Vita Digital Journal

Life through Technology & Innovation

Computer Science Department Monthly

Vol. 1 | Issue 3 | April 2026

VITA DIGITAL JOURNAL

Life through Technology & Innovation

Computer Science Department Monthly

Volume 1 | Issue 3 | April 2026

Published by:
Department of Computer Science,
Marian College of Arts and Science,
Thiruvananthapuram.

Chief Editor: Livin M Miranda
Student Editors:
Santhipriyan M
Joel George Mathew

mcasmedia123@gmail.com
https://www.mcas.ac.in/

EDITORIAL

The progress of space exploration has always reflected humanity's determination to discover, innovate, and move beyond known boundaries. One of the landmark achievements in recent times was Artemis II, the crewed mission of NASA. Artificial Intelligence and Machine Learning supported data analysis and autonomous functions, while cybersecurity measures protected communication networks and mission systems. Simulation technologies enabled scientists and engineers to test multiple scenarios before launch, reducing risks and improving reliability. Embedded systems and robotic technologies further strengthened mission efficiency and performance.

The success of Artemis II reminded the world that Computer Science is not confined to classrooms or laboratories. Programming, data science, networking, automation, and intelligent systems have become essential tools in solving complex challenges and expanding human knowledge beyond Earth.

As we present the third issue of Vita Digital Journal, we encourage our readers to recognise the transformative power of interdisciplinary learning. Space exploration today is not only an achievement of aerospace engineering but also a celebration of computing excellence and human intellect.

May this issue inspire young minds to think boldly, innovate responsibly, and pursue ideas that can shape the future of science and technology.

- Chief Editor

Mr. Livin M Miranda

Head, Department of Computer Science

Index

Federated Learning
Concepts, Implementations & Real-World Examples

Akash Aloysious George
S4 BSc Computer Science

ABSTRACT

Federated learning (FL) is a distributed learning technique that allows for machine learning across multiple decentralised devices or institutions without needing to centralise raw data. FL was first proposed in 2016 by Google and is a technique for resolving a fundamental conflict in artificial intelligence development, where large and heterogeneous data is needed for development, but organisations cannot share this data due to privacy, legal, and competitive concerns.

In FL, individual devices or organisations train individual models on individual data and share model parameter updates (gradients or weights) to a central server, which combines them to improve a global model. The raw data is not shared.

In this article, the basic concepts of federated learning are discussed, and the major domains in which federated learning has been applied are reviewed. In addition, specific scenarios of federated learning are provided. The major challenges of federated learning are also discussed, and the countermeasures are reviewed.

Keywords: federated learning, privacy-preserving ML, distributed learning, differential privacy, secure aggregation, FedAvg

INTRODUCTION

The development of machine learning has seen tremendous growth in recent times. This has led to the insatiable need for large amounts of labelled data. In the past, organizations have relied on the collection of user data in large quantities and the storage of the data in data warehouses. This has led to the development of robust models, but there have also been concerns about the privacy and security of the data.

The development of federated learning by McMahan et al. of Google in 2016 has provided a different perspective on the conventional way of learning. In federated learning, the model is taken to the data instead of the data being taken to the model. This has led to the development of collaborative learning, where the data and models remain private.

The architecture is "elegantly simple in concept and technically rich in practice. The global model is created and stored on a server, and a copy is sent to a number of participants. Each participant takes the global model and fits it to their own data, computing gradients and sending them back to the server. The server combines them to produce a new global model. This is repeated until convergence is reached.

There are three key features that make this paradigm particularly compelling for modern AI development:

- Privacy is built-in, and user data is stored only on the device that created it.
- Regulatory compliance is greatly simplified, including GDPR, HIPAA, and CCPA.
- ·Scalability without centralization is possible, allowing models to learn from billions of users without a single data store.

Key Concepts

To understand the implementations of federated learning, it is important to understand the basic concepts involved in federated learning. Here are some key concepts involved in federated learning:

- Global Model: This refers to a machine learning model that is updated by the server in each communication round based on the contributions of the clients.
- Local Model: This refers to a local copy of the global model that each client device fine-tunes independently based on the local data available in the client device.
- Model Update/Gradient: This refers to the update in the machine learning model computed by the client device. This update is the only piece of information that is sent to the server. The original data is not sent to the server.

- Aggregation/FedAvg: This refers to the aggregation of the model updates computed by the client devices. This aggregation is done by the server. It is done by computing the weighted averages of the model updates based on the sizes of the local datasets.
- Communication Round: This refers to one cycle in the federated learning process.

How Federated Learning Works

Training Round — Step by Step

The following flowchart represents the steps for one federated learning round, from the distribution of the model to the update of the global model. The steps are as follows:

Step 1 — Global model initialisation The global model, or the model's weights W_t, is maintained or updated by the server. A number of participating clients are selected for the training round.

↓

Step 2 — Model distribution The server sends the current global model's weights, W_t, to all the selected client devices or institutions.

↓

Step 3 — Local training Each client receives the global model's weights, W_t, and trains the model on its local data, D_i, for some number of epochs.

Step 4 — Gradient / weight upload Each client sends the difference between its updated model's weights, W_i, and the global model's weights, W_t, or the delta, to the server. The data, D_i, is not shared.

↓

Step 5 — Secure aggregation The server gathers updates from all the contributing clients. Optional: secure aggregation protocols, like cryptographic masking, are used to prevent the server from viewing the updates sent by the clients.

↓

Step 6 — FedAvg aggregation The server calculates the new global weights using the following formula: W_{t+1} = SUM_i (n_i / N) * W_i, where n_i represents the data points of each client i and N represents the total data points across all clients.

↓

Step 7 — Next round or convergence The new global weights are sent out. This process is repeated for T rounds, after which the global model converges on the validation metric.

↓

FedAvg Algorithm

The FedAvg algorithm (McMahan et al., 2017) is the most popular aggregation method. The basic idea behind this algorithm is that multiple SGD updates can be performed on the client side before communication, which significantly reduces the number of communication rounds for convergence compared to the synchronous SGD algorithm.

FedAvg — Algorithm Summary

Server initialization: global weights W_0

For communication rounds t = 1, 2, ..., T :

- *Choose fraction C of clients*
- *Send W_t to all clients*
- *Clients perform E iterations of SGD on local data and compute W_k*
- *Clients send W_k to server*
- *Server combines weights W_{t+1} = SUM_k (n_k / n) * W_k*

Return global weights W_T

WHERE FEDERATED LEARNING IS USED - IMPLEMENTATION

Federated learning is used in a variety of industries that involve privacy, regulatory requirements, and/or business needs that do not allow centralised model training.

The following table describes the major domains where federated learning is used:

Domain Use	***Case***
Mobile/Edge AI	*Keyboard autocomplete, voice recognition, personalization of devices, prediction of application usage*
Healthcare & Biomedical	*Disease detection using images, prediction of drug interactions, EHR analysis across hospitals*
Financial Services	*Fraud detection, credit risk modeling, pattern recognition of money laundering among competing financial institutions*
Autonomous Vehicles	*Training of perception models, object detection, recognition of hazards using fleet dashcam images*
Telecommunications	*Traffic anomaly detection, predictive maintenance, QoS optimization among towers*
Retail & E-Commerce	*Recommendation systems, prediction of demand, personalization without customer profile sharing*
Smart Manufacturing	*Predictive maintenance, defect detection among nodes of distributed factories*
Government & Defence	*Cross-agency analytics with high data sovereignty requirements*

HEALTHCARE

Healthcare is perhaps the most critical application area of federated learning. Patient information is subject to various laws such as HIPAA in the USA, GDPR in Europe, and other such laws in other parts of the world. Sharing patient information between hospitals is legally complex and often not possible.

