based Applications: Open Issues and Future Trends. In *Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing (IC3-2022).* Association for Computing Machinery. 10.1145/3549206.3549289

Deshmukh, A., Sreenath, N., Tyagi, A. K., & Eswara Abhichandan, U. V. (2022). Blockchain Enabled Cyber Security: A Comprehensive Survey. *2022 International Conference on Computer Communication and Informatics (ICCCI),* (pp. 1-6). IEEE. 10.1109/ICCCI54379.2022.9740843

Ding, S., Shao, Z., Guo, S., & Zhu, W. (2019). IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? *IEEE Consumer Electronics Magazine*, *8*(4), 22–30.

Fan, K., & Xu, H. (2019). Blockchain and Artificial Intelligence: Revolutionizing Cybersecurity and Cyberdefense. *IEEE Intelligent Systems*, *34*(6), 92–96.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 154076–154130.

Gupta, V., & Sehgal, V. (2019). Blockchain and Artificial Intelligence for Secure and Privacy-Preserving Industrial IoT. *Future Generation Computer Systems*, *97*, 624–637.

Jayaprakash, V., & Tyagi, A. K. (2022). Security Optimization of Resource-Constrained Internet of Healthcare Things (IoHT) Devices Using Asymmetric Cryptography for Blockchain Network. In: Giri, D., Mandal, J.K., Sakurai, K., De, D. (eds) *Proceedings of International Conference on Network Security and Blockchain Technology.* Springer, Singapore. 10.1007/978-981-19-3182-6_18

Krishna, A. M., & Tyagi, A. K. (2020). Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology. *2020 International Conference on Emerging Trends in Information Technology and Engineering*. IEEE. 10.1109/ic-ETITE47903.2020.332

Mishra, S., & Tyagi, A. K. (2019). Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technology. *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),* (pp. 123-128). IEEE. 10.1109/I-SMAC47947.2019.9032557

Nair, M. M., & Tyagi, A. K. (2022). Preserving Privacy Using Blockchain Technology in Autonomous Vehicles. In: Giri, D., Mandal, J.K., Sakurai, K., De, D. (eds) *Proceedings of International Conference on Network Security and Blockchain Technology*. Springer, Singapore. 10.1007/978-981-19-3182-6_19

Nair, M. M., & Tyagi, A. K. (2023). Chapter 11 - AI, IoT, blockchain, and cloud computing: The necessity of the future. In Rajiv Pandey, Sam Goundar, Shahnaz Fatima (eds.), Distributed Computing to Blockchain. Academic Press. doi:10.1016/B978-0-323-96146-2.00001-2

Pandey, A. A., Fernandez, T. F., Bansal, R., & Tyagi, A. K. (2022). Maintaining Scalability in Blockchain. In A. Abraham, N. Gandhi, T. Hanne, T. P. Hong, T. Nogueira Rios, & W. Ding (Eds.), *Intelligent Systems Design and Applications. ISDA 2021. Lecture Notes in Networks and Systems* (Vol. 418). Springer. doi:10.1007/978-3-030-96308-8_4

Puthal, D., Nepal, S., Ranjan, R., Chen, J., & Mohanty, S. P. (2019). The Blockchain as a Decentralized Security Framework [Guest Editorial]. *IEEE Cloud Computing*, *6*(1), 16–21.

Raza, S., Wallgren, L., & Voigt, T. (2017). Edge Computing for Industry 4.0: Scenarios and Challenges. *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS),* (pp. 1451-1456). IEEE.

Samaniego, M., & Yang, B. (2020). A Survey on Blockchain Technology for Networking and Communications: Challenges and Opportunities. *IEEE Communications Surveys and Tutorials*, *22*(1), 713–734.

Sheth, H. S. K. (2022). Deep Learning, Blockchain based Multi-layered Authentication and Security Architectures. *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC),* (pp. 476-485). IEEE. 10.1109/ICAAIC53929.2022.9793179

Siddharth, M. (2021). Issues and Challenges (Privacy, Security, and Trust) in Blockchain-Based Applications, In: Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles. IGI Global. doi:10.4018/978-1-7998-3295-9.ch012

Suryadevara, N. K., & Mukhopadhyay, S. C. (2018). Wireless Sensor Network Based Industrial Monitoring Applications: A Comprehensive Survey. *IEEE Communications Surveys and Tutorials*, *20*(2), 1403–1427.

