A Scalable Multi-Attribute-Based Non-Replicative Authentication for CPS Based Cloud Resource Sharing

Dr. N. Sowri Raja Pillai[1], S. Ajay[2], V.Hariharan[3], N.Vimalraj[4] J. Kumaran [5]
Department of Information Technology,
RAAK College of Engineering and Technology,
Puducherry, India.
sowrirajacse@gmail.com

Abstract – With the rapid adoption of Cyber-Physical Systems (CPS) integrated with cloud computing environments, ensuring secure resource sharing is becoming increasingly critical. This paper presents a novel authentication framework designed to address security concerns in CPS-based cloud resource sharing environments. The proposed solution introduces a scalable, multi-attribute-based, non-replicative authentication mechanism that enables secure and efficient resource access. By utilizing a combination of unique attributes such as device identity, context information, and environmental factors, our approach mitigates the risk of unauthorized access while preventing the replication of authentication credentials. The framework ensures robust protection against common attacks in cloud environments, including unauthorized access and credential theft. Through simulation and performance evaluations, we demonstrate the effectiveness and scalability of the proposed method in large-scale CPS networks. This solution significantly enhances the security, scalability, and reliability of cloud-based resource sharing in CPS ecosystems, contributing to a safer and more efficient deployment of interconnected systems.

Index Terms – Cybersecurity, Cyber Physical Systems (CPSs), Deep Learning (DL), Attack detection.

1. INTRODUCTION

Cyber-physical systems (CPSs) are inducing profound changes in the modern society. Composed of computation, communication, and physical systems and processes, CPS integrate, and coordinate heterogeneous components with increasing intelligent, interactive, and distributed operations in the modern critical infrastructures. The emerging smart grid, being one of the most complex CPS ever built in history, witnesses such transformations during the ongoing integration of power and energy systems with information and communication technologies (ICTs) [22]. The fundamental changes in this critical infrastructure are leading toward far-reaching impacts on not only the energy, but also a number of critical interdependent sectors. The smart grid encompasses complex systems of power, energy, control, sensory, computing, and communication. The complexity and heterogeneity in this architecture have underscored the potential challenges to its security and resilience. On one hand, the interconnection of bulk power systems is complicating the protection against inherent physical vulnerabilities therein. On the other hand, the cyber-integration requires substantial investments on security designs and upgrades against unforeseen patterns and threats from the cyberspace. The collective research effort on Cybersecurity and physical security have been striding fast and fostering a new area of CP security for the smart grid [23].The Cyber-physical Systems (CPSs) combine the physical and digital worlds, where embedded digital controllers interact with the physical world through environmental sensors and actuators [24]. Our modern world is reliant on their function—from when you turn your lights on in the morning, which requires electrical generation and distribution (smart grids), to having your smart coffee machine brew your morning coffee automatically based on your wake-up time, to your commute via car, bus, train, or e-bike, which is enhanced by integrated embedded systems for both their operation and in their manufacturing processes. It is thus

imperative that designers of CPSs take into account security when implementing their systems.

This is not trivial, as illustrated by the range of high profile CPS attacks including the Stuxnet worm damaging Iranian centrifuges [25], the German Steel Mill attack, which prevented a blast furnace from shutting down and caused significant damage [26], and the ransomware attack on Colonial Pipeline, which caused serious disruption to gasoline supply in the United States and resulted in a multi-million dollar payout to the attackers [27]. However, attacks are not just limited to industrial plants, Internet of Things (IoT) devices have been compromised and used to launch Distributed Denial of Service (DDoS) attacks [28], [29] weaknesses in over-the-counter drones have been demonstrated [30], and compromise of Additive Manufacturing (AM) can cause propeller defects which fail in flight [31].

A. Cyber-Physical Systems

The main differences between IT and cyber-physical systems security in general are highlighted by Cardenas et al. 2009, 2011) and the Manufacturing and Cyber divisions of the National Defense Industrial Association (NDIA) [15–17]. Although the authors use Industrial Control Systems (ICSs) as representatives of cyber-physical systems, the differences discussed next are still true for almost any other cyber-physical system, such as production systems. The first difference is that patching and continuous updates, common practices in IT systems security, are not well suited for CPS [15–17]. Due to high equipment and downtime costs, frequent updates may not be possible in CPSs, since updates would require getting certain equipment offline and not being able to perform its function for a certain amount of time. Realtime availability is of utmost importance in CPSs [13]. Furthermore, it may take months just to plan for an upgrade and could be difficult to financially justify on regular basis [12-13]. Another difference is the presence of a large number of legacy equipment in CPSs when compared to IT systems [13]. The issue with legacy equipment is that they are, as a result of their age, less secure than the more advanced recent equipment. Due to being old and not being able to necessarily get frequent updates, such equipment would contain more weaknesses, which can be exploited more easily during cyberphysical attacks. In addition, much of these equipment would have a diverse range of operating systems [17]. Such a wide range of operating systems not only makes it tough for different equipment to communicate together, but it also makes the equipment more difficult to update and consequently more vulnerable. Perhaps the most obvious and significant difference here is the “physical” aspect of CPSs, i.e., their interaction with the physical world [13]. With the focus of computer and IT security on information protection, it is not enough to rely on computer and IT systems security measures as they do not consider how cyber-attacks would affect the physical world; i.e., IT security is necessary but not sufficient for CPS security [23]. With such a physical aspect, there are now human safety concerns associated with the security of CPSs [25], including operators, personnel, and customers’ safety. This physical aspect also means that there are additional intrusion detection options in CPS. Traditional firewalls may prevent intrusions from outside the system, but not attacks from inside the system, such as those by disgruntled employees .

