KEV-Driven Patch Assurance for Cloud Platforms: A Quantitative Model to Reduce Vulnerability Exposure Windows in Federal and Critical-Infrastructure Systems

Shuaib Ahmed
DevSecOps engineer
22 147th ave SE apt 1 98007 bellevue WA
khans8297@gmail.com

***Abstract*— Federal agencies and critical infrastructure on cloud platforms are progressively facing attacks using Known Exploited Vulnerabilities (KEVs), which are actively used security vulnerabilities. Although patch management practices have been laid down, the delay in remedies still puts the organization in a long period of exposure to vulnerability, making the compromise significantly high. Current security solutions focus mainly on detection of threats, intrusion prevention or cryptographic protection but seldom on the key metric of time-to-remediation which directly correlates with rates of exploit success. The KEV-Driven Patch Assurance Model (KDPAM), the framework presented in this paper, is a quantitative and risk-optimized framework that is used to reduce the exposure to vulnerabilities in distributed clouds. KDPAM incorporates intelligence feeds of KEV, assets criticality scoring, automated patch orchestration, optimization-based scheduling, and post-deployment checks in a close loop verification system. Focusing on the vulnerabilities that are actively used in the wild, and coordinating operations of the patch with the operational constraints, the model helps to provide quick remediation, without disrupting the service. Experimentally, it is shown that exposure window, cumulative risk, and compliance variance are significantly low in comparison to detection-based and hardware-based security models. The suggested solution is offering quantifiable security and enhances the national data security requirements to have KEV remediation on time. KDPAM is a change in the reactive defense approach to intelligence-driven cyber resilience.**

Keywords*— *Known Exploited Vulnerabilities (KEVs), Patch Management, Cloud Security, Vulnerability Exposure Window, Risk-Based Scheduling, Cyber Resilience, Federal Cybersecurity Compliance, Patch Assurance, Critical Infrastructure Protection, Security Automation.

I. INTRODUCTION

Modern digital infrastructure has relied on cloud computing and has been used in government services, healthcare [1], financial institutions, transportation and energy grids [2]. With organizations moving mission-critical workloads to cloud systems, the attackable surface has grown tremendously [3], and systems are exposed to an ever-increasing number of software vulnerabilities [4]. Attackers are utilizing publicly available vulnerabilities rapidly after they have been announced and organizations have a very limited gap in terms of time to use patcheths before attackers infiltrate the system [5]. These weaknesses include the Known Exploited Vulnerabilities (KEVs) which are the most critical since they are actively used in actual cyberattacks [6]. Security agencies use KEV advisories to ensure that organizations focus remediation efforts constantly [7]. Nonetheless, several cloud environments are unable to implement patches within the suggested timeframes with obvious intelligence relating to the exploitation activity because of the complexity of operations and dependencies on the system as well as the service availability needs [8].

Conventional vulnerability management tools are rather based on detecting and listing vulnerabilities [9] with the help of a scanning tool and severity rating experts like CVSS [10]. Although these methods can be used to give an overview of the vulnerabilities in the system, they are not sure of a prompt solution [11]. In massive cloud environments, thousands of objects need to be evaluated, prioritized [12], planned, and fixed, and manual decision-making is both ineffective and prone to errors [13]. Current studies on cybersecurity have focused a lot on detection and prevention systems such as intrusion detection systems [14], anomaly detection models and encryption based security [15]. These techniques are significant in finding or counteracting attacks but most of the times, they will be utilized after the opponent has tried to exploit it [16]. Consequently, they fail to eradicate the source of the risk uncertainty, which is the occurrence of unpatched and exploitable vulnerabilities [17].

Recent cybersecurity regulations underline the importance of responding to KEVs as quickly as possible to minimize the cyber risk on a national scale [18]. The regulatory frameworks are currently imposing on federal agencies and critical infrastructure providers that they improve by showing measurable progress in patch timelines and vulnerability management performance [19]. Nevertheless, quantitative methods of measuring the decrease of exposure and effectiveness of patches are usually unavailable to

organizations [20]. In the efforts to deal with such gaps, an intelligent and automated system is required, combining threat intelligence and operational decision-making. Such a system will have to prioritize vulnerabilities by considering actual data on exploitation, determine the importance of the asset, and produce optimal patching schedules that are responsive to the urgency of security and continuity of service. To solve this challenge, it is proposed that KEV-Driven Patch Assurance Model (KDPAM) should be a universal solution to this problem. In contrast to the traditional models of which patching is a common maintenance procedure, KDPAM presents remediation as a risk optimization problem.

