Enhancing IIOT security using ML with Blockchain technology

Amit Raheja, Anu Tonk
Department of Multidisciplinary Engineering, The NorthCap University, Gurgaon, Haryana

Abstract: **The Internet of Things (IoT) brings significant commercial, financial, and societal implications for the way we live. Contributing nodes in these networks of the IoT setting are resource-restricted, making them susceptible to web-oriented attacks. In this work, significant attempts were undertaken to solve issues related to privacy and security in IoT networks, mostly using classic cryptographic algorithms. Nevertheless, the distinctive features of nodes in the IoT make current approaches in the literature to be inadequate to cover all aspects of the security spectrum of networks of the IoT setting. In this work, a cutting-edge, secure, and privacy-preserving framework tailored for machine learning models within the Industrial Internet of Things (IIoT) ecosystem, is implemented. The proposed solution synergizes four integral components: Distributed Entity/Branch (DISTEN) for robust model encryption, Central Authority/Coordinating Server (CENTAUTH) for comprehensive key management, the Interplanetary File System (IPFS) for scalable and efficient model storage, and the Ethereum Blockchain (ETHBC) for the immutable recording of transactions and verification of hashcodes. This innovative framework focuses on encrypting ML models using AES symmetric keys generated by CENTAUTH. Finally, we present the validation of the performance prospects of our IIOT security paradigm using ML with Blockchain technology.**

Keywords: **Industrial Internet of Things; Blockchain; Machine Learning; Central Authority/Coordinating Server; Interplanetary File System; and Ethereum Blockchain.**

1. INTRODUCTION

Over the course of the current era of digital transformation, the incorporation of machine learning (ML) and deep learning algorithms into the Industrial Internet of Things (IIoT) has emerged as a fundamental component for innovation in a variety of fields, including healthcare, manufacturing, transportation, and smart cities. This growth has occurred as a result of the fact that these algorithms have become increasingly sophisticated. The evolution of industrial practices towards more data-driven and intelligent systems is facilitated by these technologies, which are lauded for their ability to improve operational efficiency and promote predictive analytics Khattab & Youssry (2020). These technologies play a significant part in the development of industrial practices. When these algorithms are used to handle more sensitive information, on the other hand, it results in the introduction of new vulnerabilities and privacy concerns. This is particularly true in businesses where the significance of data sensitivity cannot be exaggerated. According to the findings of a study that was conducted by Hussain et al. (2020), the possibility of unauthorised access or manipulation using machine learning models might potentially result in substantial impacts. These effects could include the disclosure of personal data or the formation of choices that are not correct.

The existing security measures that are in place to safeguard machine learning models often lack comprehensiveness Hussain et al. (2020). This refers to the fact that they are not sufficient to provide adequate protection against the whole spectrum of cyber threats that are prevalent in the modern digital environment. According to Chaabouni et al. (2019), a substantial number of these interventions focus on particular aspects of security, such as the encryption of data or the transfer of models in a secure way. On the other hand, they do not address the full need for a robust framework that ensures the integrity of data, the protection of privacy, and the management of access during the whole lifecycle of machine learning models. This fragmented approach to security highlights the need for an integrated solution that is capable of providing end-to-end protection for machine learning models. This is especially important in the context of the Industrial Internet of Things (IIoT), where the stakes for data privacy and security are elevated to an unusually high level Wu et al. (2021).

Taking into consideration these issues, the solution that has been proposed represents a significant

advancement in terms of safeguarding machine learning models inside the Internet of Things (IoT) Sarker et al. (2022) and Malhotra et al. (2021). The framework offers a defensive mechanism that is both high-quality and composed of several layers. The strength of current encryption, decentralised storage solutions, and the irreversible nature of blockchain technology are all used in order to achieve this goal Politou et al. (2019). This one-of-a-kind method not only lessens the possibility of machine learning models being hacked, but it also addresses issues that are of fundamental importance, such as reducing the amount of space that is necessary for model storage and safeguarding the validity and security of sensitive data Bagaa et al. (2020). In addition, the usage of the Ethereum blockchain for the purpose of access control ushers in a new paradigm in terms of the administration of models that are both secure and transparent. Both dynamic access control and tamper-proof record-keeping are crucial for guaranteeing that data integrity is maintained in applications that are utilised for the Internet of Things Restuccia et al. (2018). This paradigm makes it possible to implement both of these features.

The key highlights of this work are to (i) study the merger of blockchain and machine learning for ensuring secure handling of data within industrial IoT frameworks (2) implement data privacy preservation with IPFS for industrial IoT systems.

This work describes the innovative usage of AES encryption to safeguard the ML models against the access of unauthorized persons. Moreover, this work explains about the IPFS usage which acts provides an effective decentralized storage for large encrypted models. The implementation of Ethereum blockchain framework which gives a secured and transparent access control along with the verification of the integrity are briefed here. Some of the additional advantages possessed by this work are the enhanced security layers, improved effectiveness of the operations and reduced risk of data breaches.

2. BACKGROUND & LITERATURE REVIEW

To ensure the effective implementation of IoT, it is critical to investigate the fundamental causes of issues related to privacy and security. More exactly, the terminology IoT has been hurled from the current techniques; hence, it is vital to determine if the security concerns in IoT are fresh or are an updated version of the legacy from the previous techniques Hussain et al. (2020). In the literatures, there were many works like this. Fernandes et al. (2017) examined the shared characteristics and variations in safety concerns between IoT and conventional IT platforms. They additionally addressed concerns related to confidentiality. Hardware, software, networks, and programs are the primary motivators for arguments over shared and distinct characteristics Hamamreh et al. (2018). According to these categories, safety concerns associated with conventional IT and the IoT share essential commonalities Sfar et al. (2018) and Jing et al. (2014). Nevertheless, the fundamental worry of the IoT is the resource limits that impede the use of previously accessible advanced safety measures in networks of IoT settings Čolaković and Hadžialić (2018). Additionally, remedies for safety and confidentiality challenges in the IoT necessitate cross-level architecture and optimized methodologies.

In essence, we observe convergence of technologies such as machine learning and the IIoT in this new era of technical and societal advancements. Nevertheless, this development is accompanied by a growth in the number of security risks. By offering an integrated solution that incorporates AES encryption, IPFS for decentralized storage, and Ethereum blockchain for access control and integrity verification, the framework creates a new standard for security in the IoT sector. This is accomplished by establishing a new standard. Furthermore, it contributes to the overarching goal of cultivating a digital ecosystem that is trustworthy, efficient, and secure for the future of business Shokri and Shmatikov (2015) and Li et al. (2016). Not only does it improve the safety of machine learning models against unauthorized access and data breaches, but it also adds to the overall objective of providing a digital ecosystem that is safer.

Let us now look at such new era technical and societal advancements proposed by different investigators as literature review below.