Federated learning removes this barrier as well. A consortium of hospitals can come together to develop a model to detect tumors in MRI scans, sepsis in ICU patient information, or rare disease signatures in genomic information without any hospital ever seeing information from other hospitals. The information is still within each hospital's firewall.

The MELLODDY project (2021) is a pan-European initiative in pharmaceutical research. Ten competing pharmaceutical companies used federated learning to develop predictive models in drug discovery without any of them sharing their proprietary information. All of them worked together to develop a predictive model that was better than each of their individual predictive models.

Mobile Computing

The amount of behavioral data being created by mobile computing is staggering, including all key strokes and voice commands. People are no longer willing to share this information sent to remote servers.

One of the first commercial applications of federated learning at scale is Google's Gboard keyboard (2017). Gboard learns user keyboard habits, slang, and emoji preferences entirely on the client side. Periodically, when the phone is idle, plugged in, and connected to Wi-Fi, a compressed model update is sent to Google's servers. The aggregate improvements are sent back to all users. No user's actual typed text is sent to Google's servers.

Apple is using similar techniques for Siri and QuickType predictions, including on-client learning and differential privacy to guarantee that even the gradients cannot be reverse engineered to recover typed text.

Financial Services

Collectively, banks have access to transactional data that can be combined to significantly improve fraud detection models. Unfortunately, sharing transactional records between rival banks is not permissible under current financial privacy regulations and antitrust laws.

Federated learning can address this issue by facilitating collaborative learning of fraud models without sharing underlying transactional records. The FATE framework (Federated AI Technology Enabler), created by WeBank, has become widely used in Chinese financial services for this exact purpose. Multiple banks collaborate to learn a common fraud detection model while using cryptography to ensure that none of their raw data is shared.

Autonomous Vehicles

Autonomous cars collect terabytes of sensor and camera data per hour of driving. This includes images of people's faces, licence plates, personal properties, and patterns of movement. This is a huge privacy risk if centralized.

Automotive original equipment manufacturers are using federated learning to pool driving knowledge across entire fleets.

When a car drives by a strange road condition, construction zone, or unusual pedestrian behavior, its local model contributes to the knowledge pool. This knowledge pool helps make every car in the fleet safer without any of them uploading its camera feed.

REAL-WORLD EXAMPLES

Google Gboard - Keyboard Next Word Prediction

Case Study: Google Gboard (2017 - present)

Organisation: Google / Alphabet

Problem: Improve autocomplete and next word prediction without collecting what users type.

Scale: Billions of Android devices across 200+ countries.

How it works:

1. Stores a rolling window of past typing interactions locally on the device.
2. Downloads the latest global language model to the device when idle, on charger, and on unmetered wifi.
3. Fine-tunes locally on past typing history for a small number of steps.

4. Sends a compressed gradient update to Google's servers (a few KB).
5. Google collects updates from millions of devices and releases an improved global language model using FedAvg.

Privacy Guarantees: We add noise to each update on the device based on differential privacy. It is mathematically impossible to know what any given person typed based on their update. We can't know what any given device sent because of secure aggregation.

NVIDIA FLARE — Medical Imaging Across Hospitals

Case Study: NVIDIA FLARE (FL Application Runtime Environment)

Organization: NVIDIA (Platform), used by over 20+ hospital networks across the globe.

Problem: Train a high-accuracy model for tumor segmentation using MRI scans without sharing data across hospitals.

How it works:

1. A group of hospitals decides to work together under a data-sharing agreement. The agreement only includes updates to the models.

2. Each hospital installs NVIDIA FLARE on their local GPU cluster.

3. The FLARE server sends out the initial 3D U-Net-based segmentation model to all hospitals.

4. Each hospital trains the model using local MRI scans and annotations. 5. Gradient updates are sent to the FLARE server after encryption.

5. The FLARE server aggregates all updates and sends the new model.

Results: Studies have proven that federated models can achieve, if not outperform, centrally pooled models. All data remains local to each hospital.

Regulatory Compliance: All data stays local to each hospital, under HIPAA and GDPR regulations. This setup is equivalent to a data-use agreement.

WeBank FATE – Cross Bank Fraud Detection (China)

Case Study: WeBank FATE – Framework Overview

Organization: WeBank (China) – Open-sourced under the name FATE: Federated AI Technology Enabler

Problem: Multiple competing banking institutions want to collaborate to improve cross-bank fraud detection without sharing transactional data on their customers.

Regulatory Compliance: All data stays local to each hospital, under HIPAA and GDPR regulations. This setup is equivalent to a data-use agreement.

How It Works:
1. Each bank finds overlapping customers through private set intersection.

2. Each bank has a different vertical slice of the financial profile of the identified overlapping customers
.
3. Each bank trains its side of a split neural network on its vertical slice of features.

4. Each bank shares its encrypted intermediate representations to compute the forward pass through the combined neural network.

5. Gradients are back-propagated through the same encrypted channel.

Results: Improved fraud recall rates for all participating banks compared to any one bank's model alone – without any sharing of raw data.

Apple - On-Device Siri & QuickType

Case Study - Apple On-Device Learning

Organization - Apple Inc.

Problem - Improve Siri voice recognition and QuickType keyboard prediction for each user without uploading voice recordings and typed text.

How it works:
1.User interactions like corrected autocomplete and Siri queries that needed to be repeated are logged locally on the iPhone/iPad.

2.On-device learning refines the personal model using Neural Engine acceleration.
3.Differential privacy is applied by adding calibrated random noise to any statistics before they are sent to Apple.
4.Only aggregate and anonymous statistics are used to update the central model.
5.Individual user data and model weights are not used to update the central model.

The main difference between the Apple approach and the Google approach is that the Apple approach does not upload the gradient. Instead, it sends differentially private aggregate signals to update the global model. This is more similar to local differential privacy than federated learning. However, the privacy guarantee is the same for both approaches. In the case of the Apple approach, there is no raw data being uploaded from the local device.

Privacy Guarantee - This approach provides a formal differential privacy guarantee. Epsilon values are published in Apple's privacy white papers.

KEY CHALLENGES

Despite its promise, federated learning introduces several technical and practical challenges that active research continues to address:

Challenge	*Description*
Non-IID data	*Client data is not IID, and data on each device is dependent on the behavior of the client.*
Communication cost	*Client data is not IID, and data on each device is dependent on the behavior of the client.*
Systems heterogeneity	*Devices can be of varying types.*
Privacy leakage	*There is the possibility of leakage of private data due to gradient inversion attacks.*
Byzantine attacks	*There are possibilities of attacks on the server by the devices.*
Free-rider problem	*Devices not contributing enough to the process and yet enjoying the benefits of the global model.*
Convergence speed	*FL converges slowly due to the IID data and the communication time between devices.*

PRIVACY-ENHANCING TECHNIQUES

The federated learning approach is privacy-friendly, but it is not necessarily privacy-secure. The following techniques are used in combination with the basic FL protocol to improve the privacy of the approach:

Differential Privacy (DP)

In the differential privacy approach, random noise is added to the model updates. The noise is such that the probability of inferring an individual's data from the aggregated data is bounded by the parameter epsilon.

Applied in: Google Gboard, Apple on-device learning, healthcare FL.

Trade-off: More noise implies better privacy, but the model accuracy will also degrade. The privacy budget epsilon should be carefully set

Secure Aggregation

In the secure aggregation approach, the central server learns only the sum of the client updates. The approach uses cryptographic protocols such as secret sharing or homomorphic encryption.