B. Cyber-Physical Production Systems

The nature of production systems themselves also plays a role in the inefficiency of just applying regular IT security measures to achieve cyber-physical security. Current manufacturing enterprises consist of a large number of heterogeneous components with a wider range of security requirements such as controllers, machining equipment, assembly equipment, post-processing equipment, and inspection equipment. Furthermore, cyber-physical production systems have a more complex IT structure, with more security concerns. Those diverse technological components communicate together through a wide variety of architectures, protocols, and network technologies that are not necessarily available in regular IT systems. For instance, MTConnect1 is a new emerging communication protocol between manufacturing equipment [22]. Additionally, manufacturing has currently entered the Industry 4.0 era with more emphasis on easier automation and data exchange. Along with the Internet of Things (IoT), more manufacturing equipment (other than computers) is now connected to the Internet such as sensors, cameras, etc. Industry 4.0 has also

resulted in even more connectivity to easily extract and share data with cloud computing and new communication protocols. This increased connectivity has led to a growing reliance on creating almost everything within a digital environment using Computer-Aided Engineering (CAE) support tools, such as Computer-Aided Design (CAD) and Manufacturing (CAM) software, resulting in more security concerns. All the aspects discussed in this section show that cyberphysical production systems have additional security requirements. Therefore, for securing cyber-physical production systems, more tools are needed along with the available traditional IT cyber-security tools, ones accounting for the physical aspect in particular. A review of the current research efforts in the field of cyber-physical security for production systems is presented next.

C. Cyber-Physical Security Efforts in Production Systems

The focus of current cyber-physical security research efforts for production systems has been traditionally on security issues regarding ICSs and Supervisory Control and Data Acquisition (SCADA) networks [21]. As a result, the security of production systems has been grouped into the generic area of critical infrastructure [21,25] such as electric power grids, water and waste management systems, and transportation systems [29]. However, production systems are becoming more sophisticated. In addition, control systems are just one component within production systems and a cyber-physical attack can occur anywhere within the manufacturing enterprise and the corresponding supply chains.

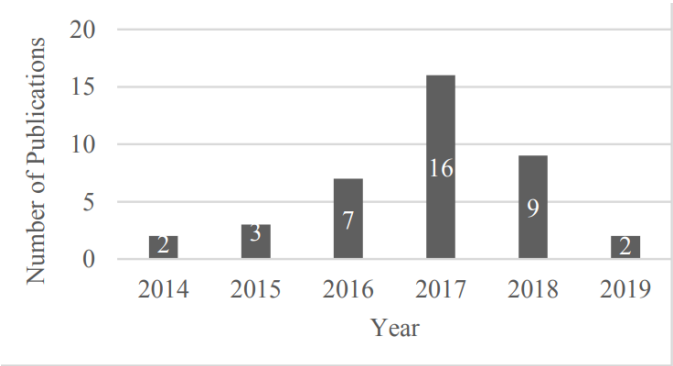


Fig 1. Number Of Reviewed Publications In This Field In The Last 5 Years.

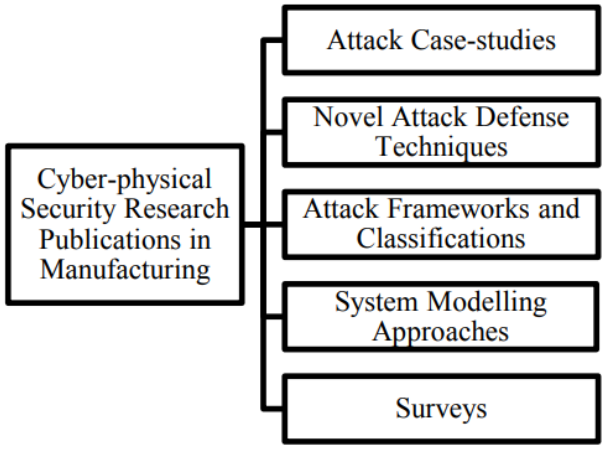


Fig 2. Identified Categories For The Cyber-Physical Security Research Publications In Manufacturing.