Mahalle and Railkar (2022) conducted research that provides an analysis of the challenges that are associated with identity management. For the applications of smart manufacturing, Mrabet et al. (2022) suggested an organized structure combining ML (i.e., Machine Learning) with BCT (i.e.,

Blockchain technology) within the framework of the IIoT. Utilizing Federated Learning (FL), Yazdinejad et al. (2022) developed the Block Hunter threat hunting framework, which automatically searches for threats in IIoT networks based on blockchain technology. With many machine learning models integrated into a federated environment, Block Hunter employs a cluster-based architecture for anomaly identification. As per the research work, Block Hunter was regarded as the first federated threat-hunting methodology for IIoT networks that protects privacy while detecting unusual activity. Zhang et al. (2023) proposed a cloud-edge-end architecture based on blockchain technology and creates a blockchain-based trust mechanism. It achieved device mutual confidence by using PoRep, a proof of replication depending upon branching logic systems. After being broadcast to other nodes, the device data was kept on servers to produce proofs and come to a consensus. Motamarri et al. (2024) To continually monitor and adjust to new threats, the suggested system made use of anomaly detection designs that were trained on past data. The capacity of the IoT network to identify and react instantly to complex intrusion attempts was improved by this dynamic threat detection technique. Hosen et al. (2023) outlined an IPFS-dependent immutable data storage structure, a consortium blockchain, a secure P2P and group communication supporting edge computing architecture for IIoT devices, and a sophisticated threat detection design to safeguard private information and spot cyberattacks. Utilizing revised ECC, PUF, and Lagrange interpolation, a hybrid security technique was used to ensure secure communications. The novel technique known as Deadline Latency Energy was suggested by Lakhan et al. (2022). In this case, many solutions were used to create the Federated Learning method of DLEBAF which was enabled by Blockchain. In the topic of cyber security for IoT and IIoT, Tyagi (2024) offered information about possible synergies between AI and blockchain. It was ideal for protecting sensitive data and transactions since it has properties including data integrity, transparency, and tamper resistance. Kumar et al. (2023) introduced a novel DT model that makes it easier to create a virtual environment in order to mimic and reproduce IIoT security-critical procedures. Ismail et al. (2024) introduced an ISC with BC capabilities that incorporates an ML security model into a multi-layered strategy. To find the lightweight model for cyber-attack detection that is appropriate for deployment in an IIoT context with limited resources, a comparison research and performance analysis of several ML classification approaches were carried out, with an emphasis on supervised methods. Gupta et al. (2022) used an AI model based on long short-term memory on the edge servers to distinguish between malicious and benign message requests from the machines, then routed them to the network of OR (i.e., Onion Routing). A novel P2TIF (i.e., Privacy-Preserved Threat Intelligence Framework) was introduced by Kumar et al. (2022) to safeguard private data and detect cyber threats in IIoT conditions. Mansour (2022) developed the BAC-IDS method, an efficient Blockchain-Assisted Cluster-based Intrusion Detection System for IIoT. The BAC-IDS concept that was suggested focused on grouping IIoT devices to identify intrusions and provide secure data exchange using blockchain technology. Salim et al. (2022) put out a safe Digital Framework with Blockchain support for the early identification of Bot development in a Smart Factory setting. For a collection of edge-layer devices, a DT (i.e., Digital Twin) was created to gather device data and use Deep Learning to examine packet headers for connections with external, distinctive IP addresses that were open. Tang et al. (2022) put out the TrusCL collaborative learning scheme, which was safe and reliable. By carefully balancing HE (i.e., Homomorphic Encryption) and DP (i.e., Differential Privacy), the scheme achieved the trade-off between performance and accuracy while guaranteeing privacy protection. Using blockchain technology, Zhou et al. (2022) created an STFS (i.e., Secure and Trusted Federated) data-sharing system.

3. PROPOSED METHODOLOGY

Through a series of meticulously designed steps that ensure both the integrity and privacy of the model, the methodology that has been outlined provides a comprehensive approach to secure a deep learning model. This is especially true for a model that is based on the Convolutional Neural Network (CNN) architecture and was trained on the MNIST dataset LeCun et al. (2024). In order to get started with the procedure, an existing CNN-based model from MNIST that has been stored in the h5 format must be uploaded. This stage is very important since it is the one that kicks off the process of safe handling by incorporating the model into the suggested security framework itself.

After being successfully uploaded, the model is put through a verification procedure to confirm that it is genuine and has not been altered in any way. This verification serves as a precaution against tampering or corruption, ensures that only legitimate and untampered models move through the subsequent phases of the framework, and prevents any instances of them occurring. After the model has been validated, the production of a central authority key is an essential stage in the technique. The encryption procedure relies heavily on this key, which acts as the cryptographic component that protects the model from being accessed by unauthorised parties. The key that is used by the central authority is built to be resilient and secure, and it makes use of the most advanced cryptographic standards available in order to guarantee the best possible degree of security.

The encryption of the MNIST model is the next step in the process, which comes after the development of the key for the central authority. This encryption is carried out with the help of the Advanced Encryption Standard (AES) algorithm, which is a symmetric encryption method that is well-known for its dependability and broad acceptance in safe data handling methods. By ensuring that the model is made unreadable to anybody who does not hold the associated decryption key, the AES encryption protects the model's confidential and private information.

The next step is to store the encrypted model in the InterPlanetary File System (IPFS), which is the next phase. In order to eliminate the hazards that are associated with centralised data storage, IPFS provides a decentralised storage solution. This is accomplished by dispersing the storage among a large number of nodes. This not only increases accessibility and redundancy, but it also strengthens the model's security by reducing the number of major points of failure. The generation of a one-of-a-kind hash code that represents the model's position inside IPFS occurs when the model is stored in IPFS. It is essential to have this hash code in order to retrieve the model for usage in the future while preserving the confidentiality and authenticity of the data that has been saved.

After then, the hash code that was formed is recorded on a blockchain so that the security measures may be strengthened even more. This stage makes use of the inherent security properties of blockchain technology, such as immutability and transparency, in order to record the hash code in a safe manner. By storing the hash code in a blockchain, it is possible to verify that each access or retrieval of the model can be tracked and confirmed. This provides an extra degree of security and accountability to the process.

In the end, the technique reaches its zenith with the decryption of the model for the purpose for which it was designed, which in this instance is digit categorization. The AES algorithm is used during the decryption process, which is similar to the encryption procedure but is carried out in reverse. Decrypting the model needs the central authority key, which ensures that only authorised users who have access to the key may unlock and use the model. This step is required in order to decrypt the model. The successful decryption of the model signifies the conclusion of the secure handling procedure, which in turn makes the model suitable for use in the process of completing concerned jobs on the MNIST dataset Sid (2024).

A thorough and secure strategy to managing deep learning models is provided by the framework via this extensive methodology. This technique goes from uploading and encrypting the models to storing them and eventually decrypting them for usage. This approach guarantees that the highest standards of data integrity and privacy are maintained throughout the whole process.

