International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# IoT Network based Cyber Attack Mitigation in Digital Twin with Multi Level Key Management Using Enhanced KNN Model

**Mrs.Valluri.Padmapriya[1] , Dr. Muktevi Srivenkatesh[2]**

**Submitted**: 10/12/2023 **Revised**: 21/01/2024 **Accepted**: 31/01/2024

**Abstract:** Internet of Things (IoT) technology have already been ingrained in many aspects of daily life, including public health, smart vehicles, smart grids, smart cities, smart manufacturing, and smart homes, with the number of Internet-connected devices estimated to reach about 30 billion by 2030. As a result, businesses began adopting and refining Digital Twin (DT) solutions. There are many security threats that will affect DTs despite their usefulness in enabling IoT systems. IoT devices with limited resources are more vulnerable to brute-force attacks, which can then be used as part of a botnet to launch cyber attacks. The increased likelihood of a large-scale cyber attack is compounded by the difficulty in preventing the transmission of malicious scripts to other devices while the botnet is still forming. Knowledge-driven open-source digital twin technologies of industrial control systems are selected after careful consideration of their implementation details. This digital twin is used by the cyber security analysis method to simulate various process-aware attack scenarios and produce a training dataset that reflects the process's measurements during both normal and attack operations. In a perfect world, Digital Twins would each have their own cryptographic identity separate from the host system to avoid attacks. In the actual world of industry, digital twins often operate in shady settings. Systems that mimic a significant part of the functionality of the device being twined fall into this category, but analytical methods also play a role. If an attacker wants to compromise the system's functioning including the Digital Twin, they need to have a thorough understanding of the target system. The suggested architecture also incorporates a cyber attack detection system that uses machine learning model. Critical systems benefit greatly from having a digital twin. However, digital twins also have applications in cyber security and safety. Cryptography enabled Multi Level Key Management using Enhanced K-Nearest Neighbor (CMLKM-EKNN) model that generates a key set in the IoT network for making strong authentication is proposed in this research. The proposed model key set contains key pairs that can be used for only one time to avoid attackers to reuse the keys for attacking the network. The EKNN model identifies the neighbor nodes, perform analysis and allocate weights to the features for attack detection in the network. A digital twin-based paradigm to aid in improving the cyber security of Cyber Physical Systems (CPSs) is proposed. Based on the strategy, the digital twin system can secure the CPSs. The proposed model when compared to the traditional model provides better security levels in the IoT Network.

***Keywords:*** *Internet of Things, Digital Twins, Cyber Physical Systems, Cryptography, Network Attacks, Key Management, Virtual Object, K Nearest Neighbor, Authentication, Security.*

## 1. Introduction

The future seems promising for many different uses of Digital Twins (DT), including supply chain, healthcare, maintenance planning, etc. The inherent features of DT make it highly relevant to practical applications [1], but they also make it susceptible to cyber attacks. As a result, DT's security is crucial to that of the underlying communication and computing infrastructure [2]. It is crucial to protect the digital twin from dangerous attacks as fraudsters are always developing new attack methods. An effective security mechanism, such as an Intrusion Detection System (IDS), can achieve this goal [3]. Critical industrial infrastructures are monitored and automatically controlled in real time by Industrial Control Systems (ICS) [4]. Because they were designed for isolated settings, the communication protocols used in ICS are often insecure. Furthermore, with Industry 4.0, systems are becoming more and more Internet-connected and vulnerable to hacks [5]. The need for reliable IDS in industrial settings is underscored by recent assaults on Iranian nuclear facilities, the Ukrainian power grid, and natural gas pipeline firms in the United States [6].

There has been a dramatic increase in the number of fields in which digital technologies can be applied. Cloud computing, IoT, edge computing, fog computing, and digital twins are just a few examples [7]. The digital twin bridges the gap between these technologies by providing executives with a digital representation of the physical assets sensed by IoT gadgets [8]. As a result, both the danger and the cost can be drastically lowered through the use of digital tools to redesign, reassemble, or create new models [9]. IoT consists of the digital twin's bare bones infrastructure and is crucial to the project's success. Physical layer, network layer, and application layer are the three main functional layers of the

[1]*Research Scholar, Department of Computer Science-GITAM School of Science, GITAM Deemed to be University Visakhapatnam, Andhra Pradesh, India*
[1]*Assistant Professor, Bhavan's Vivekananda College, Secunderabad, Telangana, India*
[2]*Associate Professor, Department of Computer Science-GITAM School of Science, GITAM Deemed to be University Visakhapatnam, Andhra Pradesh, India*
*MailID:padmapriya1bvc@gmail.com, smuktevi@gitam.edu*

IoT, which is a connection of sensor nodes. In other words, the IoT provides a functional framework for digital twins, making their deployment conceivable [10]. Digital twins are becoming increasingly popular in many fields, including manufacturing, healthcare, smart cities [11], supply chain, etc. As long as the real and digital objects are identically mapped, the digital twin can provide its users with a high degree of customization [12]. However, even a single, carefully crafted copy could compromise the system's functionality in significant ways. It may even cause havoc in the industries that have accepted it if this happens. The main reason for this is security concerns, but there are other factors at play as well [13]. The general DT setup of a smart home is shown in Figure 1.

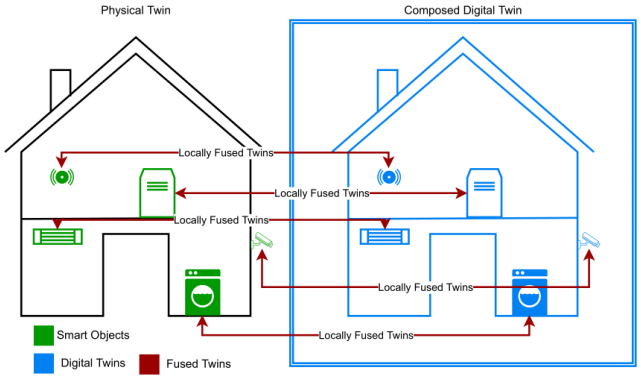


**Fig 1:** General DT of a Smart Home

The IoT, like other networks, has numerous security risks. Additionally, due to the importance of IoT to the functioning of the digital twin, security attacks against IoT would also impact the digital twin's operation [14]. The IDS is the most promising method for reducing security risks across a wide range of networks, including the IoT. The intrusion detection system acts as a safeguard against various threats. In addition, machine learning was proposed as an element of IDS to help detect assaults [15]. In IDS, supervised machine learning techniques are used, meaning they are taught and tested with data that already includes the traits and properties that characterize a given attack type [16]. In order for such an algorithm to be effective, the goal function must be described in terms of characteristics within a suitable dataset [17]. Therefore, choosing the most promising dataset that translates the issue statement correctly or making use of real-time data is an inherent step towards the creation of IDS [18]. The general intrusion detection model in DT is shown in Figure 2 [14].

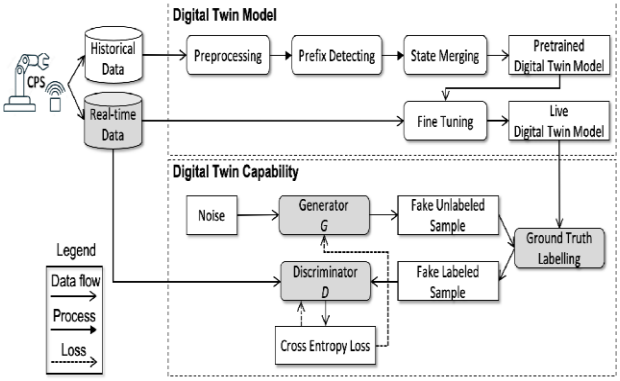


**Fig 2:** IDS in DT

Interest in using digital twins for industrial control systems has skyrocketed in recent years. Digital twins have attracted a lot of interest because of the cutting-edge capabilities they provide in fields like modeling, optimization, and predictive maintenance [19]. Recent research has explored the potential of digital twins as a tool for intrusion detection in ICS. In order to do so, this research proposes a security framework for industrial control systems [20], complete with a digital twin for security monitoring and an intrusion detection system based on machine learning for real-time detection [21]. The digital twin system implemented in this research is an independent, freely-distributable simulation of a manufacturing filling facility [22]. This solution is selected after exhaustively comparing it to other available knowledge-driven open-source digital twin solutions for industrial control systems [23].