In fact, ICSs and manufacturing could be viewed, despite potentially overlapping, as two separate domains [31], having different objectives and implementation techniques [26]. Hence, although the security of ICSs could encompass manufacturing processes [31], the review here is more concerned with the security of production processes alone, rather than focusing on the control systems included. Research in the field of cyber-physical security of production systems is relatively new but has been expanding quickly. In this work, about forty relevant research publications have been reviewed that were published since the year 2014. A breakdown of the reviewed publications by year is shown in Fig 1. It can be seen from the figure that there has been a slight steady increase in the number of publications between 2014 and 2016. Afterwards, the amount of publications has significantly increased starting from the year 2017. The majority of the publications in this specific field can be broken down into five main categories: 1) cyber-physical attacks case-studies, 2) novel cyber-physical attack defense techniques, 3) cyber-physical attack frameworks and classifications, 4) system modelling approaches, and 5) surveys; as shown in Fig 2.

D. Attack Case-studies

The first area within the field of cyber-physical security for manufacturing includes research publications showcasing different small-scale cyber-physical attack examples and their effects on the manufactured products. Researchers in this area typically aim to also raise awareness about the issue of cyberphysical security in manufacturing through demonstrating the relative ease of applying a cyber-physical attack to a specific production process. As an example, Wells et al. (2014) discussed some of the cyber-security related weaknesses existing in production systems before presenting a case-study for a subtractive manufacturing process [29]. In the case-study, the manufacturing of a tensile test specimen on a Computer Numerical Control (CNC) milling machine was attacked through altering the tool path files as part of an undergraduate student project. The purpose of the case-study was not only to demonstrate the attack feasibility, but also to assess the diagnostic abilities of future engineers [29]. None of the student groups involved were able to identify the existence of an attack, with three out of seven students groups not even bothering to measure the final product since it “looked correct” [29]. Turner et al. (2015) went into more detail about the just mentioned case-study and echoed the concerns by Wells et al. (2014) of the lack of enough awareness about cyber-physical security [15]. In addition to discussing this case study, the authors also analyzed some potential attack surfaces2 within manufacturing such as the design tool chain, control, and direct equipment attack surfaces, among others [17]. In another publication, Zeltmann et al. (2016) presented an example of a cyber-physical attack on an additive manufacturing process [17]. The authors first started by providing an overview of potential risks existing in the field of additive manufacturing before presenting their attack casestudy [18]. Also using tensile test specimens, they investigated the effects of two types of changes in additive manufacturing; namely, embedding internal defects and altering the printing orientation [48]. Two types of non-destructive testing were then used to demonstrate the decreased performance and evaluate attack detectability. Specifically, ultrasonic inspection and Finite Element Analysis (FEA) techniques were used for the cyber-physical attacks detection and to evaluate their effects, respectively [18]. The results showed that both types of attacks were not easily detectable and would have a negative impact on the material’s performance. In the same setting of additive manufacturing, Belikovetsky et al. (2016) presented an interesting case-study with the aim of sabotaging a manufactured functional part [29]. In doing so, the authors also proposed an approach to identify attack opportunities3 , analyzed the attack’s full chain, and develop a methodology to assess attack difficulty in additive manufacturing [28]. In the demonstrated attack, a 3D printed propeller of the quadcopter was compromised remotely through maliciously changing its design file, causing the quadcopter to collapse while flying [29]. To make the attack successful, the authors had to design it in such a way that the change was not noticeable and, at the same time, the product does not fail right away during operation, requiring them to experiment with different design iterations first [29]. In addition to having to do some trial-and-error experimentation, this attack also required at least some type of basic knowledge with the product and process involved.