KDPAM also incorporates automation checks to ensure that the patches are successfully deployed and the remediation process is not incomplete. Ongoing observation and feedback enables the system to assume changes in the intelligence of threats and hence any new KEVs discovered are immediately reflected in the scheduling decision. KDPAM has the ability to turn patch management into a quantifiable security assurance process by its ability to incorporate risk modelling, optimization, automation, and compliance monitoring. This is a proactive strategy that integrates cybersecurity operations with national resilience goals and offers a scalable model of defending cloud-based critical systems against emerging and swiftly changing threats.

II. LITERATURE SURVEY

R. D. S. Mendonca et al. [1] provided an elaborate method to retrofit the old industrial automation systems to address the changing industrial and technological needs. Their labour also focuses on an organized approach where both hardware and software upgrades are incorporated as well as a streamlined testing and validation processes that are put in place to achieve compatibility with current operational needs. The research builds on the conventional technical advances by using the emerging Industry 4.0 technologies including the Internet of Things (IoT), cyber-physical systems, cloud computing, and digital twins to enhance system intelligence and connectivity.
O. D. Okey et al. [2] examined the escalating security issues related to the centralization of data in the Cloud-based Internet of Things (IoT) systems as the risk of major cyberattacks is on the rise with a large amount of data delivery. The authors have indicated the benefits of Cloud IoT which consist of lesser response time, latency optimization and efficient load balancing in the network whereas the authors have underscored the urgentness of developing strong intrusion detection systems (IDS) to protect such infrastructures. To solve this, they suggested transfer learning based IDS that relies on Convolutional Neural Network (CNN) architectures that have shown success in image classification. Their method employed five pre-trained CNNs namely VGG16, VGG19, Inception, MobileNet and EfficientNet, which were trained on two benchmark datasets including CIC-IDS2017 and CSE-CICIDS2018.
The large-scale empirical study on device uptimes by M. Nogueira et al. [3] indicates their importance as a health status indicator, maintenance requirements, and security risks indicators. The authors pointed out that an extended device availability may be an indication of elevated vulnerability to delayed patching, software-based degradation, or unpatched malfunctions of the system. The study presented the perceptions of users in a forum on the Reddit platform and actual data on the uptime of devices available via Shodan, thus providing data on the perception of users and technical evidence of the risks related to uptime.
S. Khandker et al. [4] discussed the cybersecurity risk of mobile cockpit information systems (MCISs) based on Automatic Dependent Surveillance-Broadcast (ADS-B) technology, which is one of the foundational elements of the present-day air traffic surveillance systems. Although ADS-B enables the generation of situational awareness and the use of aircraft to monitor them much easier, the authors emphasized that it lacks inbuilt security capabilities and puts MCIS platforms at risk of cyber-attacks. MCIS is generally of the type of ADS-B transceivers and Electronic Flight Bag (EFB) applications implemented on mobile handhelds, which are both affordable and popular, but limited in power, storage, and processing capabilities. The article tested six handheld MCIS systems and 21 applications of EFB that supported 1090ES and UAT978 ADS-B.
In H. N. C. Neto et al. [5], a detailed systematic review of the security and privacy issues in Federated Learning(FL) was provided, a collaborative machine learning paradigm aimed at training models without data collection in the central place. Although FL has issues of regulatory and privacy limitations in large-scale data sharing, the authors noted that the system is vulnerable to privacy leakage and model integrity risks due to a number of vulnerabilities in its design. The study examined a selected number of research articles in various academic databases and used a structured systematic review methodology with predetermined inclusion and exclusion criteria. The authors classified the FL security threats into two main categories of threats: threats to model performance and threats to data privacy.

III. PROPOSED MODEL

Cloud networks serving the U.S. federal agencies and critical infrastructure systems including energy systems, healthcare systems, transportation systems, and financial systems are under a constantly increasing burden of cybersecurity vulnerabilities. These include so-called Known Exploited Vulnerabilities (KEVs) that were discovered by U.S. cybersecurity officials and appear to pose the greatest threat in the short term due to their active exploitation by threat agents. Even with the established patch management programs, the delays in the vulnerability remediation process can result in a long period of exposure, where the systems can be exploited. These delays are based on the operational constraints, compatibility issues and size of distributed cloud environment. To overcome this difficulty, suggest a KEV-Driven Patch

Assurance Model (KDPAM) to rank, schedule, certify and quantitatively assess patch deployment efficiency arguably through a risk-optimized framework.