A digital twin is a computer simulation that can almost perfectly mimic the behavior of its real-world counterpart. A digital twin represents the most up-to-date version of a physical system and is maintained during the system's entire life span. Recent research have focused on how digital twins can be used to improve ICS security [24], even if the original concept of digital twin was to improve the manufacturing system life-cycle. It is possible to communicate process control alarms from a digital twin to its physical counterpart in the case of a security breach [25]. Since digital twin-based security analysis does not need to be executed on resource-constrained devices, it opens the door to employing techniques for cyber security analysis that necessitate more extensive computer resources. In addition, digital twins prevent disturbances and harm to the actual system during security examination performed off-site [26].

This digital twin is used in the cyber security analysis method to simulate various process-aware attack scenarios and produce a training dataset that reflects the process's measurements during both normal and attack operations [27]. The digital twin is used to develop and carry out 23 different attack scenarios, across four distinct attack types: naming command injection, network DoS, calculated measurement injection [28], and naïve measurement injection. The suggested architecture also incorporates an

intrusion detection system that uses machine learning. There are two phases to this intrusion detection system's architecture [29]. Information technology systems prioritize data security and privacy, while operational technology systems prioritize system availability. While a reasonable level of delay is acceptable in IT systems, any security measures used in ICSs must not interfere with the continuous flow of industrial operations. Since ICSs are embedded in operational infrastructures, attacks against them can have devastating effects because they are directed at the underlying physical process. Such attacks are typically created after learning about the regulated industrial process, allowing them to avoid the regular security procedures and not break any protocol standards.

Research using commercial digital twin solutions of ICSs is difficult to access. This is because allowing access could lead to a data breach of confidential information related to systems utilized in industrial settings. As a result, academics need access to digital twin solutions of ICSs that are freely available as open source. However, there is a dearth of resources that address the design and execution of digital twins with open-source software and tools. This research examines existing open-source digital twin solutions for ICSs and proposes a security framework based on this concept. The ICS digital twin and an ML based IDS work together in this framework to keep systems safe from infiltration [30]. Researchers and students in the field of cyber security in ICSs can benefit from a framework like this that makes use of open-source tools and software. Strong cyber security measures are necessary to protect against cyber threats in light of the proliferation of internet-connected gadgets. Cyber security for the IoT encompasses a wide range of approaches and tools designed to protect against intrusion from the digital realm. Due to factors such as low processing power, few security features, and susceptibility to attacks like denial-of-service and distributed denial-of-service, cybersecurity is complicated when it comes to IoT devices and systems.

Technologies like machine learning and artificial intelligence are used in IoT cyber security methods like encryption, authentication, access control, and threat detection and response. With assistance from the sending node, the entering node, and the receiving node, the lightweight key generation method was utilized to encrypt the data in transit. The data's final server's identity has been used as a master key for encryption and decryption. Encryption and decryption times are cut down with the suggested method's short key length. When decryption and transmission of data take longer than expected, this might be used as evidence of malicious behavior on the part of internal nodes. Appropriate security measures must be put in place to guarantee the safety of systems. The proposed paired key encryption mechanism is meant to detect malicious nodes and shut them down before any data is stolen in transit. In addition to enabling secure communication, the system may also be able to identify a wide variety of network threats, such as active attacks, network attacks, denial of service attacks, Man in the Middle attacks, jammer attacks, and passive attacks. The lowest energy consumption occurs at internal nodes, which helps the network last longer and improves quality-of-service measures.

Due to the potential risk of exposing the underlying ICS, commercial digital twin solutions are not freely available for academic research. Because they don't include cyber-attack implementations or dataset generation for ML-based IDS development, existing open-source ICS digital twins aren't adequate for security research. In this research, we proposed an Enhanced KNN (EKNN) approach for attack mitigation in the digital twin based IoT network handling complex data with heterogeneous views. Any type of view can be utilized when applying the EKNN method, as long as a distance function can be defined on that view. The EKNN includes an integral learning component that learns the weight of each feature for detection of attacks. Furthermore, the EKNN method factors in not only the training data, but also the unknown instance itself when assessing the importance of different views in classifying the unknown instance. The proposed model uses asymmetric cryptography based model for hey set generation in the network. Cryptography enabled Multi Level Key Management using Enhanced K-Nearest Neighbor model that generates a key set in the IoT network for making strong authentication is proposed in this research. The strong authentication model allows only authorized users to access the network and also it will be easy for detection of attacks in the network. This paper briefly discuss about the issues on cyber security, its impact and loss of network resources. This paper proposed a model that is used for cyber-attack mitigation and removal of nodes causing attacks in the network. The proposed model does not concentrate on new variants of attacks due to lack of attack samples for training

## 2. Literature Survey

The critical role that Critical Infrastructures play in maintaining the availability of many key services has led to a rise in interest and concern over the past several years about the creation of security monitoring and management methods for these systems. The unique qualities of these systems and the inherent aversion of Critical Infrastructures operators to activities implying downtime make this a challenging assignment. When it comes to analyzing security or evaluating potential mitigation techniques, a digital twin's accurate virtual representation of a physical object or process can provide a faithful environment. However, having them deployed on-premises can be pricey, necessitating a sizeable CAPEX whose return is conditional on the skill with which one plans and deploys an appropriate

support infrastructure, and on the success with which one implements efficient and scalable data collection and processing mechanisms that can make the most of the acquired resources. In this paper, Sousa et al. [1] demonstrated the ELEGANT project's off-premises methodology for developing and deploying Digital Twins for protecting vital infrastructure. Such Digital Twins facilitate the development and validation of Machine Learning models to counteract security concerns like Denial of Service attacks by modeling production PLCs in real time and collecting data in a scalable and efficient manner.

Due to the IIoT's rapid growth, industrial processes will need to be digitized in order to maximize network efficiency. Combining IIoT and DT transforms real-world things into digital copies that may be used more effectively in data analytics. However, DT-enabled IIoT creates a deluge of data, the majority of which is transmitted to the cloud or edge servers for real-time analysis. Threats and attacks on continuing communication, however, are caused by unstable public communication channels and a lack of confidence among participating institutions. Kumar et al. [2] offered a blockchain and Deep Learning (DL) integrated system to provide decentralized data processing and learning in an IIoT network, which was inspired by the preceding discussion. The framework begins with the presentation of a new DT model that makes it easier to build a virtual environment in which IIoT's security-critical processes may be simulated and replicated. Second, the author suggested a method of transmitting data via a blockchain that use smart contracts to safeguard the data's validity and integrity during transmission. The DL technique is made to use the IDS against legitimate data acquired from the blockchain. To learn the spatial-temporal representation, DL proposes a Long Short Term Memory-Sparse AutoEncoder (LSTMSAE) method. In order to learn long-distance features and reliably detect attacks, the proposed Multi-Head Self-Attention (MHSA)-based Bidirectional Gated Recurrent Unit (BiGRU) method makes use of the extracted characteristics.

To aid and improve manufacturing processes in industries, DT have been proposed. Positive results from implementing DT have prompted projections that more than half of the major industries will reap DT's rewards by the year 2021. Unfortunately, there is no generally agreed-upon explanation for DT. Khan et al. [3] provided an extended structure of DT, the spiral DT-framework, to aid researchers in developing a shared narrative about DT. In addition, the author recommended leveraging blockchain technology, as opposed to cloud or fog, to manage DT data securely and reliably. Since the conventional blockchain experiences delays in transaction confirmation and is susceptible to quantum attacks, the author suggested a novel blockchain variation, called twinchain, that is both quantum-resistant and provides instantaneous transaction confirmation. The model also provided a plan for using twinchain in the production of a robotic surgical system.