2. RELATED WORK

Recently, regarding the increasing number of attacks in industry, many researchers have been attracted to this problem, and some studies have been done. Authors of [15] have proposed a method to detect the threats in IIoT based on Hidden Markov Model (HMM). In this method, HMM is used to model sequential data which is generated from IIoT devices. A Genetic Algorithm (GA) is applied to optimize the parameters of HMM. Also, a dynamic window-based sequence extractor has been proposed to extract multiple sequences simultaneously before processing by multi-HMM. In [16], an anomaly detection method has been proposed for IIoT named ASTREAM, which can accomplish efficient and accurate anomaly detection with good scalability. This method merges the sliding window, change detection, and model update strategies into LSHiForest, and it can effectively handle the infiniteness, correlations, and distribution change of data streams. Trust affects the consumption pattern of a specific service that is provided by an IIoT device. However, due to the lack of perception in machines, trust cannot be built especially since each object is interpreted differently and different applications running on the IIoT devices may assign different trust scores. Hence, the authors of [17] first propose trust metrics. Then, they present a trust model based on the neutrosophic weighted product method (WPM) used by IIoT applications to assess IIoT devices' trust scores. The developed model assesses devices' trustworthiness based on the spatial knowledge, temporal experience, and behavioral patterns retrieved from the IIoT devices. Finally, they use neutrosophic K-NN clustering and neutrosophic support vector machines (SVM) to classify the extracted characteristics to generate the final trust score and make a decision. Generally, available methods for attack detection can be divided into two different groups: model-based methods, like designing estimators, and data-based methods, like using machine learning methods. Here, we survey some of these methods. Some studies have proposed using machine learning (ML) algorithms to detect attacks. These algorithms can be employed to learn normal behavior from available data and then compare measured samples with these learned models to determine if that is anomalous or not. In [18], a review of recently proposed deep learning (DL) solutions for detecting cyber-attacks has been provided that shows DL modules can be used to detect cyber-attacks. Also, some studies have proposed model-based methods. In [19], a distributed filtering algorithm is proposed to estimate the system state, and an attack detector is designed by considering a dynamic threshold. The authors of [20] proposed adding watermarking signals to the control inputs and checking received observations by various statistical tests to detect attacks. However, adding these watermarking signals can increase the control cost. In this paper, they tried to reduce the control cost when the system is not under attack. The authors of [21] also proposed adding the watermarking signal to control input by designing a dual-rate control framework, including a model predictive controller and a state-feedback predictor-based controller. Also, they consider a reconfiguration block to mitigate the effects of the watermarking signal on control costs.

Anomaly and intrusion detection in industrial control systems (also called cyber physical systems) have been extensively studied. A number of comprehensive surveys are dedicated to the classification of techniques and methodologies in this area (e.g., [1] and [2]). A well-known approach to intrusion detection in ICS is based arXiv:1806.08110v2 [cs.CR] 10 Dec 2018 on modeling and simulation of the system [3], [5]. Practical problems with this approach are the need for precise knowledge of the system's design and configurations, as well as the need to accurately modeling the system's complex physical behavior. According to Mitchell et al. [2], ICS anomaly detection methods include knowledge and behavior-based methods. Knowledge-based detection techniques search for known attack characteristics, similar to malware signature techniques in IT intrusion detection. While having low false positive rates, these approaches require maintaining an updated dictionary of attack signatures and are ineffective against zero-day attacks. In contrast, behavior-based techniques search for anomalies in runtime behavior. These techniques are more common in ICS intrusion detection, since ICS systems are automated and present more regularity and predictability than typical IT systems. The proposed method utilizes behavior-based techniques.

Another approach to classifying intrusion detection methodologies is based on the data being monitored. Numerous studies have presented network traffic-based intrusion detection [3]. Ghaeini et al. [6] use this approach on the SWaT dataset used in our study. In this work we have study an alternative approach based on the data collected from the sensors and actuators, thus focusing on the system behavior at the physical layer. Anomaly detection techniques used in ICS intrusion detection can be broadly divided into supervised, unsupervised and semisupervised techniques. Supervised techniques require prior labeling of the system behavior, including the samples of malicious behavior. Acquiring precise and representative labeled data is very hard to obtain in practice, and this data is highly dependent on the specific system. Therefore, most of recent research on ICS intrusion detection uses unsupervised (unlabeled data from real data) [13] and semi-supervised (training from a set of clean data with no anomalies) approaches. Unsupervised SCADA intrusion detection was investigated in [7] which describes a technique based on one-class SVM and k-means clustering. Semi-supervised learning approaches are trained using a collection of "good" data, which is assumed to completely represent normal system behavior and contain no attacks. While both assumptions should be examined closely, they can be fulfilled in many practical situations. Semi-supervised methods usually have lower false-positive rates than their fully unsupervised alternatives [8], [9]. Multiple machine learning techniques are used in ICS anomaly detection. They include support-vector machine [7] [10], random forest [1] as well as artificial neural network [3], [11] and others. In the past few years some research has been performed applying deep and recurrent neural networks to this area [15], [12], [13]. In our research 1D convolutional neural networks (1D CNNs) are used, and demonstrate superior attack detection abilities and higher F1 scores than previously published papers [12], [13]. Previously, 1D CNNs were used for detecting faulty motor bearings based on univariant motor current data [14]. In this study we apply 1D CNNs to multivariant time series data and use it to detect multiple instances of cyberattacks. To the best of our knowledge, our work is the first to use 1D CNNs for cyberattacks detection in ICSs.