Applied in: Google FL, NVIDIA FLARE, FATE.

Trade-off: High computation cost.

Homomorphic Encryption (HE)

In the homomorphic encryption approach, the computation (addition, multiplication) is performed on the encrypted data. Clients encrypt the updates, and the server aggregates the updates. The final aggregated update is decrypted.

Applied in: Vertical FL (FATE), healthcare.

Trade-off: High computation cost. The approach supports only linear computation.

CONCLUSION

Federated learning is an important breakthrough in the development of machine learning. The decentralized nature of the training process and the fact that data is not shared ensure the development of new forms of AI, which are not only possible but also legal and ethical.

The success of Google's keyboard predictions, the detection of cancer by hospital networks, and the fight against fraud by banks are all examples of the success of federated learning. The protocol has been well established, and the only area for research is how to overcome the challenges.

The challenges are not insurmountable, and the success of federated learning will ensure the development of new forms of AI, which will not only be legal and ethical but also possible. As the world becomes increasingly privacy-conscious, the need for federated learning will not only be felt but also made possible.

REFERENCES

- McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. (2017). "Communication-Efficient Learning of Deep Networks from Decentralized Data". https://arxiv.org/abs/1602.05629
- Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). "Federated Machine Learning: Concept and Applications". https://arxiv.org/abs/1902.04885
- Google AI Blog (2017). "Federated Learning: Collaborative Machine Learning without Centralised Training Data". https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

Role of Generative AI : Software Engineering and Its Impact on the IT Industry

Adarsh Tom
S4 BSc Computer Science

ABSTRACT

GenAI has emerged as one of the most important innovations in contemporary software engineering, becoming such in record time. Nowadays, there are many GenAI-powered tools available to automate code creation, testing, detection of potential vulnerabilities, and even writing documentation. In this paper, we will take you through the process of how genAI is revolutionizing each step in the Software Development Life Cycle (SDLC), discuss adoption rates, actual productivity gains observed based on current industry statistics, highlight risks associated with code generated by AI, and analyze the implications of all these developments for people working in software development.

Based on facts, we can say that productivity gains on the task level range from 10% to 55%, but to fully realize their potential, an organization needs to change the whole SDLC.

Index Terms—Generative AI, software engineering, code generation, SDLC automation, developer productivity, large language models, AI risk, workforce transformation

INTRODUCTION

A profound change occurred once large language models learned to generate code. Unlike the compilers, integrated development environments, and version control systems that came before, the generative AI paradigm works at a fundamentally different level of abstraction—a place where the developer can describe their intentions using natural language and get code back in response.

The data tell the story. GitHub Copilot had already amassed 20 million active users by mid-2025 and is being used by 90% of Fortune 100 firms. About one in four lines of internally written code at Google and Microsoft was generated using AI techniques. In 2025, enterprises were spending more than $4 billion on AI tools for writing code—the largest share of overall AI department budget allocations. There is no longer any need to speculate here—this trend defines contemporary software engineering.

"Natural language specifications are replacing explicit code as the primary human input into software development."

In this paper, we explore the technologies enabling such trends, the effects seen in empirical research, the dangers inherent to AI-based code generation, and the implications for the lives of professional software developers.

USE OF GENERATIVE AI THROUGHOUT SDLC

Coding In the domain of code generation

The impact of Generative AI tools stands out clearly. Provide GPT-40 or Claude Sonnet with a task description in plain English and get code written across many languages. Under controlled experiments, developers with GitHub Copilot accomplished tasks 55% faster, while pull request times were cut from 9.6 days to 2.4 days, translating to a 75% reduction in process duration. At high adoption companies, up to 61% of the code lines written by Java programmers are generated with the help of AI.

Quality Assurance and Testing

Generative AI helps create unit tests, integration tests, and regression tests for applications based on the current codebase. Leading organizations are taking advantage of the shift left approach that incorporates GenAI tests earlier in the process to ensure that the coding speed gains do not lead to bottlenecks later on due to lack of testing resources. AI-driven static analysis tools perform real-time codebase audits and detect vulnerabilities and flaws faster than manual reviews.

Documentation and Bug Fixes

The automation of documentation becomes an area of the software development lifecycle that practically takes care of itself. The resulting productivity gains cannot be understated; Amazon claims to

SDLC Phase	Traditional Approach	GenAI Approach
Coding	Manual code review,	GenAI generates ; human
Testing	Manually written testing	Automati cally generate
Debuggin g	Manual trace	AI flags & suggests fixes
Docs	Often skipped	Auto-generate d from
Review	Code review conducte	GenAI pre-screening

INDUSTRY ADOPTION AND IMPACT MEASUREMENT

Productivity and Business Value

According to the Bain & Company Technology Report 2025, average productivity gains of 10-15 percent are achieved when AI Assistants are used. For businesses that go further and completely redesign their engineering workflows around AI, productivity gains can be much larger. Goldman Sachs applied the technology to its engineering platform, using its own code base, allowing it to automate context-aware code generation, automation of the testing process, and compliance checks in real time with all engineering teams.

"AI speeds up the coding process—but everything after coding needs to be redesigned to turn coding speed into delivery speed."

This is what is really important about such technologies as organisations that use AI and do not redesign the way they review code, integrate it and deploy it will not get any benefits.

Market Dynamics

In 2025, two out of three software companies deployed GenAI tools. The market forecast predicts GenAI sector to increase from 7.84 billion in 2024 to 783.27 billion in 2037. GenAI can bring between 2.6 and 4.4 trillion annually into the world GDP, with software development being one of the top areas

RISKS AND LIMITATIONS

Code Quality and Hallucination

The AI-produced code is not necessarily right. The large language models use probabilities to generate results, meaning that their output can be highly plausible but subtly incorrect. This leads to accumulation of technical debt. In the study by GitClear, an observable

increase in the churn, or editing of recent code, was found coincident with growing usage of the AI tools. Human review is crucial, especially if the code will work in production.

Security and Legal Issues

Since the generative models are based on training on public code repositories, they can produce security flaws seen in the training set. Developers may lack the time for proper security reviews and thus put the systems in danger. At the same time, it is yet unclear who holds the copyright on AI-produced code, leaving active litigation over its usage in multiple countries.

IMPLICATIONS FOR THE WORKFORCE

Evolving Roles of Software Developers

Instead of doing away with the software developer profession, GenAI redefines it. Software developers now assume more of an orchestration role, verifying the outputs of AI, with technical skills becoming more oriented towards system design, code analysis, accurate requirement specification, and ensuring ethical governance in AI-enabled decision-making processes. Gartner predicts that 80% of software engineers will be required to reskill by 2027 in order to effectively collaborate with these tools. Stanford University studies show that there was a 20% decline in employment rates among software developers aged 22- 25 between 2022 and 2025, but causal relationships need further research

New Specialisations

Specialised roles have emerged in the software development process with the incorporation of GenAI: AI integration engineers, responsible for integrating and maintaining AI tools; AI security auditors, tasked with reviewing generated code for possible weaknesses; MLOps engineers, responsible for building and operating AI development frameworks; and prompt engineers, specialised in optimising prompts to generate optimal results from AI.

FUTURE DIRECTIONS: AGENTIC ENGINEERING

The current AI programming tools are sophisticated but essentially reactive—they act on human inputs at every stage. The future is radically different. AI systems following the agentic paradigm receive a goal, autonomously break it down into subtasks, generate and execute code, conduct tests, debug errors, and reach a working solution without much human input. Initial applications like Claude Code and

Devin have proved not only the real promise but also the current shortcomings of this paradigm, especially when it comes to correctness in complex architectures.