Recent statistics and studies reveal that insider threats result in far greater loss than external attacks. To mitigate the dangers posed by insiders, an increasing number of businesses are installing or acquiring detection systems. However, there are major obstacles to the prompt and accurate detection of insider threats. In this research, Wang et al. [4] used Digital Twins and deep learning models that prioritize the user's attention to suggest a novel method for detecting insider threats. The paper begins with an overview of insider threats and the difficulties of detecting them. Then, this paper discusses the progress that has been made in recent years to address the challenges of insider threat detection. Then, the author offered recommendations for overcoming these obstacles: The authors address this issue by developing a novel intelligent insider threat detection framework that utilizes Digital Twin (DT) and self-attention based deep learning models, conducting insight analysis of user behavior and entities, implementing contextual word embedding techniques with the Bidirectional Encoder Representations from Transformers (BERT) model and sentence embedding techniques with the Generative Pre-trained Transformer 2 (GPT-2) model for data augmentation, and finally, using these methods to detect threats that would otherwise go undetected Therefore, this research developed deep learning models based on self-attention to rapidly identify insider threats. In order to detect insider threats, this research proposes a streamlined transformer model called DistilledTrans and applies the original transformer model, BERT + final layer, Robustly Optimized BERT Approach (RoBERTa) + final layer, and a hybrid approach combining pre-trained (BERT, RoBERTa) with a Convolutional Neural Network (CNN) or Long Short-term Memory (LSTM) network model.

The use of intrusion detection to safeguard IoT from hostile attacks is becoming increasingly important as IoT devices grow more commonplace. Traditional intrusion detection systems work well, but the lack of data in the IoT makes them ineffective. In this study, Wu et al. [5] presented an approach to this problem by utilizing unsupervised heterogeneous domain adaptation (HDA) to create an adaptive bi-recommendation and self-improving network (ABRSI). Effective intrusion detection in data-poor IoT target domains is made possible by the ABRSI, which transfers enhanced intrusion knowledge from a data-rich network intrusion source domain. The ABRSI uses adaptive bi-recommendation matching to facilitate the dissemination of granular knowledge about intrusions. The alignment of incursion categories in the shared feature space and the bi-recommendation interests of two RSs create a positive feedback loop. Furthermore, the ABRSI employs a self-improvement process, increasing the transfer of incursion information in four independent methods. Assigning hard

pseudo labels (PLs) more accurately is the goal of a voting process that takes into account both RS decisions and label relationships. Target instances that cannot be allocated a hard PL will instead be assigned a probabilistic soft PL, creating a hybrid pseudo-labeling method that encourages variety and target data participation during intrusion knowledge transfer. At the same time, the ABRSI allows for a wide variety of soft pseudo-labels to be used on a local and personal scale. Finally, an error knowledge learning mechanism is used to exploit in a malicious way the aspects that lead to detection uncertainty, learning from both new and old errors to avoid repeating the same mistakes.

In the case of IoT intrusion detection (IID), a lack of data makes data-dependent algorithms impractical. In order to combat this issue, Wu et al. [6] employed the information-dense network intrusion detection (NID) domain to improve the precision of intrusion detection in IID environments. To facilitate more effective knowledge transfer during an incursion, this paper makes use of a geometric graph alignment (GGA) strategy to hide geometric differences between domains. Each intrusion domain is represented as a graph, with nodes representing intrusion categories and edges representing the relationships between nodes. A muddled discriminator that can't tell the difference between intrusion domain graphs' adjacency matrices is responsible for maintaining the overall form. To prevent misalignment of the graph due to rotation or symmetry, the author employed a rotation avoidance technique and a center point matching mechanism. Additionally, vertex-level alignment is accomplished through the transfer of category-wise semantic knowledge. Fine-grained pseudo-label (PL) assignment is generated by exploiting the target data via a PL election method that takes into account network prediction, geometric property, and neighborhood information simultaneously. The transferred intrusion knowledge can improve IID performance when the intrusion graphs are geometrically aligned from various granularities.

The IoT is rapidly expanding in scope as we enter the "Internet plus" era, and its infrastructure is growing at an unprecedented rate. An era marked by the "Internet of Everything" is on the horizon. The proliferation of IoT terminals and software increases the network's susceptibility to intrusion attempts of all kinds. As a result, developing an intrusion detection model that ensures the IoT's safety, privacy, and dependability is crucial. Due to the complexity and fluidity of the IoT ecosystem, traditional intrusion detection technology has limitations such as a low detection rate and limited scalability. Particle swarm optimization (PSO) based gradient descent (PSO-LightGBM) is proposed by Liu et al. [7] for intrusion detection. This technique uses PSO-LightGBM to detect and identify harmful data by extracting features from the data and feeding them into a one-class support vector machine (OCSVM). The intrusion detection model is tested using the UNSW-NB15 dataset.

Since its beginnings, the IoT has expanded rapidly as a game-changing technology. The IoT is the interconnection of computing devices and data to enable greater process automation and centralization. The IoT is reshaping every aspect of business and culture. With the rapid development of this technology comes a growing requirement for exploit detection and vulnerability awareness to forestall the compromise of vital system resources and essential business operations. Unfortunately, DoS and DDoS attacks are commonplace. By comparing features from the UNSWNB15 and Bot-IoT data-sets based on flow and Transmission Control Protocol (TCP), Zeeshan et al. [8] constructed a data-set of packets from IoT traffic for use in this proposed Protocol Based Deep Intrusion Detection (PB-DID) architecture. The author solved issues like unbalanced and over-fitting to properly categorize normal, DoS, and DDoS traffic.

There are an ever-increasing number of tiny, linked gadgets that can push personal data to the Internet, making cyber-threat security one of the most difficult study disciplines of information technology today. Since a typical IoT configuration involves multiple IoT-based data sources interacting with the physical environment across a wide range of application domains, this protection is essential. However, millions of IoT devices are already deployed without any hardware security support, and many of the most popular IoT devices on the market today offer only the barest minimum in terms of security, leaving them vulnerable to constantly evolving and sophisticated attacks. Tools that can identify these types of cyber dangers are therefore essential. Eskandari et al. [9] introduced Passban, a smart IDS that can safeguard directly linked IoT gadgets. The proposed solution is unique in that it can be implemented on low-cost IoT gateways, fully utilizing the edge computing paradigm to detect cyber threats as close as possible to the corresponding data sources.

There is a lot of focus on IDS for recognizing cyber-attacks in IoT networks, which is important for the security of safety-critical IoT systems like the Internet of Vehicles (IoV). Due to its versatility and capacity to learn from a wide variety of data sources, deep learning algorithms are widely used by several IDSs in their anomaly detection engines. But this type of machine learning model has a high false-positive rate, and even specialists have trouble understanding the reasoning behind its predictions. One way in which cybersecurity professionals can verify an IDS's efficacy and build stronger cyber-resilient systems is by learning why it blocked a given packet. To increase the openness and robustness of DL-based IDS in IoT networks, Oseni et al. [10] provided an explainable deep learning-based intrusion detection system. Experts who rely on the judgments produced by deep learning-based IDS to ensure the security of IoT networks and develop more cyber-resilient systems can understand the decisions with the

framework's SHapley Additive exPlanations (SHAP) mechanism. The ToN_IoT dataset was used to verify the proposed framework and to compare it to other promising methods.