3. MATHEMATICAL MODEL

In mathematical terms, the model for a scalable, multi-attribute-based, non-replicative authentication system can be formulated as follows:

1. Authentication Problem Setup:

Let’s define:

- U={u1,u2,...,un} as a set of users (or devices) that need to access cloud resources.
- A={a1,a2,...,am} as a set of attributes, where each user/device has a vector of attributes associated with them.

Each user u_i is associated with a vector of attributes:

$$\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{im})$$

where each a_{ij} is the j-th attribute of the i-th user, e.g., identity, location, time of access, etc.

- Let $R = \{r_1, r_2, \ldots, r_k\}$ be the set of cloud resources to which users may have access.

We assume that the cloud platform can classify resources based on attributes (e.g. r_1 may only be accessible to users with a specific location attribute).

2. Authentication Scheme:

The authentication process can be viewed as a function *F* that checks if a user can access a specific resource:

F:U×R×A→{valid,invalid}

For any user u_i, cloud resource r_j, and associated attribute vector a_i, the function returns "valid" if the attributes satisfy the access conditions for that resource, or "invalid" otherwise.

This access check can be performed using an attribute-based encryption scheme where:

- Let $E_{ai}(r_j)$ denote the encryption of resource r_j based on the attributes of user u_i

The ciphertext C_i is:

$$C_i = E_a(r_j)$$

and the decryption key K_i is provided only if the attributes of user u_i match the required access policy for r_j

3. Non-Replicative Authentication:

In a non-replicative authentication system, credentials (e.g., tokens, keys) should not be duplicated across users. One way to enforce this mathematically is by using a *one-time key* or *session token* that expires after a single use. Let:

- T_i represent a time-based or session-based authentication token for user u_i, which is valid only for a specific access request.

A non-replicative mechanism ensures that once T_i is used to authenticate a user, it cannot be reused or replicated for a different session. Mathematically, we could represent this as:

T_i^{used}→ invalid (no replication)

4. Scalability and Load Balancing:

Scalability refers to the system's ability to efficiently handle an increasing number of users and resources. A mathematical model for scalability can be defined by a cost function CCC that measures the system's performance in relation to the number of users *n* and resources *k*:

C(n,k) = sum i = 1 to n sum j = 1 to k f * (a_{i}, r_{j})

where $f(a_i, r_j)$represents the computation cost of authenticating user u_i for resource r_j given their

attributes. To ensure scalability, efficient algorithms like those based on distributed hashing or load balancing techniques (e.g., sharing) could be used to reduce the overall complexity.

5. Security and Trust Model:

The security of the authentication system can be modeled using a trust function *T*, which quantifies the level of trust in the user's credentials. Trust is based on factors like the legitimacy of attributes (e.g., time, location), the expiration of session tokens, and the integrity of the resource-sharing environment:

m T(i) = ∑g(ait) (ait ∈ valid range) t=1

where g(a_{it}) is a function that measures the validity of the attribute a_{it}, and II (a_{it} ∈ valid range) is an indicator function that is 1 if the attribute is valid and 0 otherwise.

6. Access Control Policy:

Finally, an access control policy *P* determines which users can access which resources based on their attributes. This can be expressed as:

P(ui, rj) = True if a Policy (rj)

where Policy (r_j) is a set of required attribute conditions for accessing resource r_j.

4. PROPOSED WORK

This proposed method utilized the Two-Layer Recurrent Learning (TLRL) architecture, replacing traditional MLPs for remote sensing (RS) scene classification tasks. By utilizing and comparing multiple pre-trained CNN and Vision Transformer (ViT) models, we identified the most suitable pairings for the TLRL.

A. Two-Layer Recurrent Learning

Two-Layer Recurrent Layer (TLRLs), inspired by the Kolmogorov-Arnold representation theorem, is an advanced type of neural network featuring learnable activation functions on edges, unlike the fixed activations on nodes in traditional Multi-Layer Perceptrons (MLPs). These activation functions are parameterized by B-splines, which are piecewise polynomial functions defined by control points and knots. Each input feature *xp* is transformed by spline parameterized functions $\varphi q,p$, aggregated into intermediate values for each q, and then passed through functions Φq. The final output $f(\mathbf{x})$ is the sum of these transformed values, allowing the network to flexibly and efficiently capture intricate data patterns. The activation functions in TLRLs are a combination of a Basis Function and a Spline, with the Basis Function often being the Sigmoid Linear Unit (SiLU), defined as silu(x) = x 1+e-x . The spline component spline(x) = Pi $ci$$Bi$($x$) uses B-spline basis functions $Bi(x)$ and coefficients ci, which are learned during training. These coefficients determine the

final shape of the activation functions, replacing the need for traditional linear transformation parameters W and b in MLPs. The formula for the TLRL is given by:

$$f(x) = \left(\sum_{q=1}^{2n+1} \Phi \sum_{p=1} \varphi_{q,p}(x_p)\right)$$

The function $f(\mathbf{x})$ in a TLRL, where $\varphi_{q,p}(x_p)$ are spline functions and Φq are transformations.

$$\varphi(x) = w\,(b(x) + \text{spline}(x))$$

$\varphi(x)$ denotes the activation function, w is a weight, $b(x)$ is the basis function and spline(x) is the spline function.

$$b(x) = \text{silu}(x) = X / 1 + e\text{-}x$$

$b(x)$ is the basis function, implemented as silu(x) (Sigmoid Linear Unit).