According to Deloitte's 2026 enterprise survey, worker availability of AI doubled in 2025, and enterprises with 40% or more AI projects in operation are expected to increase by two times within six months. The trend towards future software pipelines where human programmers mostly work on setting the requirements and validating AI-generated solutions is obvious. But it calls for breakthroughs in verification of AI-generated code, proof of correctness, and regulation of the latter.

CONCLUSION

The data is clear: generative AI technology can significantly enhance the process of coding, testing, debugging, and documenting—with measurable gains in efficiency of 10-55%, according to the type of task and integration level involved. The new technology also poses risks that need to be managed: generated bugs, potential security weaknesses, intellectual property issues, and the eventual diminution of expert judgment in engineers using AI-produced output without critical analysis.

"Rather than whether to use generative AI, the key strategic question is about how to govern, incorporate, and develop organizational capability through its use—safely and at scale."

For the IT industry, the moment of inflection has arrived. Organizations that transform their software development process based on AI abilities, invest in necessary infrastructure, and develop complementary human skills like critical thinking, systems thinking, and ethical governance will dominate in software engineering.

REFERENCES

- MIT Technology Review (2025). Investigates GitHub Copilot's 20M-user milestone, productivity gains, and developer concerns. Dec 2025
- Tobore, Medium (2026). Broad overview of how AI is reshaping dev workflows, code-share statistics, and Amazon's $260M savings. Feb 2026
- Menlo Ventures (2025). State-of-GenAI enterprise report; AI coding tools reached $4B in spend—the largest departmental AI category. Dec 2025

Federated Learning: Intrusion Detection Systems for Secure IoT

Sheik Rayhan

S2 BSc Computer Science

ABSTRACT

Industrial Internet of Things (IIoT) and fog computing paradigms have raised new cybersecurity risks due to decentralized infrastructure, constrained resources, and innovative attack vectors. Centralized IDS suffers from major drawbacks in terms of data privacy and scalability in such distributed computing systems. In this study, we provide an extensive overview of federated learning-based intrusion detection strategies for secure IIoT and fog computing. We explore novel frameworks related to privacy-preserving machine learning models, multilayer security architecture, and continual learning algorithms to counter low rate distributed DoS attacks, Byzantine failures, and advanced persistent threats. The application of federated learning along with optimization methods, honeynets for collecting training datasets, and adaptive protocols helps significantly in achieving high detection rates without violating any privacy concerns. Our review indicates that federated continual learning can provide more than 95% detection rate and thus is superior compared to conventional neural network methods. We summarize our work by providing future research directions for secure IIoT applications.

INTRODUCTION

The advent of the Fourth Industrial Revolution brought about profound changes in manufacturing processes, medical treatment systems, and other types of essential infrastructure, which are facilitated by industrial Internet of Things (IIoT).

Such systems allow for achieving extremely high automation levels, constant control, and information-based decision-making in the realm of industry. In turn, the mentioned digital transformation of industrial operations creates new cybersecurity problems, which are difficult for existing methods of protection to solve effectively.

Today's IIoT networks include an array of embedded devices, proprietary data, and reconfigurable access points responsible for carrying out functions related to system testing and diagnosis, as well as health monitoring. One of the widely used standards facilitating access to the devices is the IEEE Std. 1687 (IJTAG) standard. Although it helps to manage systems effectively, the use of a reconfigurable design makes the mentioned systems highly susceptible to machine learning-based attacks, differential attacks, and power analysis attacks, which allow obtaining cryptographic keys and chip IDs. springeropen.com

Fog computing systems, which represent an extension of cloud computing to the network edge and provide low latency computing for use cases like autonomous systems and medical monitoring, are susceptible to certain security risks. Decentralized architecture and constrained computational capacity make fog nodes more vulnerable to targeted and elaborate cyber-attacks, in particular, low-rate Distributed Denial-of-Service (DDoS) attacks and XSS-SQLi attacks. springer.com

Centralized intrusion detection systems, despite their popularity, reveal critical shortcomings when applied in such settings. Privacy issues become relevant due to the requirement to aggregate sensitive information in central hubs, problems related to scalability emerge in line with increasing network size, and lack of flexibility prevents the timely identification of emerging types of attacks. Such constraints call for new solutions.

The current paper discusses recent trends in intrusion detection based on federated learning applied to IIoT and fog computing settings. Specifically, we focus on integrating privacy-preserving machine learning algorithms with advanced optimization techniques and evaluating continual learning methods in the context of combating emerging cyber-attacks.

BACKGROUND AND RELATED WORK

Cybersecurity Threats to IIoT

There have been many developments regarding the IIoT cybersecurity threat landscape with adversaries making use of more and more advanced methods to affect industrial operations. The Time-Triggered Ethernet (TTEthernet), which is based on the SAE AS6802 standard, offers deterministic communication and accurate clock synchronization which are critical features for the functioning of IIoT systems. But because of deployment in various connected environments, clock synchronization mechanisms become vulnerable to attacks such as latency manipulation, spoofing attacks, and Byzantine faults which go beyond the conventional fault-tolerance model. springer.com

With regard to cybersecurity threats to CPSs, deep learning-based approaches have proven to be efficient solutions by providing automated detection of attack patterns which cannot be detected using conventional approaches. Multi-agent systems analysis, with respect to both safety and cybersecurity issues, has gained significant momentum lately. ieee-jas.net

Limitations of Centralized Solutions

Centralized intrusion detection mechanisms necessitate the collection of network traffic information and system logs in a single central location, which poses a number of inherent problems in IIoT implementations:

1. Security risks: Transmission of confidential operational data through network interfaces poses the risk of interception and breach.
2. Scaling issues: Central processing nodes act as chokepoints as networks grow more complex and generate large amounts of data.
3. Potential for single points of failure: Centralized detection mechanisms may be compromised, rendering all security surveillance operations inoperable.
4. Time lags: Latency problems in round-trip communication make real-time reactive measures impossible.

Principles of Federated Learning

Federated learning is an efficient technique that allows training models in a collaborative way without moving data from various nodes. By doing so, federated learning can mitigate problems of centralized model building related to issues of security and scalability. In federated learning systems, local models are developed on the basis of locally stored data, and only local model parameters are moved to a centralized location for creating the global model.

The federated averaging technique, often used for aggregating local models, calculates weighted average of local model parameters taking into account the amount of data processed by each node. Thus, global models can be built taking into account the patterns present throughout the whole system without revealing any operational information outside local networks

INTRUSION DETECTION FRAMEWORKS USING FEDERATED LEARNING

FedContinualIDS Framework Design

A new intrusion detection framework using Federated Continual Learning (FCL) approach has been presented by researchers. The proposed FedContinualIDS model is developed specifically for detection of attacks on fog computing systems. In addition to federated learning mechanism, the proposed model uses Manta Ray Foraging Optimization (MRFO) for selecting relevant features from high-dimensional fog network data. springer.com

The proposed FedContinualIDS uses the HIKARI dataset, which contains 555,278 samples with 85 features representing real and artificial attacks. Pre-processing involves the use of Isolation Forest and Synthetic Minority Oversampling Technique (SMOTE) algorithms to remove outliers and address the issue of class imbalance in local training data only.

Local models employ Elastic Weight Consolidation (EWC) technique that mitigates catastrophic forgetting phenomenon in machine learning. EWC is employed to identify and preserve parameters important for previously learned tasks through regularization when trained on new data.