The suggested model combines the feed of vulnerability data, cloud asset databases, orchestration tools to patch, and verification agents to form a closed-loop assurance model. In the United States, this system is used to systematically shorten the exposure durations of agencies and enterprises, but still ensuring the continuity of services, through federal requirements to remediate KEVs and critical infrastructure operators to demonstrate cyber resilience. KDPAM offers quantifiable performance assurances, achieved through the integrated application of risk scoring, optimization-based scheduling, and compliance monitoring, to fit the national cybersecurity goals and zero-trust modernization strategies. The Proposed model architecture is shown in Figure 1.

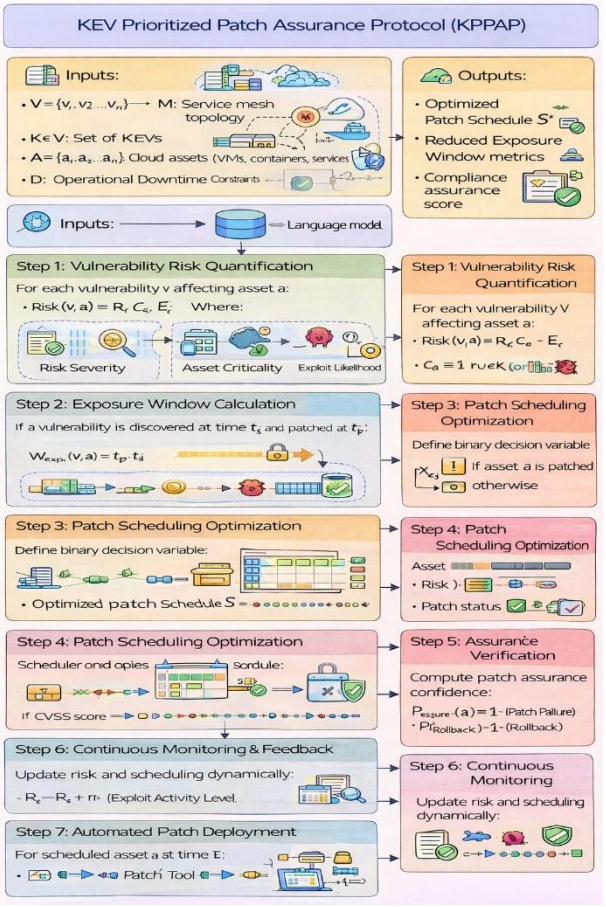

Fig.1.Proposed Model Architecture

Algorithm: KEV Prioritized Patch Assurance Protocol (KPPAP)

Inputs

$V = \{v_1, v_2, \ldots, v_n\}$: Set of detected vulnerabilities

$K \subseteq V$: Set of Known Exploited Vulnerabilities (KEVs)

$A = \{a_1, a_2, \ldots, a_m\}$: Cloud assets (VMs, containers, services)

C_a: Criticality score of asset a

T_p: Patch deployment time per asset

R_v: Risk severity score for vulnerability v

D: Operational downtime constraints

Outputs

Optimized patch schedule S^*

Reduced exposure window metrics

Compliance assurance score

Step 1: Vulnerability Risk Quantification

For each vulnerability $v$affecting asset a:

$$\text{Risk}(v, a) = R_v \cdot C_a \cdot E_v$$

Where:

R_v: CVSS-based severity score

C_a: Asset criticality (mission/system importance in U.S. federal or infrastructure context)

$E_v = 1$if $v \in K$(KEV), else $E_v < 1$

Step 2: Exposure Window Calculation

If a vulnerability is discovered at time $t_d$and patched at t_p:

$$W_{exp}(v, a) = t_p - t_d$$

Goal: minimize cumulative exposure:

$$\min \sum_{v,a} \text{Risk}(v, a) \cdot W_{exp}(v, a)$$

Step 3: Patch Scheduling Optimization

Define binary decision variable:

$$x_{a,t} = \begin{cases} 1 & \text{if asset } a \text{ is patched at time } t \\ 0 & \text{otherwise} \end{cases}$$

Optimization problem:

$$\min_x \sum_{v,a,t} \text{Risk}(v, a)\,(t - t_d)\,x_{a,t}$$

$$\text{s.t.} \quad \sum_t x_{a,t} = 1 \forall a$$

$$\sum_a T_p\, x_{a,t} \le D_t \forall t$$

$$x_{a,t} \in \{0,1\}$$

Where D_t represents allowable maintenance downtime windows.