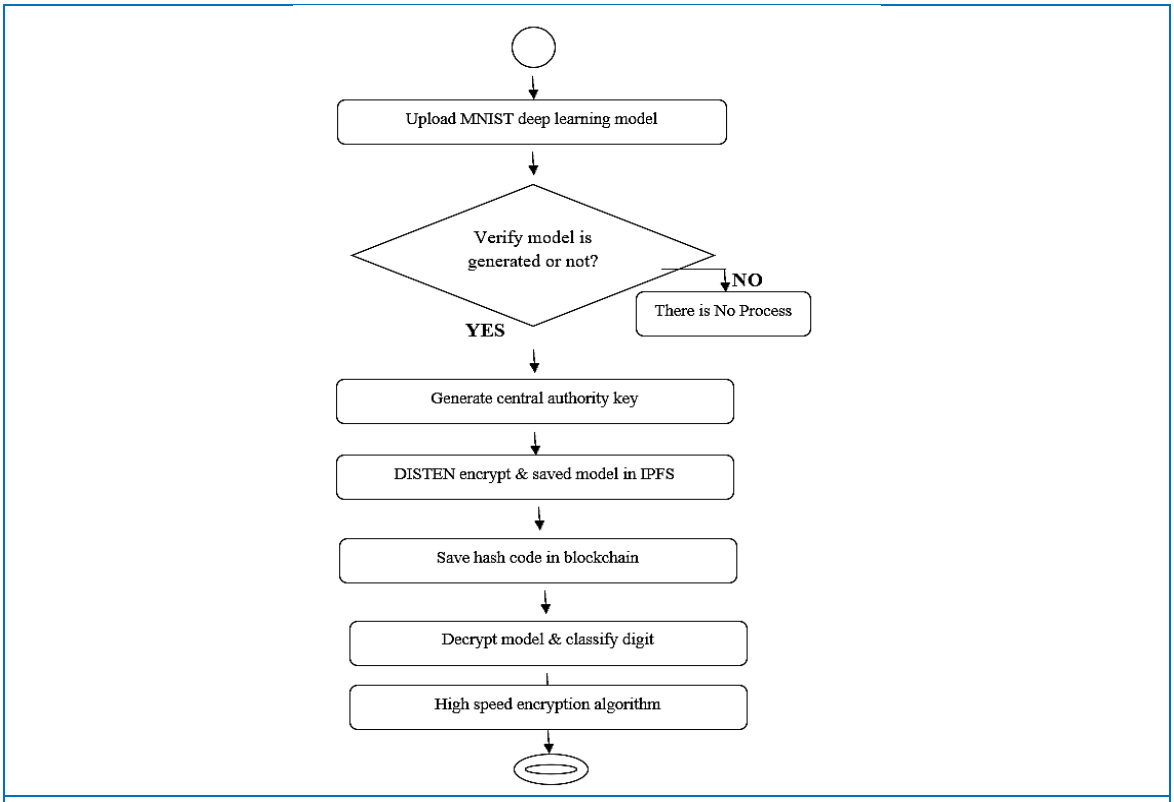

Fig. 1 Methodology Flow Diagram

Fig. 1 is a flowchart that illustrates the manner in which a deep learning model, more especially one that has been trained on the MNIST dataset, may be managed in a safe manner. Putting the MNIST deep learning model onto the cloud is the first stage in the process. Immediately after this, there is a verification process that is performed to determine whether or not the model has been produced correctly. A key for the central authority is generated if the model is successful in passing this verification. The second encryption stage, in which the Distributed Entity/Branch (DISTEN) encrypts the model before it is stored in the IPFS, which is a peer-to-peer network for storing and sharing data, requires this key in order to function properly. Following the completion of the encryption and storage processes, a hash code that is representative of the model is created and then stored on the blockchain. This offers an unchangeable record and guarantees that the model's storage location is not compromised. The last phases entail applying a high-speed encryption technique and decrypting the model when it is required for digit classification. This is likely an indication of how effective the encryption procedure that is used within this approach is. From the moment the model is uploaded until the time it is finally put to use, this whole procedure guarantees that it will be handled in a safe manner.

4. TECHNIQUES

The proposed solution involves the development of a trustworthy and privacy-preserving framework for machine learning models. This framework comprises four key components.

DISTEN: This component focuses on encrypting the ML or deep learning model, a process akin to Federated Learning. It involves multiple model owners encrypting their models using a symmetric AES encryption key, which is generated by a Central Authority or Coordinating Server (CENTAUTH).

CENTAUTH: It is responsible for generating encryption keys distributed to the DISTEN module. With these keys, the DISTEN module encrypts the ML model, ensuring that only authorized users can decrypt and access the model, thereby safeguarding against unauthorized access and data breaches.

*IPFS :G*iven the substantial size of encrypted models, storing them on traditional blockchain platforms like Ethereum is impractical. Instead, the encrypted model is stored on an IPFS server, which provides a HASHCODE indicating the model's storage location. This HASHCODE enables the secure downloading of the model from IPFS without direct storage on the blockchain.

ETHBC: Ethereum Blockchain (ETHBC): This component is utilized to store the HASHCODE

generated by IPFS in the Ethereum blockchain. The blockchain employs a Merkle tree structure, where each node is associated with a unique hashcode. Before storing a new hashcode, the blockchain verifies all transaction hashcodes to ensure data integrity and security. This verification process effectively prevents unauthorized access to the ML model.

5. PROSPECTS OF SECURITY IN IIOT SYSTEMS

When applied to genuine machine learning models, the framework has been shown to produce successful results when it is implemented in the real world. It has been proved that enhanced security may be achieved through the utilisation of powerful encryption and the verification processes that are generated by blockchain technology. In addition, there have been observable improvements in the efficiency of model storage and access, which have contributed to the smoother functioning of IIoT processes.

These findings not only provide evidence that the framework is useful in its current configuration, but they also clear the way for further research endeavours to be undertaken in the future. There is a clear possibility that the capabilities of the framework might be expanded, and that new applications within the realm of IIoT security could be investigated. This would mean that there would be opportunities for additional developments and improvements in this quickly developing industry. Fig. 2 shows pie chart on security measures. The distribution of different security technologies used in IIoT systems is shown visually in Fig. 2. With 40% of the technologies deployed, the pie chart shows that the most popular security measure is advanced encryption. This emphasises how important strong encryption techniques are for safeguarding private business information. With 30% of the market, blockchain implementation demonstrates how widely used it is becoming owing to its advantages in guaranteeing data integrity and traceability. Twenty percent of the security infrastructure is made up of decentralised storage, mostly from solutions like the IPFS, which highlights how important it is to address the vulnerabilities that come with centralised storage systems. Though they are becoming less common as more sophisticated technologies gain popularity, traditional security methods still account for 10% of the market, suggesting that older security techniques are still in use. The continuous shift in IIoT environments towards increasingly complex, layered security systems is illustrated in this graphic.