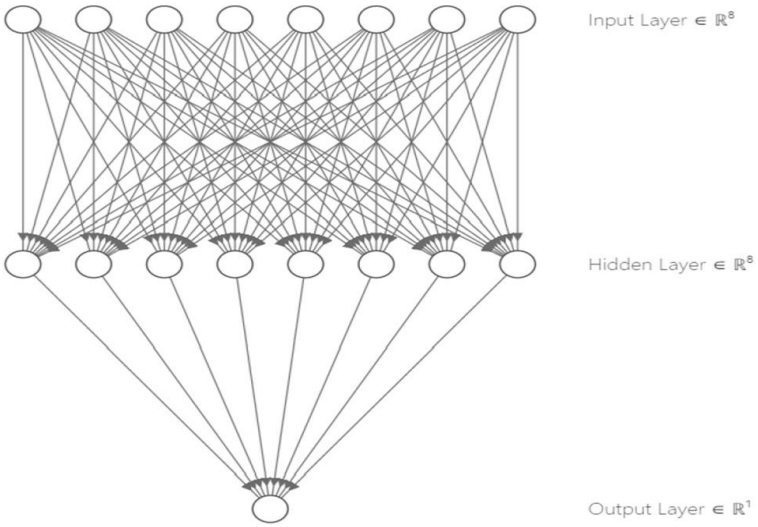
$$\text{spline}(x) = \sum c_i\, B_i(x)$$

spline(x) is the spline function, ci are the coefficients, and $Bi(x)$ are the B-spline basis functions.
TLRLs yield various advantages over MLPs, including better accuracy and interpretability with fewer parameters. They achieve this by having smaller architectures that can perform comparably or better than larger MLPs in tasks such as data fitting and partial differential equation (PDE) solving. Since TLRLs could be depicted, they are additionally helpful in discovering mathematical and physical laws in scientific applications. Moreover, TLRLs can aid in preventing catastrophic forgetting, a neural network problem when the learning of new information causes the loss of previously learned information.

B.Network for Feature Map and Similarity
The proposed algorithm integrates the ConvNeXt architecture with TLRL to enhance the learning capabilities of a pre-trained ConvNeXt model. The ConvNeXt model is first pre-trained and its layers are frozen to preserve the learned features. In place of the traditional MLP classifier, the model introduces two TLRL Linear layers. The TLRL Linear layers utilize learnable activation functions on the edges instead of fixed activation functions on the nodes, as in traditional neural networks. These activation functions are
represented as B-splines, which offer more flexibility
and stability. The TLRLLinear layer replaces linear weights with these spline functions, allowing the model to adapt more effectively to the input data. We used multiple strategies to evaluate the TLRL's performance
for RS classification tasks in remote sensing. The Two layers of the proposed RL is depicted in the below Fig.

The window size for recurrent operations is represented by m, n, and a,b, which represent stride sizes, and feature map represents a rectilinear unit model for activation of feature sets. Upon studying our set of similarity features, we initially defined nine classes of interest: Agricultural, Cloud, Desert, Mountain, Natural, River, Sea ice, Snow, and Water. All of these classes are representative of geological features or, in the case of Cloud, atmospheric features that can be directly discerned from the color and texture of the corresponding similarity feature. Defining classes with distinct visual features (i.e., the meandering pattern of a river or the white color of snow) was necessary to guide our group of expert labelers in their decision process, as no geo-reference was obtained for the images during acquisition. In

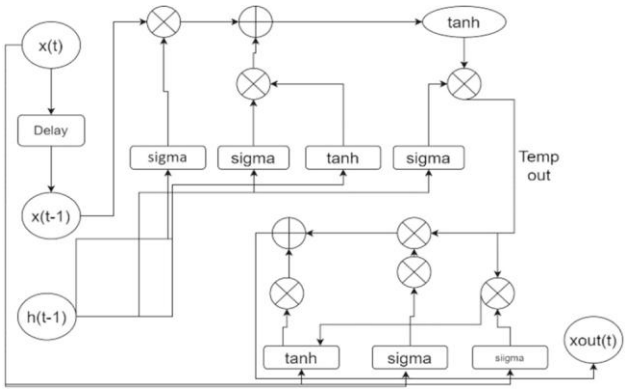
particular, we defined Natural similarity features as rural, not-exploited lands that are not mountains or deserts and do not include rivers or traces of human activities. The feature that distinguishes Natural and Agricultural similarity features is the absence/presence of human-cultivated crops. In the case of snowy mountains, the labelers were asked to label as \Snow" those similarity featurees containing more than 50% of snow pixels.