Experimental results indicate that FedContinualIDS model attains a detection accuracy of 95.67%, significantly higher than other techniques such as Artificial Neural Networks (accuracy 84.74%) and Feedforward Neural Networks (accuracy 87.92%). FedContinualIDS demonstrates improved detection accuracy of minority classes.

Honeynet-based Framework for Privacy-Preserving Machine Learning

A novel hybrid method for cyberattack classification based on honeynet-based data collection combined with the use of federated learning was introduced recently. The approach tackles the issue of obtaining attack samples while ensuring security and privacy during the data collection process in Industry 4.0 environments. springer.com The framework considers different deep learning models like GRU, LSTM, BiLSTM, TD-CNN-LSTM, TD-CNN-BiLSTM, and ResNet50-1D. The results of the analysis under both IID and Non-IID scenarios reveal that the ResNet50-1D model outperforms other deep learning models both for centralized and federated implementations

Incremental learning allows building continuously improved models in response to newly observed attack types, and federated approaches are competitive with centralized base implementations on metrics such as accuracy, precision, recall, and loss.

SECURE ACCESS PROTOCOLS FOR HARDWARE SECURITY

Multi-Dynamic Template-Based Protection

Apart from intrusion detections on networks, securing hardware access procedures is another critical aspect of comprehensive security in IoT devices. Research has focused on identifying the weaknesses in IEEE 1687 (IJTAG) networks with respect to developing secure access protocols robust against machine learning, differential, and power attacks on them. springeropen.com The classical method of utilizing static templates in implementing secure access procedures presents vulnerabilities due to lack of unpredictability, which can be exploited for key recovery by the adversary.

In contrast, using a multi-dynamic template-based secure access procedure involves the use of several templates to insert keys, where the template used depends on the last generated bit of the access bitstream.

This adds an element of unpredictability in inserting the keys and increases the difficulty level of adversarial attacks. Tests performed using eight templates show that the accuracy rate of the machine learning attack falls to 0.0002% from 98.31%. With the multi-dynamic template-based protocol in place, key retrieval time from differential analysis increases from 3 ms to 1.67×10^{10} years. springeropen.com

Efficient Protocol Implementation

The developed protocol leads to remarkable reductions in bit stream length for key insertion purposes while preserving all security features. For 16-bit templates with 256-bit key, the required bit stream length is reduced from 16.6 million bits to 12.8 thousand bits. In the case of 24-bit templates with 256-bit key, the reduction in bit stream length is observed from 4.2 billion bits to 57.2 thousand bits

Efficient implementation results have been obtained from hardware synthesis on ITC'16 IJTAG benchmarks where only minimal implementation overheads were seen – an increase in area of only 1.65% and 1.53% for TreeFlatEx and TreeBalanced benchmarks, respectively. springeropen.com

MULTILAYER DEFENSE ARCHITECTURES

Adaptive Security Framework for TTEthernet

Protecting time-sensitive industrial communication protocols necessitates a multi-faceted approach toward ensuring security. A four-layer adaptive Multilayered Defense Framework has been developed for securing the clock synchronization function in TTEthernet from intelligent cyber attacks in Industrial Internet-of-Things (IIoT) systems. springer.com

The multilayer security architecture incorporates cutting-edge security mechanisms such as:

- ·Artificial Intelligence and Machine Learning: To automate threat detection and adapt to changing threat landscapes .

- ·Distributed Ledger Technology (DLT): To maintain an immutable log of clock synchronization activities
- ·Zero Trust Architecture (ZTA): To assume no trust by default and verify everyone continuously
- ·Post-Quantum Cryptography (PQC): To protect against attacks based on future quantum computing technology

Security vs. Real-Time Performance

While the natural fault-tolerant nature of SAE AS6802 offers basic safety from random failure events, it fails to protect against deliberate and planned attacks by skilled hackers. The proposed methodology takes care of this shortcoming without compromising the ability of the system to work in real time.

The application of security features at different levels of the protocol stack facilitates defense-in-depth without compromising on performance. This trade-off between security effectiveness and efficiency is one important point that needs consideration during implementation. springer.com

COMPARATIVE ANALYSIS

The following table compares the various intrusion detection approaches used in IIoT environments

Approach	Accuracy	Privacy	Scalability	Adaptability
Centralized ANN	84.74%	Low	Limited	Static
Centralized FNN	87.92%	Low	Limited	Static
FedContinuallDS	95.67%	High	High	Continual
Honeynet + FL	Comparable	High	High	Incremental

Comparative analysis of the above results indicates that the federated learning-based approaches deliver better detection accuracy, privacy, and scalability features, which are required for distributed industrial applications

DISCUSSION AND FUTURE WORK

It is clear from the reviewed studies that great strides have been made in the development of cybersecurity solutions suitable for IIoT and fog computing. Specifically, federated learning algorithms effectively tackle the privacy problem associated with centralized detection models, while maintaining better detection performance than the classical neural networks.

Some important directions for future research include:

- Heterogeneous device support: Since industrial applications often involve different types of devices with varying computing capabilities, it will be important to develop flexible federated learning algorithms to cater to such heterogeneity.
- Real-time detection delay: Even though federated learning algorithms improve on the communication overheads associated with centralized learning, there still remains scope for improving the delay involved in detection.
- Adversarial resilience: Since federated learning involves new security problems, it will be essential to devise efficient defense methods against new kinds of attacks such as model poisoning where adversaries provide wrong models.
- Standardization initiatives: Incorporation of security schemes with other standards such as IEEE 1687 and SAE AS6802 needs further collaboration between security and standardization communities.

CONCLUSION

In this paper, the advancements in intrusion detection systems based on federated learning approach have been discussed as a promising solution for implementing secure IIoT and fog computing. The Federated Continual Learning Intrusion Detection System (FedContinualIDS) framework indicates that federated continual learning enables the system to maintain the accuracy rate of 95.67%, while at the same time ensuring privacy of collected data

Secure access protocols based on multi-dynamic templates enable minimal accuracy of attacks on the machine learning model, while providing efficient implementation. AI/ML, blockchain, zero trust architecture, and post-quantum cryptography ensure comprehensive protection for time-critical industrial communication protocols. The presented innovations can help overcome the inherent constraints associated with centralized security solutions, allowing for deploying effective cybersecurity measures without violating any privacy considerations.

REFERENCES

- "Secure and scalable access protocol for enhancing IEEE 1687 network security," Cybersecurity, vol. 9, art. 37, Mar. 2026.
- "Intrusion detection model for secure fog computing: harnessing with federated continual learning using the HIKARI dataset to combat emerging attacks," Progress in Artificial Intelligence, Mar. 2026.
- V. Khullar et al., "A Honeynet-driven privacy preserving incremental learning framework for cyberattack classification in Industry 4.0 environments," Journal of Network and Systems Management, vol. 34, art. 71, Mar. 2026.
- "Securing TTEthernet clock synchronization in the IIoT: A multilayered defense against intelligent cyber-attacks," Cluster Computing, vol. 29, art. 154, Feb. 2026.
- J. Zhang et al., "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," IEEE/CAA Journal of Automatica Sinica, 2021.
- D. Zhang et al., "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," IEEE/CAA Journal of Automatica Sinica, 2021.
- B. Gupta et al., "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system," IEEE/CAA Journal of Automatica Sinica, 2021.

Geography's Role in Explaining Floods and Environmental Change in Kerala

Ms. Santhi M S
Asst. Prof.,
Dept of Geography

Kerala, renowned as "God's Own Country," offers a rich variety of geography. From the mountainous regions to dense forests and river systems to backwaters, this beautiful and diverse geographical setting contributes significantly to the environment of the area. Geography has assumed increasing significance over the last few decades, as the state faces more and more instances of floods and landslides.