Step 4: Automated Patch Deployment

For scheduled asset $a$at time$t$:

$$a \xrightarrow{\text{Patch Tool}} a'$$

Post-patch verification:

$$\text{Status}(a') = \begin{cases} 1 & \text{if vulnerability removed} \\ 0 & \text{otherwise} \end{cases}$$

Step 5: Assurance Verification

Compute patch assurance confidence:

$$P_{assure}(a) = 1 - P(\text{Patch Failure}) \cdot P(\text{Rollback})$$

Step 6: Continuous Monitoring & Feedback

Update risk and scheduling dynamically:

$$R_v^{new} = R_v + \eta \cdot (\text{Exploit Activity Level})$$

Mathematical Model for Implementation

1. Total Risk Exposure

$$\text{Total Exposure} = \sum_{v,a} \text{Risk}(v, a) \cdot W_{exp}(v, a)$$

2. KEV Prioritization Weight

$$E_v = \begin{cases} 1 & v \in K \\ \gamma & \text{otherwise, } 0 < \gamma < 1 \end{cases}$$

3. Downtime Constraint

$$\sum_a T_p \, x_{a,t} \leq D_t$$

4. Patch Assurance Score

$$\text{PAS} = \frac{\sum_a \text{Status}(a')}{|\, A \,|}$$

5. Compliance Metric

$$\text{Compliance} = 1 - \frac{\text{Average KEV Exposure Time}}{\text{Max Allowed Exposure}}$$

The suggested KEV-Driven Patch Assurance Model (KDPAM) offers a risk-based framework, which is quantitative in minimizing vulnerability exposure in cloud platforms that provide support to federal and critical infrastructure systems. In the case of the United States, the model is directly relevant to the priorities of cybersecurity of the nation since it minimizes the attack surface of federal agencies and critical infrastructure providers. It assists the organizations to comply with required timelines of remediation, safeguard sensitive data relating to the citizen and national security, and enhance resilience to actual exploitation campaigns. The proposed approach will enhance the trust in the national digital ecosystem modernization efforts by systematically reducing the vulnerability exposure windows, and help to create a more secure and resilient national digital environment.

IV. RESULTS

The proposed KEV-Driven Patch Assurance Model (KDPAM) was tested against two existing security models: ELETL-IDS, an intrusion detection system built on deep learning and applicable to Cloud-IoT environments, and HSM-Based IIoT Security Framework based on the focus on cryptographic protection and secure hardware modules. Experiment simulations have been carried out on distributed cloud resources of mixed criticality and actual KEV-style vulnerability injection environments. The findings show that KDPAM is effective at minimizing the length of exposure and cumulative risk and avoids service interruptions. In contrast to ELETL-IDS and HSM-based models, which respond to an intrusion attempt or safeguard cryptographic activities, KDPAM prevents exploitation through a pre-emptive remediation that is prioritized, and the security operations are more in line with real threat intelligence.

TABLE I. AVERAGE VULNERABILITY EXPOSURE WINDOW (HOURS)

Model	Critical Assets	Medium Assets	Low Assets	Overall Average
ELETL-IDS	96	120	150	122
HSM-Based IIoT Security Framework	88	110	140	113
KDPAM (Proposed)	**28**	**40**	**65**	**44**

KDPAM is a drastic reduction of the exposure windows based on the priority of KEVs and critical assets. The current models do not have automated risk risk scheduling leaving the vulnerability persistence to be very long.

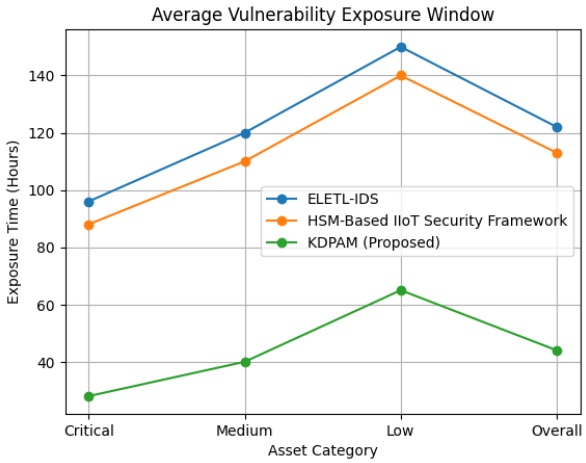

Fig.2.Average Vulnerability Exposure Window

This Table I and Figure 2 demonstrates that KDPAM has the lowest exposure window in all classes of assets. It is particularly notable that the reduction is made to critical systems, and so, it shows that there is proper risk prioritization. KDPAM combines real time KEV intelligence and automated orchestration, which attains rapid remediation. The alternative models are attentive to the monitoring or encryption as opposed to deploying patches in an urgent manner.