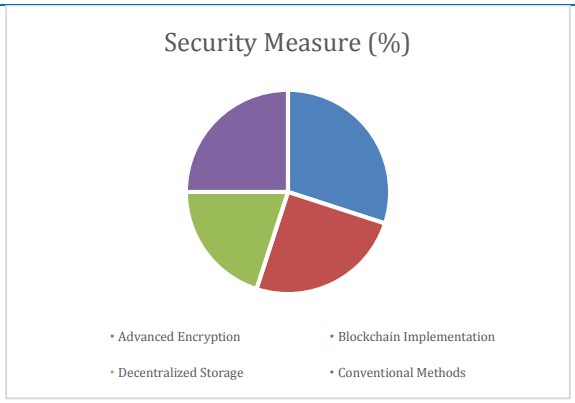

Fig. 2 Utilization of Security Technologies in IIoT Systems

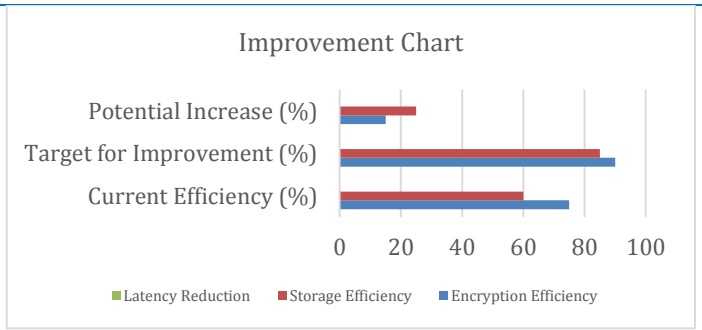

Fig. 3 Utilization of Security Technologies in IIoT Systems

The current efficiency levels of several security components in IIoT systems are outlined in Fig. 3, which is a bar chart. Additionally, targets for future improvements are included in this fig. The efficiency of encryption, the efficiency of storage, and the reduction of latency are highlighted as three of the most important aspects. Currently, the efficiency of encryption is at 75%, and the goal is to enhance it to 90% in the near future. The possibility of this growth highlights the necessity of developing more powerful encryption methods that are capable of further protecting data against rapidly increasing cyber threats. The storage efficiency is now at sixty percent, and the aim for improvement is eighty-five percent. With this information, it is clear that there is a requirement for storage solutions that are both more scalable and more resilient. This might be accomplished by boosting the adoption of decentralized storage systems. Last but not least, the chart discusses latency, which is now average 20 seconds and has a goal improvement of about 50%. Latency reduction is essential for improving the responsiveness of IIoT systems, which is essential for applications that require real-time monitoring and control. This bar chart does an excellent job of illustrating all of the areas in which innovations are required to meet the ever-increasing security requirements of IIoT systems.

6. COMPARATIVE STUDY AND OVERVIEW OF LIMITATIONS ENCOUNTERED

Comparative study

In the below table 1, we have presented the comparison of proposed security framework Vs existing IoT security solutions in the tabular form.

Table 1 Comparison of Proposed Security Framework Vs existing IoT Security Solutions

Security Solutions		Strength	Weakness	Unique Features
Recent IoT security solutions	Kaushik et al. (2023)	This IoT security framework was well-performing in means of security aspect, computational pace, size of ciphertext, size of key, and speed.	It lacked performance in means of delay, overheads concerning transmission, communication, and computation, and didn't consider scalability of the solution offered.	Their framework facilitated relatively lower consumption of memory and considerably quicker operation.
	Zhao et al. (2023)	This IoT security framework was well-performing in means of security aspect, computational pace, size of key, and overheads concerning transmission, communication, and computation.	It lacked performance in means of delay, speed, size of ciphertext, and didn't consider scalability of the solution offered.	This framework lowered the time taken for the exchange of keys.
	Tamizhselvan (2022)	This IoT security framework was well-performing in means of security aspect, computational pace, computational overhead, size of key, and delay.	It lacked performance in means of speed, transmission overhead, size of ciphertext, and communication overhead, and	The framework facilitated incorporated both the key administration and certificate authority.

			didn't consider scalability of the solution offered.	
Proposed Security Framework	Ours	Our security framework consisting of four components has better scalability prospects by being able to handle large-scale applications effectively without much struggles irrespective of what the demand is.	-	We used four components, namely, DISTEN, CENTAUTH, IPFS, and ETHBC in this blockchain-based IoT security framework.

Limitations of classic cryptographic algorithms in IoT context

In the below table 2, we have presented the common limitations observed in cryptographic algorithms in the tabular form.

Table 2 Common Limitations observed in Cryptographic Algorithms

Classic Cryptographic Investigation	Common Limitations			
	Trust	Integrity	Authentication	Cost
Wei et al. (2019)	✓			
Zafar et al. (2022)	✓			
Zhong et al. (2019)		✓		
Da et al. (2021)		✓	✓	
Singh et al. (2021)			✓	
Majeed et al. (2021)			✓	
Pahl et al. (2018)				✓
Tsang et al. (2021)				✓
Xie et al. (2019)				✓

7. RESULTS AND DISCUSSIONS

On the day of the beam test, the respective control cylinders were capped and tested in compression to determine the compressive strength of concrete. The average values of the 56-day compressive strengths are 69.2 and 68.7 MPa for Series V and S specimens, respectively. The results indicate that although the two mix designs were different, they had similar compressive strengths.

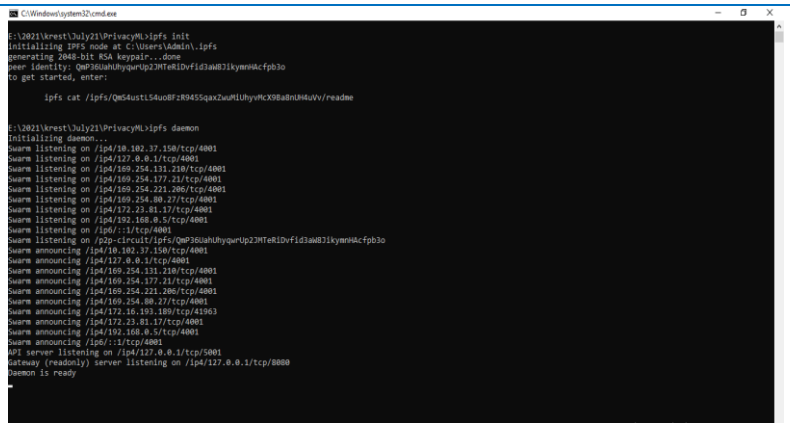

Fig. 4 IPFS Server Daemon Ready

In Fig. 4, the IPFS Server Daemon Ready (IPFS Server Loading) is shown in the form of screenshot.

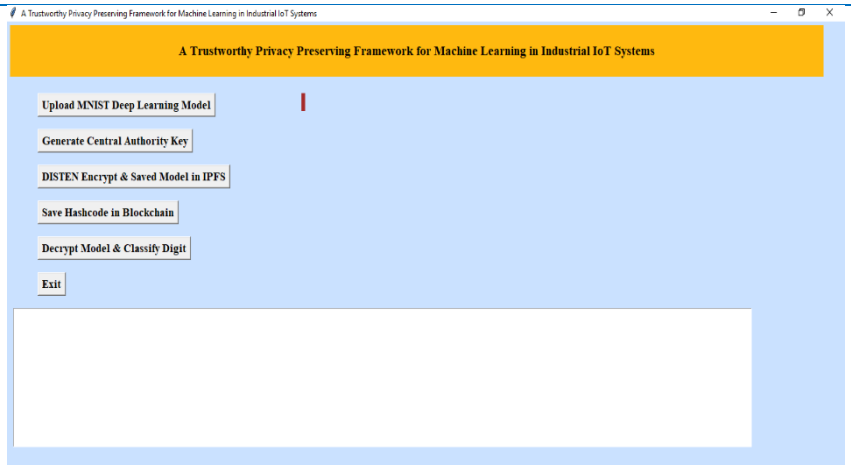

Fig. 5 Simulation GUI

In Fig. 5, the GUI simulation is shown in the form of screenshot.