Tibrewal, I., Srivastava, M., & Tyagi, A. K. (2022). Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks. In A. K. Tyagi, A. Abraham, & A. Kaklauskas (Eds.), *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*. Springer. doi:10.1007/978-981-16-6542-4_17

Tyagi, A. (2021a). Applications of Blockchain Technologies in Digital Forensic and Threat Hunting. Recent Trends in Blockchain for Information Systems Security and Privacy. CRC Press.

Tyagi, A. (2021b). Analysis of Security and Privacy Aspects of Blockchain Technologies from Smart Era' Perspective: The Challenges and a Way Forward. In Recent Trends in Blockchain for Information Systems Security and Privacy. CRC Press.

Tyagi, A. (2021c, October). AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology. *IJIN*, *2*, 175–183.

Tyagi, A. (2022a). Preserving Privacy using Distributed Ledger Technology in Intelligent Transportation System. In *Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing (IC3-2022)*. Association for Computing Machinery. 10.1145/3549206.3549306

Tyagi, A. K. (2022b). SecVT: Securing the Vehicles of Tomorrow Using Blockchain Technology. In A. A. Sk, T. Turki, T. K. Ghosh, S. Joardar, & S. Barman (Eds.), *Artificial Intelligence. ISAI 2022. Communications in Computer and Information Science* (Vol. 1695). Springer. doi:10.1109/ICCCI54379.2022.9740965

Tyagi, A. (2023). Decentralized everything: Practical use of blockchain technology in future applications. In Rajiv Pandey, Sam Goundar, Shahnaz Fatima, (eds.) Distributed Computing to Blockchain. Academic Press. doi:10.1016/B978-0-323-96146-2.00010-3

Tyagi, A. K., Agarwal, D., & Sreenath, N. (2022). SecVT: Securing the Vehicles of Tomorrow using Blockchain Technology. *2022 International Conference on Computer Communication and Informatics (ICCCI),* (pp. 1-6). IEEE. 10.1109/ICCCI54379.2022.9740965

Tyagi, A. K., Chandrasekaran, S., & Sreenath, N. (2022). Blockchain Technology:– A New Technology for Creating Distributed and Trusted Computing Environment. *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC),* (pp. 1348-1354). IEEE. 10.1109/ICAAIC53929.2022.9792702

Tyagi, A. K., Fernandez, T. F., & Aswathy, S. U. (2020). Blockchain and Aadhaar based Electronic Voting System. *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore*, (pp. 498-504). IEEE. 10.1109/ICECA49313.2020.9297655

Tyagi, A. & Kumar, S. (2022). Blockchain Technology for Securing Internet of Vehicle: Issues and Challenges. *2022 International Conference on Computer Communication and Informatics (ICCCI),* (pp. 1-6). IEEE. 10.1109/ICCCI54379.2022.9740856

Varsha, R. (2020, January 1). 'Deep Learning Based Blockchain Solution for Preserving Privacy in Future Vehicles'. *International Journal of Hybrid Intelligent Systems*, *16*(4), 223–236.

Varsha, J. & Tyagi, A. (2022). Security Optimization of Resource-Constrained Internet of Healthcare Things (IoHT) Devices Using Lightweight Cryptography. Information Security Practices for the Internet of Things, 5G, and Next-Generation Wireless Networks. IGI Global. doi:10.4018/978-1-6684-3921-0.ch009

Wang, Y., Kumar, N., Singh, R., & Alowaisheq, E. (2018). Secure Data Sharing Framework for Industrial IoT Using Blockchain and Attribute-Based Encryption. *IEEE Transactions on Industrial Informatics*, *14*(5), 2038–2046.

Xu, L. D., He, W., & Li, S. (2018). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*, *10*(4), 2233–2243. doi:10.1109/TII.2014.2300753

Yang, Z., Wu, S., Ning, H., & Lu, R. (2019). A Blockchain-Based Access Control Framework for Industrial IoT. *IEEE Transactions on Industrial Informatics*, *15*(1), 471–480.

Ylianttila, M., & Vasilakos, A. V. (2017). Security in Industrial IoT Networks: Approaches and Challenges. *IEEE Network*, *31*(3), 82–88.