## 3. Proposed Model

The importance of strong cyber security measures to protect against cyber threats has grown in tandem with the increasing number of internet-connected devices. IoT cyber security refers to the practices and tools used to protect internet-connected gadgets and infrastructure against intrusion. There are many obstacles to ensuring the safety of IoT systems and devices due to their singular characteristics. Due to their lower computing and storage capabilities, IoT devices are more susceptible to cyber attacks. Encryption, authentication, access control, and threat detection and response are just some of the many cyber security measures that must be taken to protect the Internet of Things. Data sent between IoT devices is more secure when encrypted, and only authorized users can access and interact with the system with the authentication and access control models. Technologies like machine learning and artificial intelligence are used in real-time threat detection and response to identify and counteract potential cyber threats. Since IoT devices are being utilized to operate key systems and infrastructure, ensuring their robust cyber security is essential for many sectors, including healthcare, manufacturing, and transportation. Cyber security must be a top priority, and strong measures must be put in place to protect against cyber threats, as the number of IoT devices continues to increase. With new enhancements, cutting-edge internet technologies like big data, cloud computing, the IoT, and programmable networks have advanced more quickly. Software-defined network design, however, raises the prospect of a numerous assaults due to centralized control. Anomaly detection and vulnerability assessment are the two main functions of intrusion detection systems.

While the IoT has many applications in industry, there are several security concerns that must be addressed. As a result, these pose a risk to an organization's security. The term security analytics refers to a set of tools and techniques for processing and analyzing data in order to identify and prevent potential dangers. As digital twins facilitate the creation and dissemination of new information, they make for a solid basis for IoT security analytics. Along an asset's lifecycle, a digital twin will map the physical asset to its digital equivalent. Semantics are managed, and the link between the real and virtual worlds is exploited. Improve Industrial Internet of Things security with the use of security analytics. To internalize external cyber security knowledge, it employs big data analytics techniques. Data from multiple sources can be correlated to determine the occurrence or likelihood of an incident using security analytics. Organizations can't afford to use inefficient models for security analytics since poor models lead to poor security analytics. Cyber security is enhanced when information about threats and incidents is shared between stakeholders throughout the lifecycle. For instance, according to a recent survey, more than 90% of businesses say they rely on external sources for actionable cyber security expertise. Organizations deploying sophisticated and lifecycle-centric IoT systems need new ways of thinking about the problem of knowledge generation and sharing.

To counteract increasingly complex cyber attacks, the Industrial IoT calls for improved communication and coordination among all parties involved in the product's lifetime. The concept of a digital twin has been around for some time now and is used by businesses to connect a physical asset to its digital equivalent throughout its existence. Digital twins help with security testing, boost cyber situational awareness, and fine-tune intrusion detection systems, so their applications are not confined to operational contexts. In terms of cyber security, it is estimated that 80% of firms instrument digital twins in some way, with 85% of security officers agreeing that digital twins unleash even more efficient detection and mitigation. Digital twins give a semantic layer to virtual representations by abstracting tangible assets, making problem solving easier. By layering security analytics upon the digital twin's data structure, they guarantee a deeper dive into the asset's current and past states.

Knowledge creation and knowledge transfer are two areas where digital twins show promise. This research goal is to improve cyber security in the Industrial IoT throughout its lifecycle by combining security analytics and digital twins, and to further cyber security knowledge-sharing studies. By including a replication-based intrusion detection strategy, the gap in the literature is filled about the lack of a cohesive framework for digital-twin-based security. This study helps make the Industrial Internet of Things safer by showing how to better share cyber security knowledge through the use of digital twins and analytics. Using historical and real-time data, digital twin models are learned as part of the usual process for state prediction. A Timed Automaton Machine is first statically trained from the past data. While this pre-trained digital twin model can produce very accurate simulations of the real CPS, it can only capture those behaviors for which data is already available. This model, therefore, needs to be refined with real-time data to enable it to develop in tandem with its physical counterpart during operation. The proposed model framework is shown in Figure 3.

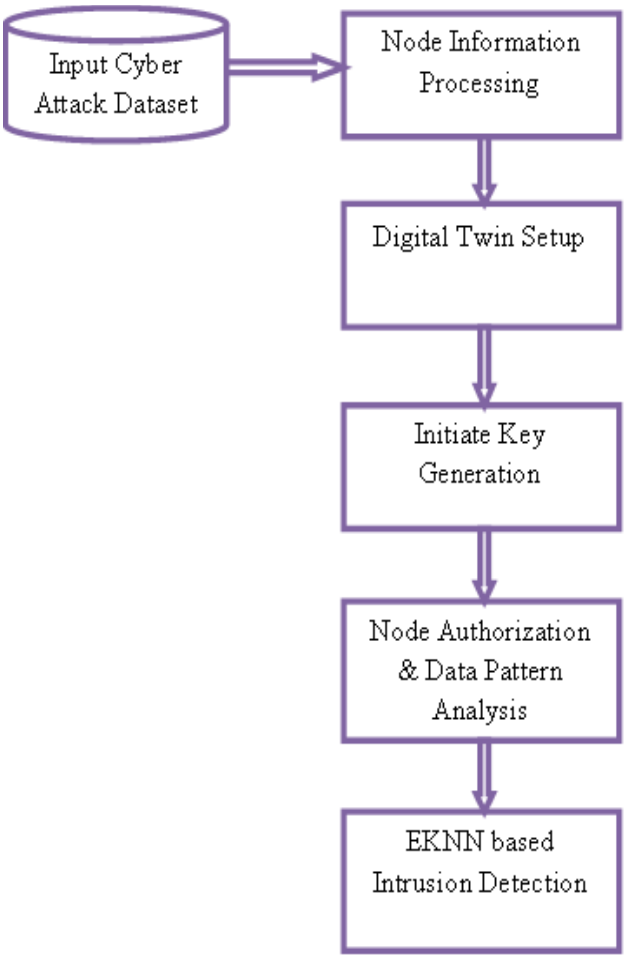


**Fig 3:** Proposed Model Framework

The intrusion detector that forms part of the digital twin functionality is here solely trained on real-time data. By contrasting the actual sensor and actuator values with the anticipated values provided by the digital twin model, the proposed method arrives at a ground truth label as training signals. The fundamental advantage of the technique is that data can be encrypted using a secret key and decrypted only at the destination node. If a hostile external or internal node generates random keys and attempts to decode the cipher data, the result will be unpredictable. When keys are created with an incorrect destination id, the algorithm throws an exception. Without having to send keys over an insecure network connection to their final destination, this method also lessens the burden on the network. The receiving node can forge its own decryption keys.

In the K-Nearest Neighbor model, K is initially determined by looking at the surrounding nodes. Euclidean distance is determined between neighbors based on the K value. Selecting neighbors based on closest distance. Among the chosen neighbors, a tally is made of the data points in each group. Put the new samples in the network group with the most neighbors, either the attacked or normal ones. The data set used for forecasting will be created. Enhanced KNN begins with a K value choose made using the nearest neighbor feature vector. The variety of network data points are used to assign weights to the neighbors chosen. It's possible to figure out how far apart the neighbors are. The feature vector is computed by assigning weights to neighbors and selecting those with the smallest distance. Taking into account all of the feature vectors and their distances while also taking the weights into account results in an updated K value. This improvement aids in picking the optimal K value for taking into account data points in the creation of the final prediction set. Cryptography enabled Multi Level Key Management using Enhanced K-Nearest Neighbor (CMLKM-EKNN) model that generates a key set in the IoT network for making strong authentication is proposed in this research.

**Algorithm CMLKM-EKNN**

{

**Input:** Cyber Attack Dataset $\{CA_{set}\}$

**Output:** Attack Nodes List $\{AN_{List}\}$

**Step-1:** The nodes in the IoT network that need to use DT will maintain the information ate the network authority. The nodes information will be maintained and an immutable label is provided to each node DT for recognition and for communication. The process of node information processing is performed as

$$TI[K] = \sum_{n=1}^{K} strip[gethour\big(CAset(n)\big) + getseconds\big(CAset(n)\big), 4)$$

$$DTNodeReg[K] = \sum_{n=1}^{K} getaddr(CAset(n)) + \omega(CAset(n)) + TI\big(CAset(n)\big)$$

Here getaddr() model considers the physical allocated address of each gadget and ω is the computational capability of a node and TI is the time instant of the node at registration.