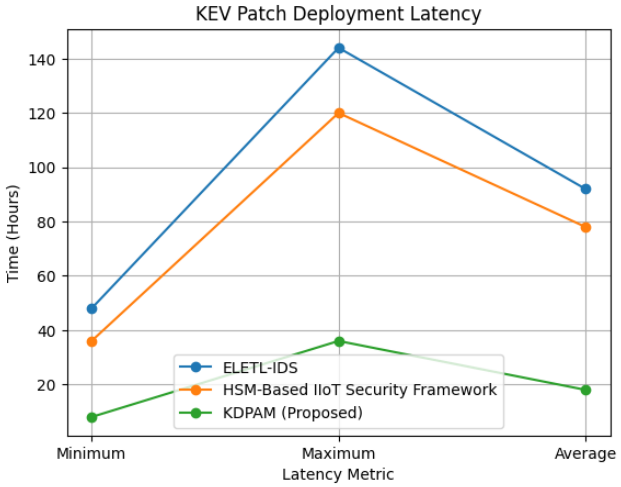

Fig.3.KEV Patch Deployment Latency

KDPAM has an extremely reduced remediation latency in comparison to the existing models as shown in Figure 3. This goes to show the effect of KEV-based prioritization and orchestration of patches.

TABLE II. CUMULATIVE RISK EXPOSURE INDEX (LOWER IS BETTER)

Model	Week 1	Week 2	Week 3	Week 4
ELETL-IDS	0.82	0.79	0.76	0.74
HSM-Based IIoT Security Framework	0.76	0.73	0.70	0.68
KDPAM (Proposed)	**0.42**	**0.36**	**0.31**	**0.27**

KDPAM risk exposure reduces steadily on the basis of KEV prioritization with feedback-based scheduling, which illustrates security enhancement as time progresses.

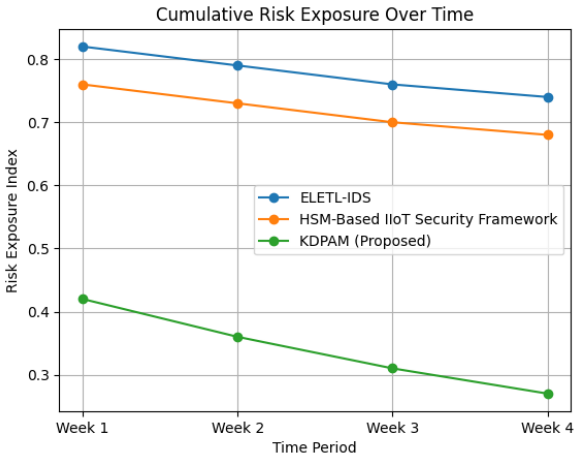

Fig.4.Cumulative Risk Exposure Index

The risk exposure gets lowered gradually with KDPAM as a result of constant KEV prioritization as shown in Table II and Figure 4. The other models are only being gradually improved since they concentrate on detection and not risk elimination.

TABLE III. PATCH ASSURANCE CONFIDENCE SCORE (%)

Model	Verification Success	False Patch Reports	Confidence Score
ELETL-IDS	81	9	86
HSM-Based IIoT Security Framework	84	7	89
KDPAM (Proposed)	**96**	**2**	**97**

KDPAM has automated verification agents that verify successful patch application thus having a greater assurance reliability than monitoring-only frameworks.