GEOGRAPHICAL FEATURES OF KERALA

The state of Kerala lies between the Western Ghats on its eastern side and the Arabian Sea on its western side. The geographical features of this narrow strip of land are categorized into three broad physiographic divisions:

1. The Highland Zone (Eastern Zone)
This zone comprises mountainous landscapes with undulating topography, dense forest cover, and plantation cultivation. Some examples of districts in this zone include Idukki and Wayanad.

2. The Midland Zone (Central Zone)
This zone includes undulating landscapes comprising hills and valleys which are agriculturally very productive.

3. The Lowland Zone (Western Zone)
These regions comprise fertile river deltas, backwaters like Vembanad Lake, etc.

This varied landscape directly influences rainfall patterns, drainage systems, soil types, vegetation, and settlement distribution.

FLOODS AND ALTERATIONS IN THE CLIMATE

Recently, there has been an increase in extreme climatic conditions like floods in Kerala. One of the most prominent occurrences was the Kerala floods that occurred in 2018.

Although the occurrence of monsoonal rainfall has always been part of the climate conditions in Kerala, alterations in its pattern and intensity have made it even more dangerous for people. Through geography, one can see how rainfall patterns affect the occurrence of floods through studying the nature of interactions between brief rainfall periods and rivers. The rivers in Kerala are small in size and swift; moreover, they start in Western Ghats and empty out into the ocean within a short distance from the start.

The human element makes it even worse since people continue cutting down vegetation in the Western Ghats, reducing their water retention capacities and increasing the volume of runoff. At the same time, unplanned construction and urbanization have become major obstacles for water flows.

LANDSLIDES IN HIGH ALTITUDE AREAS

Landslides are another example of an environmental problem faced in the high altitude regions of Idukki and Wayanad. This is due to the presence of rugged terrain and weak geology. In times of heavy rains, the rainwater gets into the ground and weakens the stability, leading to landslides. Quarrying, construction of roads, and deforestation further contribute to the weakening of the slopes. Geographical study will help identify the potential landslide prone areas and their risks.

ROLE OF GIS AND ADVANCED TECHNOLOGY

The application of advanced technology has played a vital role in advancing the study of geography in Kerala. With the help of geographic information systems and remote sensing, there is an opportunity for monitoring environmental change in a more accurate way. It enables researchers and policy makers to observe rainfall data, analyze the flow of rivers, and prepare hazard maps. In emergencies, GIS plays a key role in planning evacuation routes, coordinating rescue efforts, and assessing the extent of damage.

ENVIRONMENTAL CONSERVATION AND SUSTAINABLE DEVELOPMENT

Geography is very important even in environmental conservation and sustainable development. It is because the environment of Kerala, especially that of the Western Ghats and other natural geographical resources such as the rivers,

wetlands, and backwaters, is highly prone to any kind of human interference. The Western Ghats are natural barriers that have an influence on precipitation patterns and contain high biodiversity. Also, the wetlands and backwaters serve as natural flood control mechanisms through the absorption of excess water. The importance of protecting such geographical features cannot be underestimated in terms of sustaining ecological stability. Geography stresses the need to undertake sustainable land use policies, afforestation, soil conservation, and preservation of water bodies.

Climate change is also an important aspect to consider as far as geography is concerned. Global warming and changing patterns of rainfall and rising sea levels are the challenges facing Kerala. Such trends are analyzed to formulate appropriate climate change adaptation measures.

GEOGRAPHY AND PREPAREDNESS FOR THE FUTURE

Geography, while helping us understand our environmental problems, can also be used to solve them. The integration of the elements of physical geography (landforms, climate, and hydrology) along with human geography (human population and usage of the land) will enable authorities to:

- Create early warning systems
- Take climate change adaptations
- Build sustainable cities
- Increase disaster preparedness

To sum up, the issues related to the environment of Kerala are inseparable from the characteristics of its geography and activities of people. Through the lens of geography, one can analyze the complex relationships between all those factors, and, in addition, find solutions to environmental and disaster management issues and ensure sustainable development.

REFERENCES

- · Government of Kerala (2018), Post Disaster Needs Assessment: Kerala Floods 2018.
- · India Meteorological Department – Climate data and monsoon reports
- · Kerala State Disaster Management Authority – Hazard and risk assessments
- · Centre for Earth Science Studies – Studies on landslides and environmental change
- · National Remote Sensing Centre – Remote sensing and GIS applications
- Intergovernmental Panel on Climate Change – Climate change reports

Post-Quantum Cryptography : Foundations, Algorithms, and Standardization

Ms. Anila A J

Asst. Prof.,
Dept of Computer Science

ABSTRACT

The fast evolution of quantum computers is becoming an urgent problem for classic public key cryptosystems such as RSA, DSA, and ECC. In this paper, we review post-quantum cryptography (PQC) as a response to a looming quantum computing era. The main focus is made on the mathematics behind quantum-resistant algorithms, on PQC standardization performed by NIST, and on the issues related to the use of PQC in practice. Specifically, we analyze four main families of PQC, namely lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate cryptography.

INTRODUCTION

The rise of large quantum computers marks a revolutionary change in computing security. In 1994, Shor's algorithm showed that with a quantum computer powerful enough, it would be possible to solve the problem of integer factorization and discrete logarithms in polynomial time, thus compromising the RSA, DSA, and ECC algorithms – the foundations upon which most modern-day encryption relies.

Grover's algorithm further threatens the realm of symmetric-key cryptography, offering a square-root advantage in searching for unstructured data. However, although Grover's algorithm effectively halves the security provided by an AES-128 cipher, AES-256 mitigates this risk easily. This is

unlike the case of public-key encryption systems, which face absolute destruction at the hands of quantum computers.

Consequently, NIST initiated the Post-Quantum Cryptography Standardization Project in 2016. Following several rounds of assessments, NIST established its initial standards for PQC in 2024, namely CRYSTALS-Kyber (FIPS 203), CRYSTALS-Dilithium (FIPS 204), SPHINCS+ (FIPS 205), and FALCON (FIPS 206).

The organization of the article is as follows: In Section II, we provide a summary of threats posed by quantum computing. Section III presents an overview of lattice-based cryptography. Hash-based and code-based cryptography are considered in Sections IV and V, respectively. Performance comparisons are discussed in Section VI, while Section VII addresses the challenges associated with implementation.

THREATS OF QUANTUM COMPUTING TO CLASSICAL CRYPTOGRAPHY

Classical cryptographic systems are built upon certain computational assumptions, such as the complexity of integer factorization (RSA), calculating the discrete logarithm (DSA, DH), or the complexity of the elliptic curve discrete logarithm problem (ECDSA, ECDH).

With sufficient quantum computing power, Shor's algorithm solves all these problems in polynomial time $O((\log N)^3)$ while the best classical solutions have sub-exponential complexities.

There is significant uncertainty in the development timeline of CRQCs, but current forecasts suggest the emergence of quantum computers with several thousand logical, error-corrected qubits within the next 10-15 years. Still, "harvest now, decrypt later" approach, which means collecting currently encrypted information for further decryption when quantum computing becomes feasible enough, calls for an urgent transition to new solutions.

Impact Assessment

RSA-2048: Completely broken with Shor's algorithm. About 4,000 logical qubits needed.
ECC-256: Broken with quantum version of Shor's algorithm, about 2,330 logical qubits needed.
AES-256: Reduced to ~128-bit effective complexity by Grover's algorithm. Still usable.