**Step-2:** A digital twin is a virtual representation of a physical IoT gadget that can be used to simulate its actual properties and operations. Smart sensors embedded in the object collect data in real time, allowing a digital depiction of the asset to be produced. To construct a digital model that accurately represents the real-world gadgets behaviors or states, data about the gadget must be collected. Information such as design documents, production methods, and engineering files may be included. The Digital Twin setup is performed as

$$DT[K] = \sum_{n=1}^{K} \mu(CAset(n), VM(CAset(n))\{setVM(n) \leftarrow setlogaddr(VM\big(CAset(n)\big))$$

Here μ is the model for the creation of virtual copy of each specified gadget. Every Virtual Mode model consists logical address so that replica will be maintained for each gadget.

**Step-3:** A public key and its accompanying private key make up a key pair. Cryptographic procedures based on computational issues known as one-way functions are used to produce key pairs. In public key cryptography, one of the two keys used to authorize the node and to encrypt or sign data. The key generation is performed as.

$$Va[K] = \sum_{n=1}^{K} getVal(n)$$

$$Vb[K] = \sum_{n=1}^{K} getVal(n) where\ Vb > Va$$

$$Vc[K] = \sum_{n=1}^{K} Vb(n) + Va(n)$$

$$Mkey[K] = \sum_{n=1}^{K} \frac{Vc(n) + Va(n)}{Vb(n)} + (Vc \oplus Vb)$$

$$Rkey[K] = \sum_{n=1}^{K} (MKey \oplus Vc) \ll 2$$

$$Keyset[K] = \sum_{n=1}^{K} \{Mkey(n) : Rkey(n)$$

The key pairs are used to perform node authentication and these keys are used to access the DT data in the network to identify the intrusions.

**Step-4:** The proposed model performs node authorization to check if the node is allowed to make use of a resource or access a file. In most cases, the network authority won't grant access to a node without first authenticating. The controlling authority and DT sensors can communicate to one another safely with a method called Node Authentication. The node authentication is performed as

$$NodeAuth[K] = \prod_{n=1}^{K} getDTNodeReg(n) + getaddr(n) + getattr\big(DT(n)\big) + getKey(MKey(n))$$

$$NodeAuth[K] = \begin{cases} NodeAuth \leftarrow 1 & if\ Mkey(n) == DTNodeReg(MKey(n)) \\ NodeAuth \leftarrow 0 & Otherwise \end{cases}$$

**Step-5:** Data Pattern analysis monitors the data packets in detail to see if it behaves abnormally based on known characteristics of network packets. Network packets are monitored by a pattern-based IDS, which then compares them to a library of previously identified attack patterns. The data pattern analysis is performed as

$$DTdata[K] = \sum_{n=1}^{K} getData\big(DT(n, n+1)\big) + diff\big(DT(m, n+1)\big) + max(simm(data(n, n+1))$$

Here getData() model gathers the network data using DT model and diff() is used to identify the pattern changes in the data. simm() model identifies the similar data that DT nodes gathered.

**Step-6:** Using weights, the EKNN algorithm was used to develop this attack classification scheme. The EKNN algorithm is an example of an algorithm for supervised machine learning since it can be applied to issues of both classification and regression. From the principle that relative entities are close together, which comes this algorithm discovers groups of related information. First, the network data patterns are loaded into the EKNN algorithm, and then K is set to the number of neighbors that will be used. The distance that lies between the irrelevant characteristic and the relevant feature is then determined for each data instance. The minute difference in data patterns are also considered. Once every pattern is collected, it is sorted by distance from smallest to largest, and the first k entries' labels are taken. The EKNN model classification and attacks causing nodes are displayed as

EKNN uses the Euclidean distance to determine the degree to which a test instance differs from a given training instance. All aspects of an instance, whether they are important or not, are given equal consideration. When figuring out how far away two instances are, the EKNN model assigns different weights to the characteristics. In practice, EKNN looks like

A nearest data point from the DT sensor is considered as

$$DTdata(n, n+1) = \sum_{n=1}^{K} \frac{getaddr(n) + mindist(getaddr(n, n+1))}{len(K)}$$

When training a EKNN based model, more weight is given to features that are closer in proximity based on the nearest neighbor set taken into account in the DTdata. The process of weight distribution is performed as

$$Walloc[K] = \sum_{n=1}^{K} getmax\left(simm\big(DTdata(n, n+1)\big)\right) + \frac{mindist(DTdata(n, n+1))}{size(DTdata)} + \min\left(\text{diff}(\text{DTdata}(\text{n}, \text{n}+1)\right)$$

The intrusion causing nodes are identified and the nodes will be excluded from the network for mitigation of attacks in the DT based network. The final prediction list is generated as

$$AN_{List}[K]$$
$$= \sum_{n=1}^{K} \frac{\max\big(Walloc(n,n+1)\big) + \min\left(diff\big(DTdata(n,n+1)\big)\right)}{len(Walloc)}$$
$$+ \max\Big(\text{simm}\big(\text{Rkey(n, n + 1)}\big)\Big)$$
$$+ \lim_{\text{n}\to\text{K}} \left(\text{Walloc(n)} + \frac{\max\left(\text{simm(n, n + 1)}\right)}{\text{size(DTdata)}}\right)^2$$

}

## 4. Results

CPSs can be monitored, visualized, and predicted with the help of digital twins, which are digital representations of real-world objects. Manufacturing processes benefit from the increased efficiency and enhanced quality made possible by these capabilities. The idea of digital twins can also be used to improve the safety of a smart manufacturing facility. To be more specific, this idea can be implemented as early as the design phase by giving engineers the resources they need to identify vulnerabilities in the CPS's specification. Other technological use cases of digital twins that improve security are security testing and intrusion detection, both of which can be accomplished in systems engineering or during transmission operation. Complex systems that combine physical and digital components are known as CPS. In CPS, intrusion detection refers to the process of looking for out-of-the-ordinary activities. These discrepancies could originate in the system's controls, the network, or the surrounding physical conditions. Hardware and software failures, human mistake, and improper CPS setups are also potential causes. In order to overcome these obstacles, this research proposed a digital twin based intrusion detection model for attacks mitigation to improve QoS in the IoT Networks. The proposed model is implemented in python and executed in Google Colab. The proposed model considers the data set available at link **https://www.kaggle.com/datasets/hassan06/nslkdd.**

There are millions of digital devices that make up the IoT, and they communicate with one another with very little intervention from humans. Despite being one of the fastest growing areas of computing, the Internet of Things is susceptible to a wide variety of threats. Attacks and unusual placement on the IoT framework are becoming more of a worry in the IoT industry. With the proliferation of IoT foundation usage across many industries, the threats and attacks against these systems are also on the rise. This research presents a number of deep learning methods for reliably predicting assaults on IoT systems after doing a literature study. Some examples of attacks and anomalies that could happen in an IoT framework include injection attacks, man-in-the-middle attacks, information collecting, malware assaults, and distributed denial of service (DDoS) attacks. In order for the IoT network to prevent unwanted traffic and illegal access, it is crucial to detect assaults and harmful traffic. An essential component of any IoT solution is machine learning, which may be defined as the capacity of an intelligent device to automate or modify a state or behavior based on knowledge. Applications of ML techniques include regression and classification, and ML itself can infer useful information from data produced by devices or people. Security services on an IoT network can also be provided by ML.

There is a growing interest in using machine learning to attack detection issues, and ML is finding more and more uses across the cyber security industry. There is a dearth of literature on effective detection approaches appropriate for IoT contexts, despite the fact that numerous studies have utilized ML techniques to uncover the best ways to identify assaults. There are two primary forms of cyber-analysis that can be used to apply machine learning to the task of attack detection: signature-based and anomaly-based. In order to identify known attacks, signature-based approaches look for certain characteristics in the traffic that is associated with those attacks. The capacity to successfully identify all known threats without producing an excessive amount of false alarms is one of the benefits of this class of detection techniques.