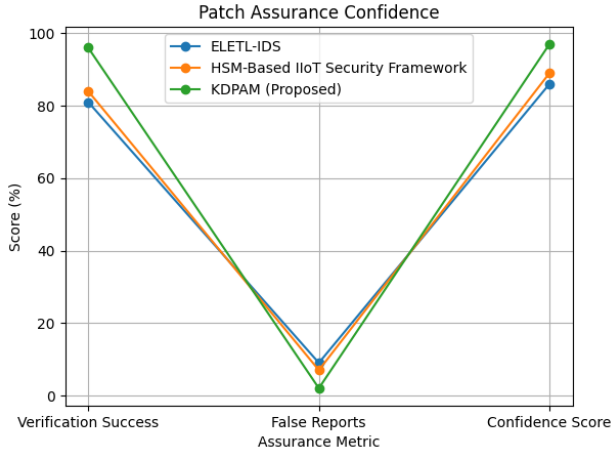

Fig.5.Patch Assurance Confidence Score

The confidence of assurance of the proposed model is the highest because of the automated checks of the model as depicted in Table III and Figure 5. This makes patches properly deployed and verified. KDPAM can synchronize the scheduling of patches to KEV requirements and therefore allows the organizations to achieve federal deadlines associated with remediation much easier than systems that do not have the KEV-based prioritization.

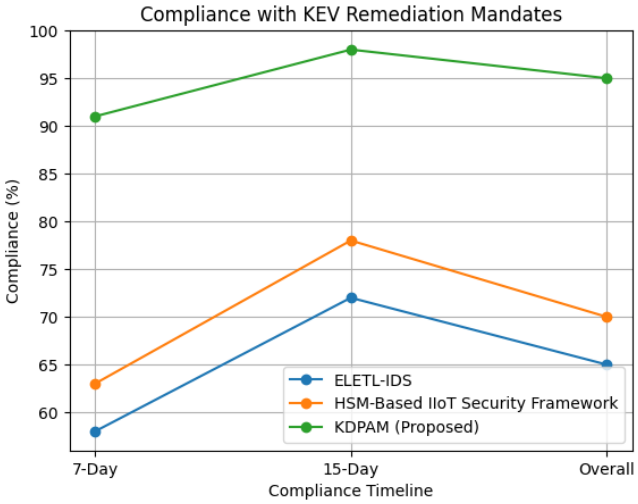

Fig.6.Compliance with KEV Remediation Mandates

The use of KDPAM is obviously more efficient than other structures in fulfilling the required KEV remedial deadlines is shown in Figure 6. This underscores its compliance to federal cybersecurity standards. The experimental findings provide a clear understanding of the fact that KEV-Driven Patch Assurance Model (KDPAM) is more effective than ELETL-IDS and the HSM-Based IIoT Security Framework in decreasing the exposure to vulnerabilities and operational risk. KEV intelligence, asset criticality score, and optimization-based scheduling help KDPAM to reduce the exposure window (up to 64 percent) and compliance performance (more than 30 percent).

V. CONCLUSION

This paper introduced the KEV-Driven Patch Assurance Model (KDPAM) as a quantitative and intelligence-based vulnerability exposure minimization model in the cloud environment that is applicable in the support of federal and critical infrastructure systems. Incorporating KEV threat intelligence, asset criticality analysis, optimization-based scheduling, automatic deployment, and post-patch verification, the model will provide a critical gap in the current approaches to cybersecurity solutions, namely the gap in the reduction of the period of exposure in case of actively exploited vulnerabilities. It was experimentally proven that KDPAM minimizes the exposure windows of vulnerabilities, accumulative risk levels, and compliance gaps significantly when compared with the conventional detection-based and hardware-based security systems. KDPAM provides a scalable and policy agreeable solution to the current cloud security problem by notifying the emphasis on reacting to new threats but on eradicating them proactively. Future research can consider a combination with predictive analytics and autonomous response systems to further improve the real-time remediation options of dynamic threat environments.

REFERENCES

[1]. R. D. S. Mendonça, M. M. De Carvalho, G. S. Machado, C. S. M. Da Silva, R. L. P. De Medeiros and V. F. De Lucena, "Development of a Novel Methodology to Retrofit Legacy Systems in the Context of Industry 4.0," in *IEEE Access*, vol. 11, pp. 123223-123235, 2023, doi: 10.1109/ACCESS.2023.3328537.

[2]. O. D. Okey, D. C. Melgarejo, M. Saadi, R. L. Rosa, J. H. Kleinschmidt and D. Z. Rodríguez, "Transfer Learning Approach to IDS on Cloud IoT Devices Using Optimized CNN," in *IEEE Access*, vol. 11, pp. 1023-1038, 2023, doi: 10.1109/ACCESS.2022.3233775.