However, similarity features lacking distinguishing features, including artifacts or enhanced noise due to the image preprocessing step, still exhibited significant ambiguity. For example, similarity features containing water without coastal areas were often indistinguishable from desert similarity features, especially when their colors appeared significantly distorted. This difficulty, however, could be mitigated by contextualizing the similarity feature within the entire feature mapimage to enable the labeler to grab additional information from the surrounding similarity features. To this end, we equipped the labelers with complete, feature mapsatellite images.We enforced a strict voter consensus to avoid including ambiguous similarity features in the dataset. More precisely, all similarity features with a voter consensus of less than 6 out of 8 votes were discarded. Checking the discarded similarity features after the labeling campaign confirmed that these contained either blurry or noisy visuals or featured overlapping classes.

C.Training for Low/ High Similarity

To prevent similarity deviations between the training and test sets, which could result in underestimating the true classification error, we made the train/test splitting at image level. In other words, all the features classified from the same image were either included as part of the training or the test set but never distributed between them. In particular, the training set was populated by using 10 labeled features per class by selecting those with perfect agreement among the labelers. Furthermore, we provided the satellite images to be used by the competitors to procure unlabeled data. At this point, our general competition design had progressed already so far that it was certain that we would use the one-layer RL for the ML model of our choice. We trained this RL on several different dataset splits and measured its performance not only as a proof of concept but also to select a dataset split of good quality. The network model for classification (1-Layer) is illustrated in the below Fig.



At first, the proposed model pulls out many different sets of features from each image. These feature sets are extracted via a novel combination of high and low representation techniques. The reason for combining these techniques is due to their differential feature representation characteristics. The above representation where different variance operations are combined with tangent operations to identify multimodal feature sets. The model initially extracts initialization (i), temporal feature (f), and temporal output features via Eqs. below as follows,

$$i = var(xin * U^{1} + ht\text{-}1 * W^{2})$$

$$f = var(xin * Uf + h_{1}\text{-}1 * Wf)$$

$$o = var(xin * U^{\circ} + ht\text{-}1 * W^{\circ})$$

Where *U*&*W* represents variance constants for the high & low similarity processes, while *h* is a kernel matrix used to activate of these features. These features are combined to form a temporal recurrent feature set (C)

$$o = var(xin * U^{\circ} + ht\text{-}1 * W^{\circ})$$

These feature sets are capable of representing input images into multimodal sets. However, this feature extraction technique's efficiency must be validated to estimate efficient augmentation operations. When all possible solutions have been found, pick the one with the highest fitness level and use its features to classify satellite images. This classification is done via a TLRL, wherein various recurrent, max pooling & drop out layers are connected to estimate augmented feature sets. The RL processes high & low similarity features and classifies them into land-specific categories.

5. CONCLUSION

The increasing complexity of CPS, coupled with the growing reliance on cloud infrastructures, demands robust authentication methods to protect sensitive resources and ensure secure, efficient, and scalable access control mechanisms. The proposed framework leverages multiple attributes associated with users and devices—such as identity, location, and device-specific characteristics—to establish a more comprehensive and secure authentication process. By using multi-attribute-based authentication, we enhance the security of the system, ensuring that access to cloud resources is only granted when all required conditions are met. This approach reduces the risk of unauthorized

access and strengthens the overall trustworthiness of the system. This framework not only enhances the security and integrity of the cloud resource-sharing process but also lays the groundwork for further advancements in the field of CPS security. Future research could explore the integration of advanced cryptographic methods and further optimizations to handle even more complex and dynamic CPS architectures.

6. FUTURE WORK

1. **Integration of Advanced Cryptographic Techniques**:
   - One potential area for future work is the integration of **advanced cryptographic techniques** such as **homomorphic encryption**, **attribute-based encryption (ABE)**, and **blockchain technology** to further strengthen security. These methods could provide enhanced privacy, integrity, and auditability, ensuring that sensitive data remains secure during theauthentication and resource-sharing processes in a decentralized cloud environment.

2. **Dynamic Attribute Management**:

   - In real-world CPS environments, the attributes of users and devices may change over time (e.g., location, device status, or role). Future work could focus on **dynamic attribute management** and the development of policies that can adapt in real-time to these changes. Implementing **dynamic attribute revocation** and **refreshment mechanisms** would ensure the system remains secure and up to date as conditions evolve.