The efficacy of an anomaly detector can be determined by putting it through a series of attacks and monitoring how well it identifies strange behavior. These traditional model based intrusion detectors have been successful, yet they still have two major flaws. For starters, most of these models rely on pre-existing log data and hence are unable to continue learning while CPS is in use. Therefore, these models fare well against typical threats but underperform against unexpected ones. There is also the issue that training network-based models requires a lot of labeled data. Nonetheless, purchasing labels in CPS is typically a costly endeavor. Therefore, it is much preferable to choose a model that can make use of unlabeled data. Cryptography enabled Multi Level Key Management using Enhanced K-Nearest Neighbor (CMLKM-EKNN) model that generates a key set in the IoT network for making strong authentication is proposed in this research. The proposed model is compared with the traditional ELEGANT: Security of Critical Infrastructures With Digital Twins (ELEGANT) and Toward Smart Manufacturing Using Spiral Digital Twin Framework and Twinchain (SDT-Twinchain) and the results represent that the proposed model performance in attack mitigation is high.

The nodes in the IoT network will be registred with the network administrator that is used for processing the nodes information. The immutable label is provided to each node in the network. The node registration process helps in recognition of nodes. The IoT Node Registration Time Levels of the proposed and existing models are shown in Table 1 and Figure 4.

**Table 1:** IoT Node Registration Time Levels

| Nodes Considered | Models Considered | | |
|---|---|---|---|
| | CMLKM-EKNN Model | ELEGANT Model | SDT-Twinchain Model |
| 20 | 11 | 16.9 | 16.1 |
| 40 | 11.2 | 17.1 | 16.3 |
| 60 | 11.4 | 17.3 | 16.5 |
| 80 | 11.6 | 17.6 | 16.9 |
| 100 | 11.9 | 17.8 | 17.1 |
| 120 | 12 | 18 | 17.4 |

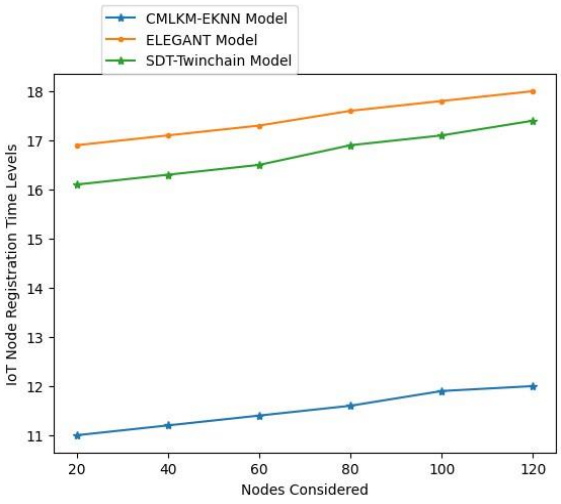


**Fig 4:** IoT Node Registration Time Levels

For each physical gadget, DT is established that gathers the information of working of internal components of each gadget. The DT data helps in monitoring the working status of each device. The Digital Twin Setup Accuracy Levels of the traditional and proposed models are depicted in Table 2 and Figure 5.

**Table 2:** Digital Twin Setup Accuracy Levels

| Nodes Considered | Models Considered | | |
|---|---|---|---|
| | CMLKM-EKNN Model | ELEGANT Model | SDT-Twinchain Model |
| 20 | 97.1 | 92.6 | 94.1 |
| 40 | 97.3 | 92.9 | 94.3 |
| 60 | 97.5 | 93.1 | 94.7 |
| 80 | 97.7 | 93.5 | 94.8 |
| 100 | 97.8 | 93.8 | 95.0 |
| 120 | 98 | 94 | 95.2 |

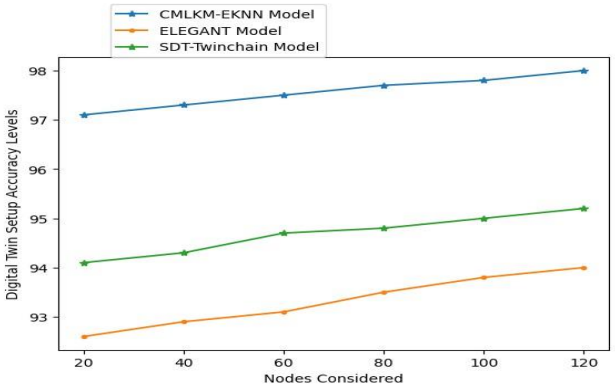


**Fig 5:** Digital Twin Setup Accuracy Levels

The proposed model makes use of cryptography technique to generate the keys. The proposed model generates the key pairs that is used for node authorization and gaining the access for data processing. The Key Generation Time Levels of the proposed and traditional models are indicated in Table 3 and Figure 6.

**Table 3:** Key Generation Time Levels

| Nodes Considered | Models Considered | | |
|---|---|---|---|
| | CMLKM-EKNN Model | ELEGANT Model | SDT-Twinchain Model |
| 20 | 14.9 | 20.1 | 23.1 |
| 40 | 15.1 | 20.3 | 23.2 |
| 60 | 15.3 | 20.5 | 23.4 |
| 80 | 15.6 | 20.6 | 23.5 |
| 100 | 15.8 | 20.9 | 23.9 |
| 120 | 16 | 21 | 24 |

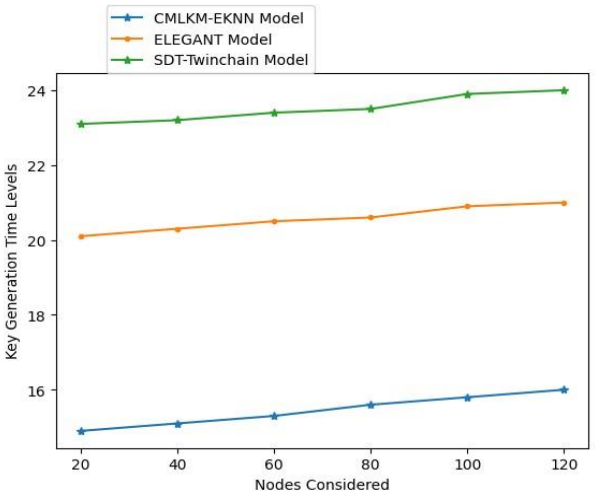


**Fig 6:** Key Generation Time Levels

The proposed model performs node authorization that is used to recognize normal and malicious nodes in the IoT

network. The node authorization is performed using a key in the key set. The Node Authorization Accuracy Levels of the proposed and existing models are represented in Table 4 and Figure 7.

**Table 4:** Node Authorization Accuracy Levels

| Nodes Considered | Models Considered | | |
|---|---|---|---|
| | CMLKM-EKNN Model | ELEGANT Model | SDT-Twinchain Model |
| 20 | 97.3 | 94.3 | 92.8 |
| 40 | 97.5 | 94.6 | 93 |
| 60 | 97.8 | 94.9 | 93.2 |
| 80 | 97.9 | 95.1 | 93.5 |
| 100 | 98.1 | 95.3 | 93.7 |
| 120 | 98.4 | 95.5 | 93.8 |

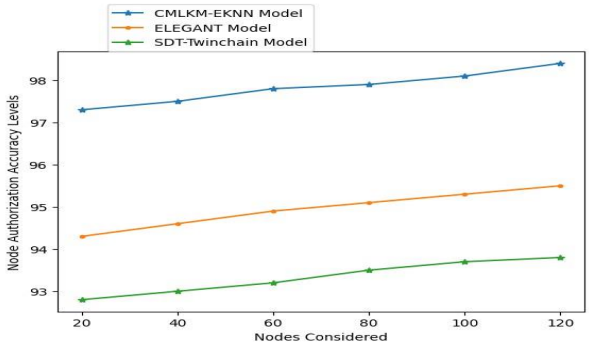


**Fig 7:** Node Authorization Accuracy Levels

The data patterns in the DT gathered is identified and the minute changes in the node levels are recognized. The changes in data pattern indicate the cause of intrusion in the network. The minute data patterns are verified among the authorized nodes to detect the malicious nodes. The Table 5 and Figure 8 represent the Data Pattern Analysis Accuracy Levels of the proposed and existing models.