LATTICE-BASED CRYPTOGRAPHY

Lattice-based cryptography is the current frontrunner family of cryptosystems designed to achieve post-quantum security and forms the basis of the majority of NIST-selected algorithms. It relies on the conjectured hardness of lattice problems.

Hard Lattice Problems

Learning With Errors (LWE) was proposed by Regev . It deals with determining whether (A, As + e) is uniformly distributed or not, where A is a random matrix, s is a secret vector, and e is an error vector. MLWE and RLWE are efficient variants of this problem, thanks to ring structure.

The SVP and CVP are canonical NP-hard problems. There exists no quantum algorithm which can give any significant advantage in efficiency when compared to classic algorithms for solving them.

CRYSTALS-Kyber (FIPS 203)

CRYSTAL-Kyber is a KEM that provides security against adaptive chosen ciphertext attacks (IND-CCA2) based on the module learning with errors problem. The CRYSTAL-Kyber algorithm works over the polynomial ring Zq[X]/(X^n+1), where n=256 and q=3329. CRYSTAL-Kyber-768 has a security level of about 180 bits classical and 164 bits quantum security. CRYSTAL-Kyber is extremely efficient in key generation, encapsulation, and decapsulation operations, making it ideal for use in embedded devices like IoT.

CRYSTALS-Dilithium (FIPS 204)

CRYSTAL-Dilithium is a post-quantum digital signature scheme designed by NIST based on the hardness of the MLWE and Module Short Integer Solution (MSIS) problems. The design of the Dilithium signature scheme uses the Fiat-Shamir with Aborts paradigm. CRYSTAL-Dilithium-3 is designed to achieve

HASH-BASED AND CODE-BASED CRYPTOGRAPHY

Hash-Based Signatures

Hash-based signatures provide a conservative approach, based only on the security of the hash function used. SPHINCS+ (FIPS 205) represents a stateless hash-based signature scheme which makes use of hypertrees of WOTS+ and FORS one-time signature schemes. The fastest version, namely SPHINCS+-128s, provides 128-bit

security against quantum adversaries and a small 64-byte public key, but still requires quite large signatures (7,856 bytes).

security against quantum adversaries and a small 64-byte public key, but still requires quite large signatures (7,856 bytes).

Code-Based Cryptography

The code-based cryptographic approach relies on the problem of decoding random linear error-correcting codes, introduced by McEliece in 1978. The Classic McEliece system, one of the four NIST finalists, employs binary Goppa codes and guarantees exceptionally high security with extensively studied parameters. Nevertheless, its massive public keys (261 KB for 128-bit security) prevent widespread adoption.

Multivariate Cryptography

In contrast to lattice-based approaches, multivariate cryptosystems utilize the hardness of solving systems of multivariate polynomial equations defined over finite fields. Although they exhibit superior efficiency during signature generation, they have been subject to cryptographic attacks. NIST's choice of UOV (Unbalanced Oil and Vinegar) as the fourth standard highlights its advanced security evaluation despite enormous key sizes.

PERFORMANCE & COMPARISON

Table I provides a comparative performance assessment of NIST-based PQC algorithms against conventional algorithms using the following parameters. The performance values were obtained via benchmarking conducted on Intel Skylake processors.

Encryption Algorithm	Type	Public Key Size	Signature/Message Size	Security Level
RSA-3072	Classical	384 B	384 B	128 classical bits
ECDSA-256	Classical	64 B	64 B	128 classical bits
Kyber-768	Lattice KEM	1,184 B	1,088 B	PQ L3
Dilithium-3	Lattice Signature	1,952 B	3,293 B	PQ L3
SPHINCS+-128s	Hash Sig	64 B	7,856 B	L1 PQ
McEliece-348864	Code KEM	261 KB	128 B	L1 PQ

CHALLENGES IN DEPLOYMENT AND MIGRATION STRATEGIES

The switch from classical cryptography to post-quantum cryptography poses formidable challenges from systems engineering perspective and goes way beyond just picking algorithms. The following factors need to be taken into account:

Cryptographic Agility:Infrastructure needs to be able to support swapping out cryptographic primitives without necessitating a complete redesign. Research is underway to enable such support on protocol level (TLS 1.3, SSH, X.509).

Hybrid Approach:Both the IETF and NIST suggest using a hybrid key exchange mechanism involving classical encryption and post-quantum encryption until it is fully rolled out as a standard [8].

Performance Cost:PQC encryption usually entails increased key and ciphertext size. Increased data overhead should be accounted for on network protocol layer. Lattice NTT hardware acceleration is an ongoing research topic.

Side-Channel Mitigation : Implementations need to be resistant to timing, power, and cache-based side-channel attacks. Implementation of masked Kyber and Dilithium has been successfully tested on embedded devices.

CONCLUSION

Post-Quantum Cryptography is one of the most important shifts in the history of information security. The ratification of NIST FIPS 203-206 standards by the end of 2024 ensures futureproof key encapsulation and signature schemes. For general usage, lattice-based solutions strike a balance between efficiency, robustness, and key sizes; meanwhile, hash-based signatures offer a conservative solution to secure code signing and CA certificates.

However, several crucial issues still need to be addressed: efficient hardware support, standards for deploying PQC in resource-constrained IoT devices, and further cryptanalysis of chosen algorithms. It is advisable to start assessing your organization's cryptographic inventory and implementing post-quantum cryptography pilots right away, especially for systems with sensitive information that must maintain confidentiality for a long period of time.

ACKNOWLEDGMENTS

The author acknowledges the academic and research community for making algorithms, their reference implementations, and benchmarking available through public sources.

REFERENCES

- P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, 1997. [Online]. Available: https://arxiv.org/abs/quant-ph/9508027
- L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th ACM STOC, 1996, pp. 212–219. [Online]. Available: https://arxiv.org/abs/quant-ph/9605043
- NIST, "Post-Quantum Cryptography Standardization," 2016–2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
- M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018. [Online]. Available: https://eprint.iacr.org/2015/1075.pdf
- O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, vol. 56, no. 6, pp. 1–40, 2009. [Online]. Available: https://arxiv.org/abs/2401.03703
- R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report 42-44, JPL, 1978. [Online]. Available: https://tmo.jpl.nasa.gov/progress_report2/42-44/44N.PDF
- E. Alkim et al., "Post-quantum key exchange — a new hope," in Proc. USENIX Security, 2016. [Online]. Available: https://eprint.iacr.org/2015/1092.pdf
- IETF, "Hybrid key exchange in TLS 1.3," Internet-Draft draft-ietf-tls-hybrid-design. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
- D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, pp. 188–194, 2017. [Online]. Available: https://eprint.iacr.org/2017/314.pdf
- NIST, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard," 2024. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.203