3. **Resource-Efficient Authentication**:

   - For large-scale CPS environments, resource efficiency becomes critical, especially in low-power or resource-constrained devices. Future work could focus on developing **lightweight authentication protocols** that optimize computational and communication overhead while maintaining high levels of security. This would be essential for IoT devices and other CPS components that are typically limited in processing power.

4. **Cross-Domain Authentication**:

   - Many CPS environments operate in **heterogeneous systems**, where devices from different manufacturers or domains need to interact with each other. Future work could explore **cross-domain authentication** strategies to enable secure resource sharing across different platforms and technologies. This may involve developing standardized protocols that ensure secure, trusted communication and authentication between CPS devices from different ecosystems.

5. **Privacy-Preserving Authentication**:

   - As privacy concerns continue to grow, future research could explore **privacy-preserving authentication mechanisms** that protect sensitive user and device data during the authentication process. Techniques like **zero-knowledge proofs** or **secure multi-party computation (SMC)** could be integrated to verify the authenticity of users and devices without revealing unnecessary personal information, balancing security with user privacy.

6. **AI and Machine Learning for Authentication Enhancement**:

   - Leveraging **artificial intelligence (AI)** and **machine learning (ML)** could improve the system's ability to adapt and respond to new threats. Future research could explore **anomaly detection** in authentication attempts by using AI to analyze patterns of access requests. These systems could identify abnormal behavior or emerging security threats and adjust authentication protocols in real-time to counteract them.

REFERENCES

[1] [1] Song Han, Miao Xie, Hsiao-Hwa Chen, and Yun Ling. 2014. Intrusion detection in cyber-physical systems: Techniques and challenges. IEEE systems journal 8, 4 (2014), 1052–1062.

[2] [2] Robert Mitchell and Ing-Ray Chen. 2014. A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys (CSUR) 46, 4 (2014).

[3] [3] Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo. 2011. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on. IEEE, 2195–2201.

[4] André Teixeira, Daniel Pérez, Henrik Sandberg, and Karl Henrik Johansson. 2012. Attack models and scenarios for networked contol systems. In Proceedings of the 1st international conference on High Confidence Networked Systems. ACM, 55–64.

[5] Hamid Reza Ghaeini and Nils Ole Tippenhauer. 2016. Hamids: Hierarchical monitoring intrusion detection system for industrial control systems. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy. ACM, 103–111.

[6] Leandros Maglaras, Helge Janicke, Jianmin Jiang, and Andrew Crampton. 2016. Novel Intrusion Detection Mechanism with Low Overhead for SCADA Systems. Security Solutions and Applied Cryptography in Smart Grid Communications (2016), 160.

[7] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C Green II, and Mansoor Alam. 2011. Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Transactions on Smart Grid 2, 4 (2011), 796–808.

[8] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C Green, and Mansoor Alam. 2011. Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid. In Power and Energy Society General Meeting, 2011 IEEE. IEEE, 1–8.

[9] Raymond C Borges Hink, Justin M Beaver, Mark A

[10] Buckner, Tommy Morris, Uttam Adhikari, and Shengyi Pan. 2014. Machine learning for power system disturbance and cyber-attack discrimination. In Resilient Control Systems (ISRCS), 2014 7th International Symposium on. IEEE, 1–8.

[11] Wei Gao, Thomas Morris, Bradley Reaves, and Drew Richey. 2010. On SCADA control system command and response injection and intrusion detection. In eCrime Researchers Summit (eCrime), 2010. IEEE, 1–9.

[12] Jonathan Goh, Sridhar Adepu, Marcus Tan, and Zi Shan Lee. 2017. Anomaly detection in cyber physical systems using recurrent neural networks. In High Assurance Systems Engineering (HASE), 2017 IEEE 18th International Symposium on. IEEE, 140–145.

[13] Jun Inoue, Yoriyuki Yamagata, Yuqi Chen, Christopher M Poskitt, and Jun Sun. 2017. Anomaly detection for a water treatment system using unsupervised machine learning. arXiv preprint arXiv:1709.05342 (2017).

[14] Turker Ince, Serkan Kiranyaz, Levent Eren, Murat Askar, and Moncef Gabbouj. 2016. Real-time motor fault detection by 1-D convolutional neural networks. IEEE Transactions on Industrial Electronics 63, 11 (2016), 7067–7075.

[15] Pankaj Malhotra, Lovekesh Vig, Gautam Shroff, and Puneet Agarwal. 2015. Long short term memory networks for anomaly detection in time series. In Proceedings. Presses universitaires de Louvain, 89.

[16] M. A. Khan and K. A. Abuhasel, ''An evolutionary multi-hidden Markov model for intelligent threat sensing in industrial Internet of Things,'' J. Supercomput., vol. 77, no. 6, pp. 6236–6250, Jun. 2021.