**Table 5:** Data Pattern Analysis Accuracy Levels

| Nodes Considered | Models Considered | | |
|---|---|---|---|
| | CMLKM-EKNN Model | ELEGANT Model | SDT-Twinchain Model |
| 20 | 97.5 | 93.7 | 95 |
| 40 | 97.6 | 93.9 | 95.2 |
| 60 | 97.9 | 94.1 | 95.4 |
| 80 | 98.1 | 94.3 | 95.5 |
| 100 | 98.4 | 94.6 | 95.8 |
| 120 | 98.6 | 94.8 | 96 |

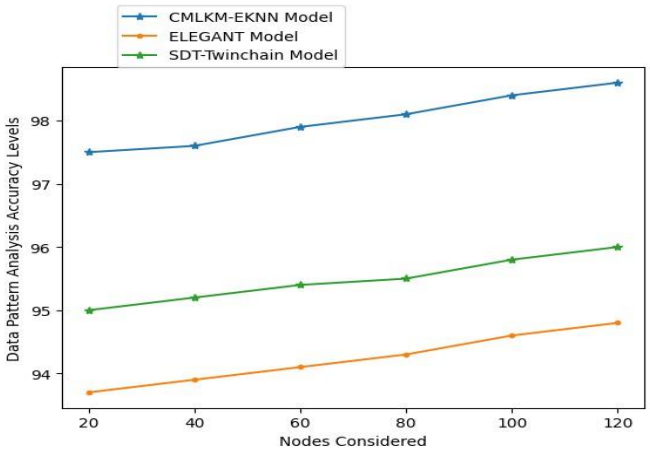


**Fig 8:** Data Pattern Analysis Accuracy Levels

The EKNN model is applied that considers the best K value and performs the accurate classification of normal and malicious nodes in the network. The pattern changes are detected accurately and nodes causing the intrusions will be detected and then mitigated to improve the network life time. The Table 6 and Figure 9 shows the EKNN based Intrusion Detection Accuracy Levels of the existing and proposed models.

**Table 6:** EKNN based Intrusion Detection Accuracy Levels

| Nodes Considered | Models Considered | | |
|---|---|---|---|
| | CMLKM-EKNN Model | ELEGANT Model | SDT-Twinchain Model |
| 20 | 97.6 | 94.3 | 93.2 |
| 40 | 97.9 | 94.6 | 93.6 |
| 60 | 98.1 | 94.9 | 93.9 |
| 80 | 98.3 | 95.1 | 94.1 |
| 100 | 98.5 | 95.3 | 94.3 |
| 120 | 98.6 | 95.5 | 94.6 |

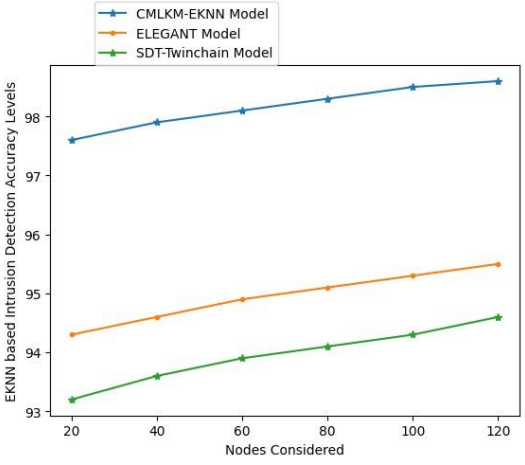


**Fig 9:** EKNN based Intrusion Detection Accuracy Levels

## 5. Discussion

The integration of Internet of Things (IoT) devices into modern culture offers advanced connectivity and remote control but exposes these devices to security threats due to their complexity and diversity. The paper introduces a solution involving cryptography and pairwise key generation for enhancing security in digital twin-based IoT systems. This approach emphasizes the need for a comprehensive and proactive approach to IoT security, encompassing hardware, software, and network infrastructure. The study's focus is on addressing security concerns in Industry 4.0, particularly in the context of digital twin technologies integrated into cyber-physical systems. The paper highlights the significance of intrusion detection systems (IDSs) in safeguarding complex and time-driven industrial processes and acknowledges the unique challenges faced by IDSs in industrial settings with legacy technologies. The proposed cryptographic approach, where data is encrypted using keys generated solely by the receiving node, enhances security for IoT devices and their data. The research's results, including data pattern analysis accuracy and intrusion detection accuracy, demonstrate the effectiveness of the proposed model compared to existing solutions.

## 6. Conclusion

Hundreds of millions of interoperable devices that require little to no human intervention make up what is known as the IoT. IoT is a rapidly expanding field in computing; nevertheless, due to the internet's notoriously hostile atmosphere, IoT is susceptible to a wide variety of assaults. A feasible solution would be to implement safeguards for IoT networks, including anomaly detection, to address this issue. Attacks can never be completely prevented, but the key to effective defense is early detection. Traditional, high-end security solutions are inadequate for protecting an IoT system due to the limited storage capacity and processing capability of IoT devices. Longer durations of connection between IoT devices without human intervention are also a recent development. In light of this, it is imperative to create intelligent network-based security solutions, such as machine learning solutions. There has been a dearth of research into attack detection in IoT networks, despite the abundance of literature on ML solutions for generalized detection problems. In the forthcoming age of industry 4.0, digital twins are expected to play a pivotal role. The thing it symbolizes can benefit from a digital twin that exists in the cloud. It is observed that digital twins, when coupled with a cyber physical system, can have embedded control systems, resulting in substantial performance and configurability advantages. However, shifting controllers to a digital duplicate on the cloud opens them up to new attack vectors. Given the complexity of such systems and the wide variety of countermeasures that might be taken, intrusion detection is crucial to ensuring the security of such systems. When it comes to safeguarding networked systems, IDSs play a crucial role. One of the few techniques with the ability to stop zero-day attacks is an IDS. It is common practice for evasion tactics to be used in tandem with various intrusion detection solutions. Unlike its counterparts in the IT and telecommunications industries, IDSs in industrial systems must keep tabs on processes that are often automated and time-driven. Furthermore, such systems often incorporate numerous legacy technologies that are either difficult to update or prohibitively expensive to do so. The capacity to connect and remotely control various gadgets via the IoT has made it an integral part of modern culture. However, the complexity and heterogeneity of these devices renders them particularly susceptible to attacks and breaches, which is of highest concern. Firewalls and IDS may not be enough to protect IoT devices; instead, smarter procedures that can handle varying degrees of data flow are required. In order to identify malicious nodes in digital twin based IoT, this research proposed a cryptography based on pairwise key generation. Public and private keys have been jointly generated by the source node and the destination. Both data encryption and decryption use the same key. The major advantage of this method is that data is encrypted with keys created by the receiving node only. Protecting IoT devices with digital twins and the data they produce requires, in the end, a holistic and preventative approach to IoT security for attack mitigation. The hardware, software, and network infrastructure should all be taken into account in this strategy. This method ensures the safety and security of DT IoT devices in the modern, interconnected environment. Cryptography enabled Multi Level Key Management using Enhanced K-Nearest Neighbor model that generates a key set in the IoT network for making strong authentication is proposed in this research. The proposed model key set contains key pairs that can be used for only one time to avoid attackers to reuse the keys for attacking the network. The EKNN model is applied on the DT model for accurate intrusion detection and then mitigation of attacks using strong node authorization model. In future, hybrid deep learning models can be applied on the DT nodes in IoT network for accurate intrusion detection with dynamic patterns so that new attacks can also be detected to improve the QoS levels.