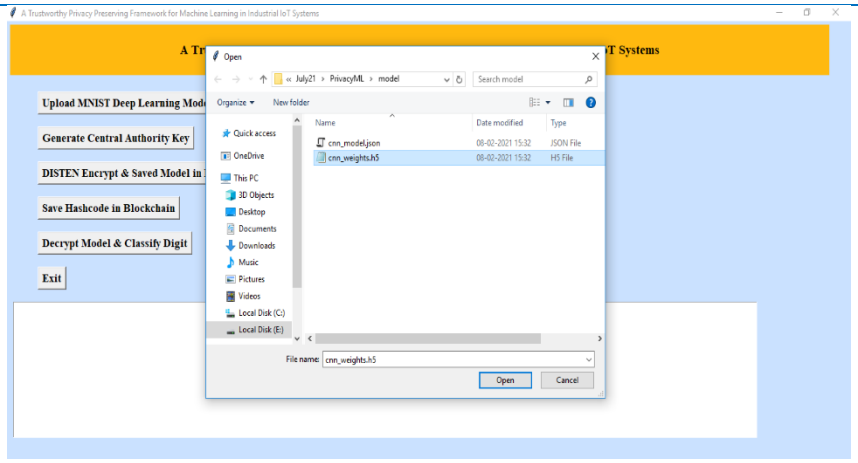

Fig. 6 Uploading Model

The uploading of the model is shown in the above Fig. 6. Here, uploading ‘cnn_weights.h5’ deep learning model and then click on ‘Open’ button to load model and now authority key will be generated.

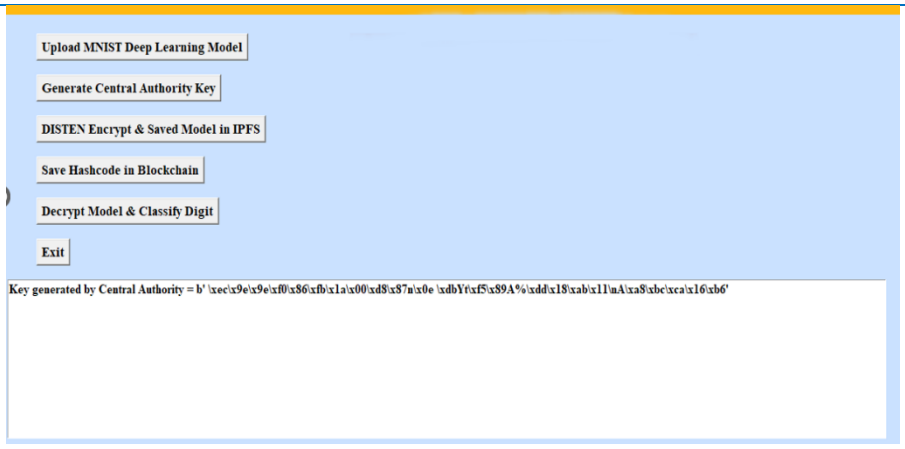

Fig. 7 Central Key Generated

In above Fig. 7 key is generated in binary format and now click on ‘DISTEN Encrypt & Saved Model in IPFS’ button to encrypt model and to save in IPFS server.

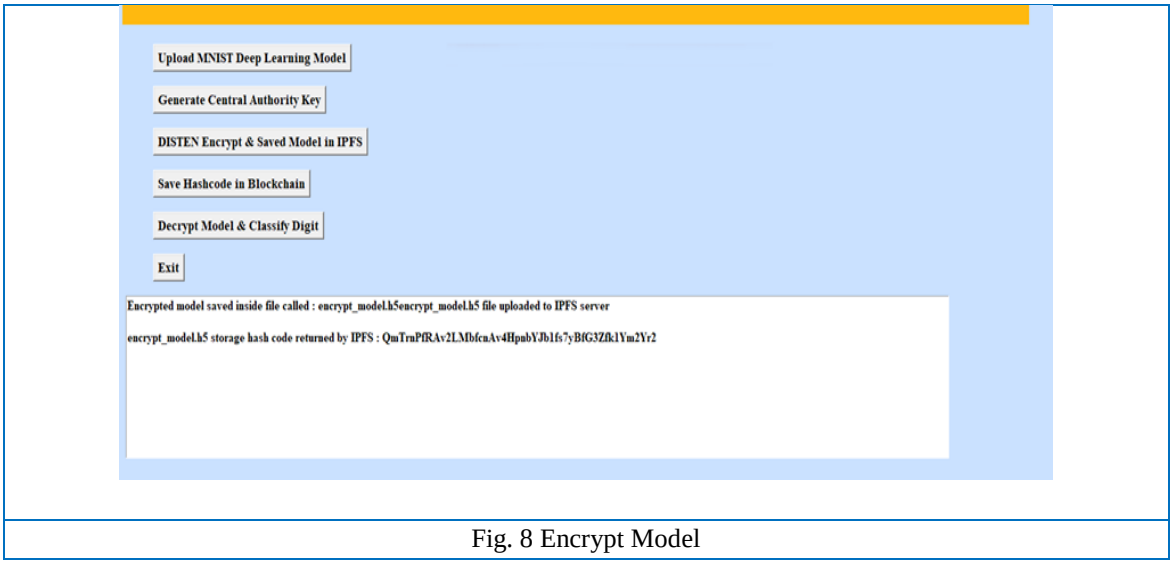

Fig. 8 Encrypt Model

In Fig. 8 encrypted model is saved as IPFS server and the hash code returned by IPFS as 'QmTrnPfRAv2LMbfcnAv4HpnbYJb1fs7yBfG3Zfk1Ym2Yr2'. Next this hash code will be saved in blockchain for further processing.