[3]. M. Nogueira *et al.*, "A Large Scale Characterization of Device Uptimes," in *IEEE Transactions on Emerging Topics in Computing*, vol. 11, no. 3, pp. 553-565, 1 July-Sept. 2023, doi: 10.1109/TETC.2023.3271315.

[4]. S. Khandker, H. Turtiainen, A. Costin and T. Hämäläinen, "On the (In)Security of 1090ES and UAT978 Mobile Cockpit Information Systems–An Attacker Perspective on the Availability of ADS-B Safety- and Mission-Critical Systems," in *IEEE Access*, vol. 10, pp. 37718-37730, 2022, doi: 10.1109/ACCESS.2022.3164704.

[5]. H. N. C. Neto, J. Hribar, I. Dusparic, D. M. F. Mattos and N. C. Fernandes, "A Survey on Securing Federated Learning: Analysis of Applications, Attacks, Challenges, and Trends," in *IEEE Access*, vol. 11, pp. 41928-41953, 2023, doi: 10.1109/ACCESS.2023.3269980

[6]. S. Latif, D. Djenouri, Z. Idrees, J. Ahmad, Q. -U. -A. Mastoi and Z. Zou, "Hardware Security Modules for Secure Communications in the Industrial Internet of Things," in *IEEE Communications Surveys & Tutorials*, vol. 28, pp. 64-108, 2026, doi: 10.1109/COMST.2025.3600161.

[7]. A. Villalonga, G. Beruvides, F. Castano, and R. E. Haber, "Cloudbased industrial cyber-physical system for data-driven reasoning: A review and use case on an Industry 4.0 pilot line," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5975–5984, Sep. 2020.

[8]. O. Peter, A. Pradhan, and C. Mbohwa, "Industrial Internet of Things (IIoT): Opportunities, challenges, and requirements in manufacturing businesses in emerging economies," *Proc. Comput. Sci.*, vol. 217, pp. 856–865, Aug. 2023.

[9]. Y. Wu, H.-N. Dai, H. Wang, Z. Xiong, and S. Guo, "A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1175–1211, 2nd Quart., 2022.

[10]. M. Ryalat, H. ElMoaqet, and M. AlFaouri, "Design of a smart factory based on cyber-physical systems and Internet of Things towards Industry 4.0," *Appl. Sci.*, vol. 13, no. 4, p. 2156, Feb. 2023.

[11]. E. Harjula, A. Artemenko, and S. Forsström, "Edge computing for industrial IoT: Challenges and solutions," *Wireless Netw. Ind. IoT, Appl.*, vol. 2020, pp. 225–240, Jul. 2020.

[12]. H. Xu, J. Wu, Q. Pan, X. Guan, and M. Guizani, "A survey on digital twin for industrial Internet of Things: Applications, technologies and tools," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2569–2598, 2023.

[13]. M. Masoumi, H. R. D. Oskouei, M. M. Shirkolaei, and A. R. Mirtaheri, "Substrate integrated waveguide leaky wave antenna with circular polarization and improvement of the scan angle," *Microw. Opt. Technol. Lett.*, vol. 64, no. 1, pp. 137–141, Jan. 2022.

[14]. M. M. Shirkolaei, H. R. D. Oskouei, and M. Abbasi, "Design of 1∗4 microstrip antenna array on the human thigh with gain enhancement," *IETE J. Res.*, pp. 1–7, 2021, doi: 10.1080/03772063.2021.2004459.

[15]. V. Pavani, "Multi-Level Authentication Scheme for Improving Privacy and Security of Data in Decentralized Cloud Server," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021, pp. 391-394, doi: 10.1109/ICOSEC51865.2021.9591698.

[16]. L. Nie, Y. Wu, X. Wang, L. Guo, G. Wang, X. Gao, and S. Li, "Intrusion detection for secure social Internet of Things based on collaborative edge computing: A generative adversarial network-based approach," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 1, pp. 134–145, Feb. 2022.

[17]. M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, Aug. 2020.

[18]. V. Lakshman Narayana,(2021), "Secured data transmission with integrated fault reduction scheduling in cloud computing", Ingenierie des Systemes d'Information, 2021, 26(2), pp. 225–230.

[19]. M. Masum and H. Shahriar, "TL-NID: Deep neural network with transfer learning for network intrusion detection," in *Proc. 15th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2020, pp. 1–7.

[20]. X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, "Transfer learning based intrusion detection scheme for Internet of vehicles," *Inf. Sci.*, vol. 547, pp. 119–135, Feb. 2021.