Marian College of Arts and Science

Department of Computer Science

V Semester B.Sc Computer Science

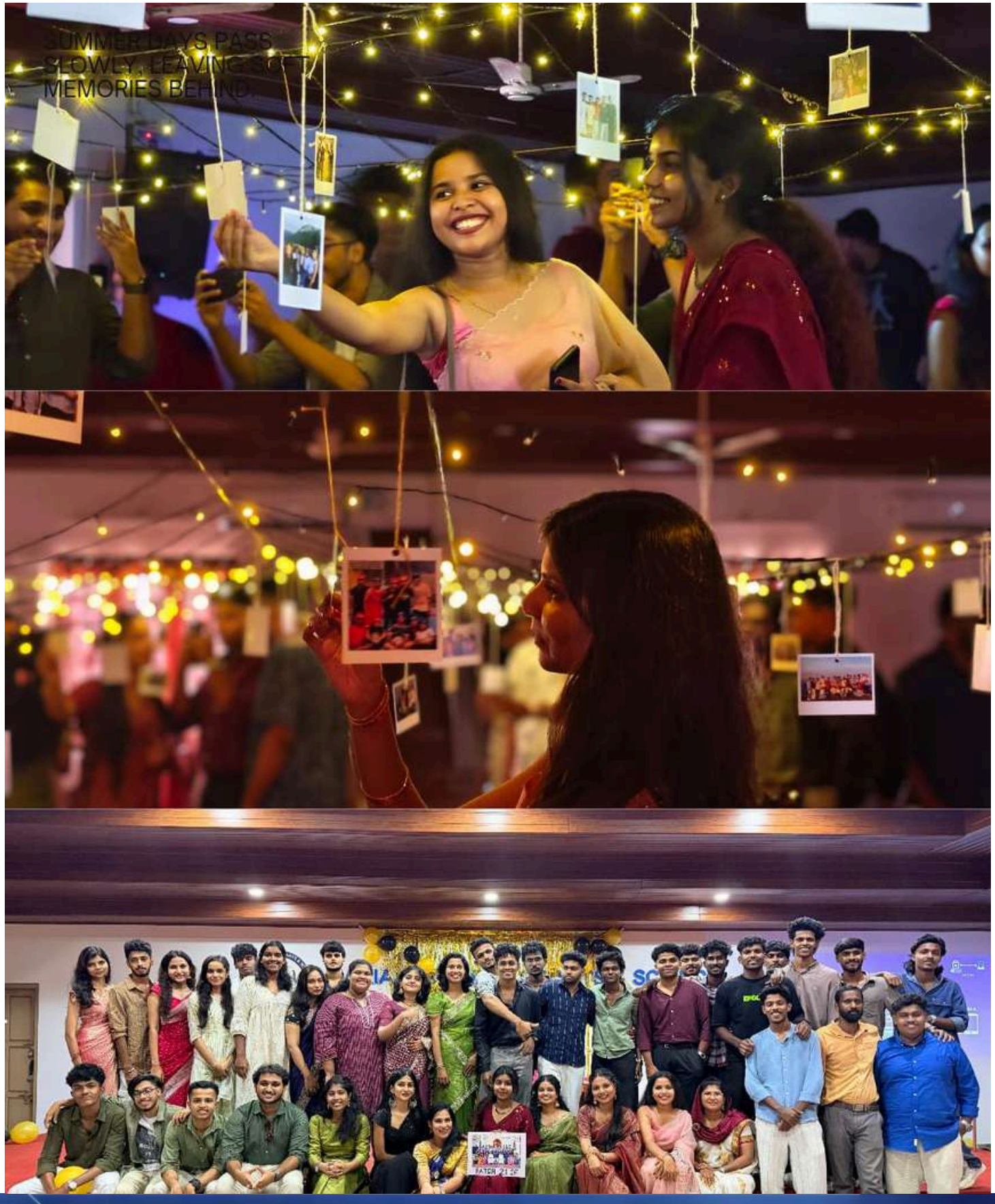
University Exam Result

SANIA BERLIN –	9.13
ANANYA VINOD –	8.98
KARTHIK A S –	8.93
DEVI NANDANA S S –	8.90
ARUNIMA M A –	8.82
ASHLEY S N –	8.80
PAVITHRA RAJESH –	8.75
ALEENA C J –	8.70
REVATHY S S –	8.53
LEONS EDISON –	8.51
DEVADUTT ANAND V –	8.44
DEVANARAYANAN –	8.39
JOTHAM RUFUS –	8.23
ARJUN M S –	8.14
VISHNU PRIYA SM –	8.02

Congratulations Toppers

CS Farewell 2026

“We extend our sincere gratitude to our seniors for their guidance and wish them success in all their future endeavors.”



CS Industrial Visit

CS-S4 visited ICT Academy located at Technopark phase 1 on 4/6/2026 as part of Industrial Visit

TECH NEWS

JMGO N3 Ultimate Launches: A New Way of Projection Powered by the World's First 3-in-1 Optical System

The JMGO N3 Ultimate introduces a significant innovation in home projection technology with its world-first 3-in-1 optical system. This system integrates lens shift, optical zoom, and a 360-degree gimbal mechanism, allowing the projector to physically adjust its position and image alignment without relying on digital correction. As a result, users can place the projector in flexible positions while still maintaining sharp image quality, avoiding the distortion and brightness loss typically caused by keystone correction.In addition to its unique optical design, the projector delivers strong performance with 4K Ultra HD resolution, high brightness levels, and a triple-laser light source that enhances color accuracy and contrast. It also includes AI-powered spatial memory, enabling the device to remember different projection setups for various surfaces or viewing scenarios. Overall, the JMGO N3 Ultimate represents a shift toward more adaptive and user-friendly projection systems, combining advanced hardware with intelligent features to improve convenience and viewing experience.

Microsoft says it’s rebuilding Windows 11 around what users actually want: performance, reliability, quality and craft

Microsoft has announced that it is rethinking the development of Windows 11 with a renewed focus on what users value most: performance, reliability, quality, and overall system refinement. This shift reflects growing feedback from users who have experienced issues such as slower updates, system instability, and inconsistent design elements.

By prioritizing these core areas, Microsoft aims to make Windows 11 faster, smoother, and more dependable in everyday use.
The company is also emphasizing "craft," meaning greater attention to detail in both design and functionality. This includes improving responsiveness, reducing bugs, and ensuring a more polished user experience across devices.
Rather than introducing only new features, Microsoft's updated approach focuses on strengthening the foundation of the operating system, signaling a move toward long-term stability and user satisfaction.

OpenAI launches 'ChatGPT Images 2.0' with smarter visual generation

Microsoft has announced that it is rethinking the development of Windows 11 with a renewed focus on what users value most: performance, reliability, quality, and overall system refinement. This shift reflects growing feedback from users who have experienced issues such as slower updates, system instability, and inconsistent design elements. By prioritizing these core areas, Microsoft aims to make Windows 11 faster, smoother, and more dependable in everyday use.
The company is also emphasizing "craft," meaning greater attention to detail in both design and functionality. This includes improving responsiveness, reducing bugs, and ensuring a more polished user experience across devices.
Rather than introducing only new features, Microsoft's updated approach focuses on strengthening the foundation of the operating system, signaling a move toward long-term stability and user satisfaction.

NCSC publishes new cross-domain architecture guidance

The National Cyber Security Centre (NCSC) has released new cross-domain architecture guidance aimed at helping organisations securely manage data flows between systems with different trust levels. The guidance introduces a modern approach to “cross domain” security, where data moves across clearly defined trust zones and boundaries using a structured pipeline of controls. Instead of relying on a single security checkpoint, the new model applies multiple layers of validation and inspection throughout the data flow, ensuring that only safe and authorised information is transferred between domains. (National Cyber Security Centre)

The updated framework replaces older design patterns and emphasizes flexibility, risk-based decision-making, and end-to-end architectural thinking. It explains key concepts such as zones of trust, control points, and layered security mechanisms, while encouraging organisations to design systems that align with evolving cyber threats. By moving away from rigid, one-size-fits-all solutions, the NCSC’s new guidance supports more adaptable and resilient cybersecurity architectures, particularly for high-risk environments where sensitive data must be shared securely across networks. (National Cyber Security Centre)

EDITORIAL BOARD