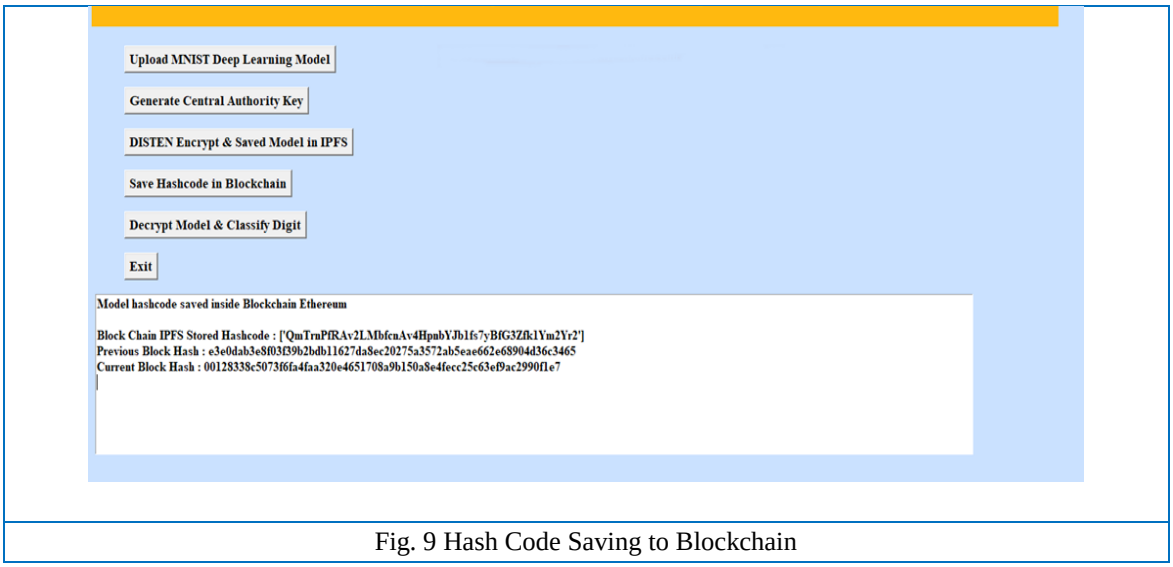

Fig. 9 Hash Code Saving to Blockchain

Fig. 9 displays a blockchain transaction where a hash code is securely recorded. The transaction details include both the current hash code associated with the latest transaction and a reference to the previous hash code, establishing a chain of data integrity and provenance. With the model securely stored in the IPFS and its corresponding hash code recorded on the blockchain, the process moves to the next phase. By selecting the 'Decrypt Model & Classify Digit' button, the user initiates the process of uploading a digit image for classification.

The application proceeds through a series of steps to classify the uploaded digit image. It first contacts the blockchain to retrieve the specific IPFS hash code associated with the stored model. Using this extracted hash code, the application locates the encrypted model within the IPFS network and proceeds to download it. Once downloaded, the model is decrypted locally using the AES symmetric key. The decrypted model is then applied to the uploaded digit image to perform classification, determining which digit is represented in the image.

This process underscores a secure, verifiable method for accessing and utilizing machine learning models in applications that require stringent data security measures.

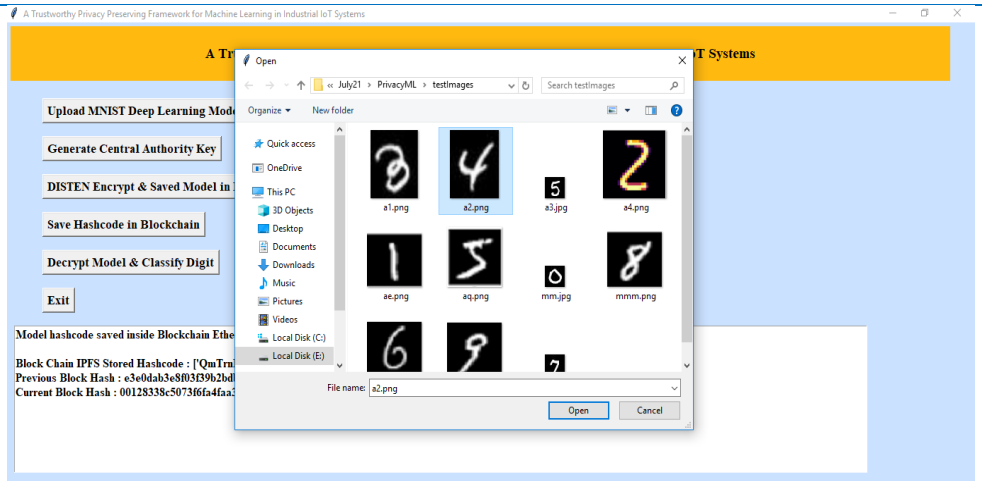

Fig. 10 Loading Image to Classify

Fig. 10 illustrates the user interface interaction where 'a2.png', presumably an image file, is selected and uploaded. Upon clicking the 'Open' button, the image is loaded. This action is likely followed by the system downloading and decrypting the associated machine learning model which then processes the uploaded image. The output, which would be displayed post this process, is not described but is presumably the result of the model's analysis of the image 'a2.png'.

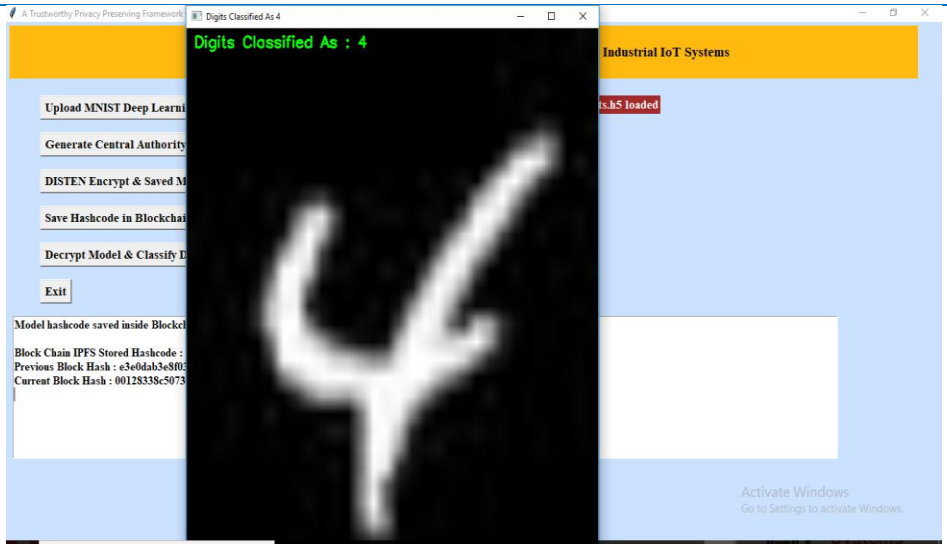

Fig. 11 Classification output

Fig. 11 showcases the output of a deep learning model classification process in green text, indicating that the model has successfully recognized and classified an image as the digit '4'. This suggests the model's capability to analyze and interpret data accurately. The implication is that similar processes can be applied to additional images, allowing for the uploading and testing of various images to classify different digits.

Across IIoT, the results of the deployment of the framework highlight the tremendous advancements that have been made in improving the security of machine learning models. The AES encryption is placed in the centre of the architecture. This encryption offers a high level of protection against unauthorised access. This encryption makes use of AES keys, which are efficiently disseminated via the CENTAUTH. This ensures that only authorised entities are able to decrypt and access the models. Conventional approaches, which frequently rely on less reliable systems, have been shown to be less effective than this technology, which has showed increased encryption efficiency.

The IPFS, which provides a solution that is both scalable and decentralised, is utilised for the purpose of storing these encrypted models. The conventional

centralised storage systems, on the other hand, are frequently less effective and more susceptible to assaults. This strategy stands in stark contrast to these traditional alternatives. Because of its decentralised structure, the IPFS not only enhances the efficiency of storage but also provides an additional layer of security by reducing the risks that are associated with single points of failure.