## References

[1] B. Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenço and T. Cruz, "ELEGANT: Security of Critical Infrastructures With Digital Twins," in IEEE Access, vol. 9, pp. 107574-107588, 2021, doi: 10.1109/ACCESS.2021.3100708.

[2] P. Kumar, R. Kumar, A. Kumar, A. A. Franklin, S. Garg and S. Singh, "Blockchain and Deep Learning for Secure Communication in Digital Twin Empowered Industrial IoT Network," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2802-2813, 1 Sept.-Oct. 2023, doi: 10.1109/TNSE.2022.3191601.

[3] A.Khan, F. Shahid, C. Maple, A. Ahmad and G. Jeon, "Toward Smart Manufacturing Using Spiral Digital Twin Framework and Twinchain," in IEEE Transactions on Industrial Informatics, vol. 18, no. 2, pp. 1359-1366, Feb. 2022, doi: 10.1109/TII.2020.3047840.

[4] Z. Q. Wang and A. El Saddik, "DTITD: An Intelligent Insider Threat Detection Framework Based on Digital Twin and Self-Attention Based Deep Learning Models," in IEEE Access, vol. 11, pp. 114013-114030, 2023, doi: 10.1109/ACCESS.2023.3324371.

[5] J. Wu, Y. Wang, H. Dai, C. Xu and K. B. Kent, "Adaptive Bi-Recommendation and Self-Improving Network for Heterogeneous Domain Adaptation-Assisted IoT Intrusion Detection," in IEEE Internet of Things Journal, vol. 10, no. 15, pp. 13205-13220, 1 Aug.1, 2023, doi: 10.1109/JIOT.2023.3262458.

[6] J. Wu, H. Dai, Y. Wang, K. Ye and C. Xu, "Heterogeneous Domain Adaptation for IoT Intrusion Detection: A Geometric Graph Alignment Approach," in IEEE Internet of Things Journal, vol. 10, no. 12, pp. 10764-10777, 15 June15, 2023, doi: 10.1109/JIOT.2023.3239872.

[7] J. Liu, D. Yang, M. Lian and M. Li, "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," in IEEE Access, vol. 9, pp. 38254-38268, 2021, doi: 10.1109/ACCESS.2021.3063671.

[8] M. Zeeshan et al., "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets," in IEEE Access, vol. 10, pp. 2269-2283, 2022, doi: 10.1109/ACCESS.2021.3137201.

[9] M. Eskandari, Z. H. Janjua, M. Vecchio and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882-6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.

[10] A.Oseni et al., "An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 1, pp. 1000-1014, Jan. 2023, doi: 10.1109/TITS.2022.3188671.

[11] G. Prettico, M. G. Flammini, N. Andreadou, S. Vitiello, G. Fulli and M. Masera, "Distribution system operators observatory 2018—Overview of the electricity distribution system in Europe", 2019.

[12] C. Foglietta, D. Masucci, C. Palazzo, R. Santini, S. Panzieri, L. Rosa, et al., "From detecting cyber-attacks to mitigating risk within a hybrid environment", IEEE Syst. J., vol. 13, no. 1, pp. 424-435, Mar. 2019.

[13] V. Graveto, L. Rosa, T. Cruz and P. Simões, "A stealth monitoring mechanism for cyber-physical systems", Int. J. Crit. Infrastruct. Protection, vol. 24, pp. 126-143, Mar. 2019.

[14] Xu, Qinghua et al. “Digital Twin-based Anomaly Detection in Cyber-physical Systems.” 2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST) (2021): 205-216.

[15] Z. Wu, H. Zhang, P. Wang, and Z. Sun, “RTIDS: A robust transformer-based approach for intrusion detection system,” IEEE Access, vol. 10, pp. 64375–64387, 2022.

[16] R. Nasir, M. Afzal, R. Latif, and W. Iqbal, “Behavioral based insider threat detection using deep learning,” IEEE Access, vol. 9, pp. 143266–143274, 2021.

[17] B. Sharma, P. Pokharel, and B. Joshi, “User behavior analytics for anomaly detection using LSTM autoencoder–insider threat detection,” in Proc. 11th Int. Conf. Adv. Inf. Technol., Jul. 2020, pp. 1–9.

[18] W. Huang, H. Zhu, C. Li, Q. Lv, Y. Wang, and H. Yang, “ITDBERT: Temporal-semantic representation for insider threat detection,” in Proc. IEEE Symp. Comput. Commun. (ISCC), Sep. 2021, pp. 1–7.

[19] F. Meng, F. Lou, Y. Fu, and Z. Tian, “Deep learning based attribute classification insider threat detection for data security,” in Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC), Jun. 2018, pp. 576–581.

[20] M. Singh, B. M. Mehtre, and S. Sangeetha, “User behavior profiling using ensemble approach for insider threat detection,” in Proc. IEEE 5th Int. Conf. Identity, Secur., Behav. Anal. (ISBA), Jan. 2019, pp. 1–8.

[21] D. Sun, M. Liu, M. Li, Z. Shi, P. Liu, and X. Wang, “DeepMIT: A novel malicious insider threat detection framework based on recurrent neural network,” in Proc. IEEE nt. Conf. Comput. Supported Cooperat. Work Design (CSCWD), May 2021, pp. 335–341.

[22] F. Liu, Y. Wen, D. Zhang, X. Jiang, X. Xing, and D. Meng, “Log2vec: A heterogeneous graph embedding based approach for detecting cyber threats within enterprise,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Nov. 2019, pp. 1777–1794.

[23] X. Larriva-Novo, V. A. Villagrá, M. Vega-Barbas, D. Rivera and M. S. Rodrigo, "An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets", Sensors, vol. 21, no. 2, pp. 656, Jan. 2021, [online] Available: https://www.mdpi.com/1424-8220/21/2/656.

[24] S. I. Popoola, B. Adebisi, R. Ande, M. Hammoudeh, K. Anoh and A. A. Atayero, "SMOTE-DRNN: A deep

learning algorithm for botnet detection in the Internet-of-Things networks", Sensors, vol. 21, no. 9, pp. 2985, Apr. 2021, [online] Available: https://www.mdpi.com/1424-8220/21/9/2985.

[25] A.Churcher, R. Ullah, J. Ahmad, S. ur Rehman, F. Masood, M. Gogate, et al., "An experimental analysis of attack classification using machine learning in IoT networks", Sensors, vol. 21, no. 2, pp. 446, Jan. 2021, [online] Available: https://www.mdpi.com/1424-8220/21/2/446.

[26] Y. Yang, K. Zheng, C. Wu and Y. Yang, "Improving the classification effectiveness of intrusion detection by using improved conditional variational AutoEncoder and deep neural network", Sensors, vol. 19, no. 11, pp. 2528, Jun. 2019, [online] Available: https://www.mdpi.com/1424-8220/19/11/2528.

[27] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques", IEEE Internet Things J., vol. 8, no. 5, pp. 3242-3254, Mar. 2021.

[28] N. Guizani and A. Ghafoor, "A network function virtualization system for detecting malware in large IoT based networks", IEEE J. Sel. Areas Commun., vol. 38, no. 6, pp. 1218-1228, Jun. 2020.

[29] O. Alkadi, N. Moustafa, B. Turnbull and K.-K.-R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks", IEEE Internet Things J., vol. 8, no. 12, pp. 9463-9472, Jun. 2021.

[30] M. Ahmad, Q. Riaz, M. Zeeshan, H. Tahir, S. A. Haider and M. S. Khan, "Intrusion detection in Internet of Things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set", EURASIP J. Wireless Commun. Netw., vol. 2021, no. 1, pp. 1-23, Dec. 2021.