The implementation of the Ethereum blockchain within the framework assists to strengthen the access control mechanism by delivering a record of transactions that is both transparent and unchangeable, as well as ensuring that the models maintain their integrity. The blockchain is able to successfully maintain a log of model access that cannot be altered, which has the impact of improving data integrity above the levels that are generally attained by traditional techniques. Furthermore, the dynamic access control that is provided by smart contracts on the blockchain presents a system that is both adaptable and safe. This is a significant advance over the static and frequently manual or semi-automated processes that are found in conventional systems.

After doing a comparison analysis with conventional security methodologies, it has been determined that the framework that has been proposed provides significant enhancements across a number of criteria. In particular, there have been considerable advancements made in the amount of time required for encryption, the effectiveness of model storage, and the prevention of security breaches. It has been demonstrated that the incorporation of AES encryption, IPFS, and Ethereum blockchain into a unified framework results in a significant improvement as far as data privacy and integrity are concerned.

Because of the automation and decentralised systems that it utilises, the framework demonstrates excellent scalability and lower operating expenses over the long term. This is particularly true in terms of operational efficiency. When compared to the significant costs that are associated with manually operating and maintaining centralised systems, this is an especially attractive situation. The framework's inherent transparent processes and safe infrastructure contribute to a rise in user trust, which is another benefit of the framework.

A comparative comparison of the newly established framework and traditional methodologies is presented. This analysis can be applied to a variety of operational and security characteristics simultaneously. The framework outperforms previous approaches, which have a tendency to vary and frequently depend on encryption systems that are less efficient. This is accomplished through the use of AES encryption in conjunction with an efficient key distribution system. With this combination, the framework displays great encryption efficiency.

When it comes to storage efficiency, the new framework makes use of IPFS for scalable and decentralised storage. This results in a significant improvement in efficiency when compared to the low to medium efficiency that is provided by previous techniques that rely on centralised storage solutions. As a result of this decentralised strategy, not only is efficiency increased, but the possibility of data loss or manipulation is also decreased.
There is a significant improvement in security in the new framework as a result of the combination of multi-layered security measures and blockchain verification. This is in contrast to the medium security that is offered by traditional approaches, which may lack comprehensive and integrated security measures. Traditional approaches sometimes fall short in this regard, demonstrating low to medium integrity and greater vulnerability to tampering. The utilisation of Ethereum blockchain within the framework offers high data integrity with tamper-proof record-keeping, which is an area in which traditional methods frequently fail.

In contrast to the static, frequently manual, or semi-automated processes that are typical of old systems, the framework implements dynamic access control by utilising smart contracts on the blockchain. This provides access management that is both flexible and secure. Maintaining this level of adaptability is necessary in order to accommodate ever-changing access requirements and security protocols.

Scalability is another area in which the framework excels. It was built to handle large-scale applications in an effective manner, whilst traditional techniques only give medium scalability and can struggle to scale with increasing demands. Scalability is one of the areas in which the framework excels. This quality is essential for the framework's ability to evolve alongside expanding datasets and user bases, as well as for its applicability to a wide variety of different businesses.

The framework places a strong emphasis on automation and decentralised systems, which results in cheaper operational expenses over the long term for the framework of the framework. When compared to traditional approaches, which incur higher expenses due to the continuous maintenance of centralised systems and the manual processes involved, this cost-effectiveness is a significant gain.

Finally, the framework encourages improved user trust by virtue of the fact that its processes are transparent and its infrastructure is completely secure. This is in stark contrast to the fluctuating trust that is connected with traditional approaches, which are mostly dependent on the transparency of an organisation and the historical security performance of the aforementioned organization.

8. CONCLUSIONS AND FUTURE WORK

The new framework significantly outperformed traditional methods in encryption efficiency, utilizing AES encryption and an effective key distribution mechanism. By adopting IPFS, the framework achieved high storage efficiency with scalable and decentralized model management, surpassing the capabilities of centralized storage systems. Enhanced security features were embedded in the framework, with multi-layered security and blockchain verification that offer a more robust defense compared to the medium level of security found in traditional methods. Data integrity was considerably improved, leveraging the Ethereum blockchain for secure, tamper-proof record-keeping, an advance over the vulnerability to tampering inherent in older systems. Access control within the framework was dynamic and flexible, enabled by smart contracts, and stood in contrast to the static nature of traditional access management. The framework was designed with high scalability to efficiently accommodate large-scale applications, addressing scalability issues often encountered with traditional methods. Operational costs were reduced in the long term through automation and the use of decentralized systems, in contrast to the higher maintenance costs associated with traditional centralized approaches. There was an increase in user trust due to the transparent processes and secure infrastructure provided by the new framework, whereas trust varied in traditional methods depending on the organization's practices. The framework not only strengthened the security of ML models within IIoT but also opened up avenues for future research and expansion, showing potential for wide application and continuous improvement.

The theoretical conceptions of both the deep learning and deep reinforcement learning can be made more robust so as to enable better quantification of the functionality of deep learning and deep reinforcement learning centered around the variables like learning effectiveness, computational complications, parameter altering procedures, and data-based topological self-arrangement. Thereby, the challenges caused by the machine learning techniques towards the security aspect of the IoT setting can be redressed at will. Towards the intuitional and effective interpretation of data, we would like to inculcate novel combined learning paradigms and innovative data visualizing approaches while building a more improved variant of the current IIOT security paradigm.

REFERENCES

[1] A. Khattab, N. J. I. o. T. C. Youssry, and Applications, "Machine learning for IoT systems," pp. 105-127, 2020.

[2] F. Hussain, R. Hussain, S. A. Hassan, E. J. I. C. S. Hossain, and Tutorials, "Machine learning in IoT security: Current solutions and future challenges," vol. 22, no. 3, pp. 1686-1721, 2020.

[3] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, P. J. I. C. S. Faruki, and Tutorials, "Network intrusion detection for IoT security based on learning techniques," vol. 21, no. 3, pp. 2671-2701, 2019.

[4] Y. Wu, H.-N. Dai, and H. J. I. I. o. T. J. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," vol. 8, no. 4, pp. 2300-2317, 2020.

[5] I. H. Sarker, A. I. Khan, Y. B. Abushark, F. J. M. N. Alsolami, and Applications, "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions," vol. 28, no. 1, pp. 296-312, 2023.

[6] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. J. S. Hong, "Internet of things: Evolution, concerns and security challenges," vol. 21, no. 5, p. 1809, 2021.

[7] E. Politou, F. Casino, E. Alepis, and C. J. I. T. o. E. T. i. C. Patsakis, "Blockchain mutability: Challenges and proposed solutions," vol. 9, no. 4, pp. 1972-1986, 2019.

[8] M. Bagaa, T. Taleb, J. B. Bernabe, and A. J. I. A. Skarmeta, "A machine learning security framework for iot systems," vol. 8, pp. 114066-114077, 2020.

[9] F. Restuccia, S. D'oro, and T. J. I. I. o. T. J. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," vol. 5, no. 6, pp. 4829-4842, 2018.

[10] E. Fernandes, A. Rahmati, K. Eykholt, A. J. I. S. Prakash, and Privacy, "Internet of things security research: A rehash of old ideas or new intellectual challenges?," vol. 15, no. 4, pp. 79-84, 2017.

[11] J. M. Hamamreh, H. M. Furqan, H. J. I. C. S. Arslan, and Tutorials, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," vol. 21, no. 2, pp. 1773-1828, 2018.

[12] A. R. Sfar, E. Natalizio, Y. Challal, Z. J. D. C. Chtourou, and Networks, "A roadmap for security challenges in the Internet of Things," vol. 4, no. 2, pp. 118-137, 2018.

[13] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. J. W. n. Qiu, "Security of the Internet of Things: perspectives and challenges," vol. 20, pp. 2481-2501, 2014.

[14] A. Čolaković and M. J. C. n. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," vol. 144, pp. 17-39, 2018.

[15] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, 2015, pp. 1310-1321.

[16] S. Li, T. Tryfonas, and H. J. I. R. Li, "The Internet of Things: a security point of view," vol. 26, no. 2, pp. 337-359, 2016.

[17] P. N. Mahalle and P. N. Railkar, Identity management for internet of things. River Publishers, 2022.

[18] H. Mrabet, A. Alhomoud, A. Jemai, and D. J. A. s. Trentesaux, "A secured industrial Internet-of-things architecture based on blockchain technology and machine learning for sensor access control systems in smart manufacturing," vol. 12, no. 9, p. 4641, 2022.

[19] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. J. I. T. o. I. I. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks," vol. 18, no. 11, pp. 8356-8366, 2022.

[20] F. Zhang, H. Wang, L. Zhou, D. Xu, and L. J. F. G. C. S. Liu, "A blockchain-based security and trust mechanism for AI-enabled IIoT systems," vol. 146, pp. 78-85, 2023.

[21] N. Motamarri, G. Satish, H. Uma, A. Barve, H. Patil, and S. N. Taqui, "Identification and Containment of Intrusion Attacks in an IIoT Network based on Machine Learning and Blockchain Technology," in 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), 2024, pp. 70-77: IEEE.

[22] A. S. Hosen, P. K. Sharma, D. Puthal, I.-H. Ra, and G. H. Cho, "SECBlock-IIoT: A Secure Blockchain-enabled Edge Computing Framework for Industrial Internet of Things," in Proceedings of the Third International Symposium on Advanced Security on Software and Systems, 2023, pp. 1-14.

[23] A. Lakhan et al., "Federated learning-aware multi-objective modeling and blockchain-enable system for IIoT applications," vol. 100, p. 107839, 2022.

[24] A. K. Tyagi, "Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications," in AI and Blockchain Applications in Industrial Robotics: IGI Global, 2024, pp. 171-199.

[25] P. Kumar et al., "Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network," vol. 10, no. 5, pp. 2802-2813, 2022.

[26] S. Ismail, S. Dandan, D. W. Dawoud, and H. J. I. A. Reza, "A Comparative Study of Lightweight Machine Learning Techniques for Cyber-attacks Detection in Blockchain-Enabled Industrial Supply Chain," 2024.

[27] R. Gupta, N. K. Jadav, H. Mankodiya, M. D. Alshehri, S. Tanwar, and R. J. I. T. o. I. I. Sharma, "Blockchain and onion-routing-based secure message exchange system for edge-enabled iiot," vol. 19, no. 2, pp. 1965-1976, 2022.

[28] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, and G. J. I. t. o. i. i. Srivastava, "P2tif: A

blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot," vol. 18, no. 9, pp. 6358-6367, 2022.

[29] R. F. J. E. S. w. A. Mansour, "Blockchain assisted clustering with intrusion detection system for industrial internet of things environment," vol. 207, p. 117995, 2022.

[30] M. M. Salim, A. K. Comivi, T. Nurbek, H. Park, and J. H. J. S. Park, "A blockchain-enabled secure digital twin framework for early botnet detection in IIoT environment," vol. 22, no. 16, p. 6133, 2022.

[31] X. Tang et al., "Secure and trusted collaborative learning based on blockchain for artificial intelligence of things," vol. 29, no. 3, pp. 14-22, 2022.

[32] Z. Zhou, Y. Tian, J. Xiong, J. Ma, and C. J. I. T. o. I. I. Peng, "Blockchain-enabled secure and trusted federated data sharing in IIoT," vol. 19, no. 5, pp. 6669-6681, 2022.

[33] C. C. Yann LeCun, Christopher J.C. Burges, "https://yann.lecun.com/exdb/mnist/," (Accessed on 12 August, 2024), 2024.

[34] H. Sid, "https://www.mathworks.com/matlabcentral/fileexchange/27675-read-digits-and-labels-from-mnist-database," (Accessed on 12 August, 2024), 2024.

[35] A. Kaushik et al., "Post quantum public and private key cryptography optimized for IoT security," vol. 129, no. 2, pp. 893-909, 2023.

[36] Z. Zhao, S. Ma, and P. J. C. C. Qin, "Password authentication key exchange based on key consensus for iot security," vol. 26, no. 1, pp. 1-12, 2023.

[37] C. J. T. o. E. T. T. Tamizhselvan, "A novel communication-aware adaptive key management approach for ensuring security in IoT networks," vol. 33, no. 11, p. e4605, 2022.

[38] L. Wei, J. Wu, C. Long, and Y.-B. J. I. P. Lin, "The convergence of IoE and blockchain: security challenges," vol. 21, no. 5, pp. 26-32, 2019.

[39] S. Zafar, K. Bhatti, M. Shabbir, F. Hashmat, and A. H. J. A. o. T. Akbar, "Integration of blockchain and Internet of Things: Challenges and solutions," vol. 77, no. 1, pp. 13-32, 2022.

[40] L. Zhong, Q. Wu, J. Xie, Z. Guan, B. J. C. Qin, and Security, "A secure large-scale instant payment system based on blockchain," vol. 84, pp. 349-364, 2019.

[41] L. Da Xu, Y. Lu, and L. J. I. I. o. T. J. Li, "Embedding blockchain technology into IoT for security: A survey," vol. 8, no. 13, pp. 10452-10473, 2021.

[42] S. Singh, A. S. Hosen, and B. J. I. A. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed iot network," vol. 9, pp. 13938-13959, 2021.

[43] U. Majeed et al., "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," vol. 181, p. 103007, 2021.

[44] C. Pahl, N. El Ioini, and S. Helmer, "A Decision Framework for Blockchain Platforms for IoT and Edge Computing," in IoTBDS, 2018, pp. 105-113.

[45] Y. P. Tsang, C.-H. Wu, W. Ip, and W.-L. J. J. o. E. I. M. Shiau, "Exploring the intellectual cores of the blockchain–Internet of Things (BIoT)," vol. 34, no. 5, pp. 1287-1317, 2021.

[46] J. Xie et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges," vol. 21, no. 3, pp. 2794-2830, 2019.