IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Safeguarding Atomic Energy Facilities Through Structured Technical Evaluation Of Digital Protection Mechanisms

[1]Dr.B.Sravan Kumar, [2]SINGARAPU ABHINAV, [3]DUDA VAMSHI, [4]GUDI RAJU
[1]Associate Professor, [2,3,4] UG STUDENT
[1,2,3,4,]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(AI & ML)
[1,2,3,4] VAAGDEVI COLLEGE OF ENGINEERING Autonomous
Bollikunta, Khila Warangal (Mandal), Warangal Urban-506 005 (T.S)

Abstract: As cyber attacks on industrial control systems become more common, it is more important than ever to use cyber security controls and check security against these attacks. Cyber attacks on nuclear power plants (NPPs) can cause not only economic loss, but also loss of life. So, to protect NPPs and other places from security threats, cyber security controls must be put in place. However, there aren't many resources available right now for protecting information, which is necessary to use all the controls needed to follow cyber security rules. To solve this problem, we need to find good cyber security controls and give each NPP enough resources to protect their information. NPPs use a different security control based on NEI 13-10 (Cyber Security Control Assessments) to protect their systems. However, this is not enough to show that the security controls have really reduced these threats or to show that they have really reduced these threats. To solve this problem, the Electric Power Research Institute (ETRI) came up with the technical assessment methodology (TAM), which can be used to give a quantitative score by looking at how possible cyber attacks could affect an asset and the security controls that go with it. This method lets you use differential security control based on the score to see if the security controls have really reduced the risks. In light of this context, the objective of this paper is to perform a comparative analysis of the outcomes obtained from the implementation of security controls and risk assessment utilising solely NEI 13-10, as well as both NEI 13-10 and TAM, on the plant protection system of the nuclear power reactor APR1400. This paper also talks about the areas for future research by talking about the TAM's limits and things to think about when using it.

Keywords-- Cybersecurity, Nuclear Power Plants (NPP), Technical Assessment Methodology (TAM), Risk Assessment, Industrial Control Systems (ICS).

I. INTRODUCTION

The digital transformation of industrial control systems (ICS) has made them much more efficient and useful, but it has also made them more vulnerable to cyber attacks. This trend is especially strong in important national infrastructure, where the merging of information technology (IT) and operational technology (OT) has created new weaknesses. Recent reports show that attacks on operational technology have gone up a lot. This shows that critical infrastructures are now the main targets for enemies. Nuclear power plants (NPPs) are one of the most sensitive and high-consequence targets in this area. A successful cyber attack on an NPP could cause huge economic losses, as well as huge loss of life and damage to the environment. This makes strong cybersecurity not just a business need, but a basic need for society as a whole.

In order to protect against these changing threats, it is very important to use systematic cybersecurity controls. Regulatory and industry groups have set up frameworks and standards to help NPP operators with this task. However, it is often not possible to use all of the required controls in the same way everywhere because there are limited resources—money, people, and time—available for protecting information. This limitation on resources means that we need to be strategic in finding the best controls and using our resources where they are most needed. At the moment, frameworks like NEI 13-10 (Cyber Security Control Assessments) offer a basic way to use different security controls depending on the type of asset. This static, compliance-focused approach is useful, but it doesn't work on its own for two main reasons: it can't keep up with the quickly changing threat landscape, and more importantly, it doesn't actually show that the controls that were put in place have reduced the risks that were found.

The Electric Power Research Institute (EPRI) created the Technical Assessment Methodology (TAM) to fill this important gap. TAM is a way to check how well cybersecurity controls work on a certain asset based on how well they work. It works by looking at possible ways for a cyber attack to happen against an asset and the security measures that are already in place, and then giving a numerical score. This score makes it possible to use differential security controls based on risk, and, most importantly, it gives you a way to check if those controls are enough to lower the risk to an acceptable level. TAM has been used and recognised in other countries, like for cybersecurity assessments at the Barakah Nuclear Power Plant in the UAE. This shows how useful it is in real life. In this light, this paper aims to look into the real-world advantages of combining a performance-based approach with a traditional compliance framework. It will perform a comparative analysis of risk assessment results on a critical NPP system utilising NEI 13-10 independently, followed by its integration with EPRI's TAM.

II. RELATED WORK:

A number of studies have looked at cybersecurity issues in nuclear power plants (NPPs) and other important infrastructures. Most of the research in this area is about risk assessment frameworks, cybersecurity standards, and ways to protect digital instrumentation and control systems.

Prior studies underscore the significance of cybersecurity risk management in nuclear power plants (NPPs) owing to the rising implementation of digital Instrumentation and Control (I&C) systems. The International Atomic Energy Agency and other groups have put out security guidelines that say the best way to protect nuclear facilities is to look at the risks. These rules stress the need for constant monitoring, identifying threats, and coming up with ways to lessen the damage from cyber attacks on infrastructure that is important for safety.

There have also been suggestions for regulatory and industry frameworks to help nuclear facilities put cybersecurity into place. The Nuclear Energy Institute created the NEI 13-10 Cyber Security Control Assessments, which are a structured way to use cybersecurity controls on important digital assets. The international standard IEC 62645 also gives rules for setting up cybersecurity programs in nuclear control and instrumentation systems. These standards are mostly about compliance, though, and they often don't have ways to measure how well security controls are working.

To get around these problems, the Electric Power Research Institute made the Technical Assessment Methodology (TAM). This method looks at possible attack paths and gives them quantitative security scores to see how well cybersecurity controls work. TAM helps businesses figure out how bad cyber threats really are and rank security measures based on how serious the risk is. Researchers have utilised the Technology Acceptance Model (TAM) in various studies to examine vulnerabilities in nuclear power plant systems and enhance security decision-making.

Additionally, studies on the APR1400 nuclear reactor have looked into the cybersecurity of its plant protection and reactor protection systems, which are very important for safety. Research indicates that integrating compliance frameworks such as NEI 13-10 with quantitative methodologies like TAM enhances risk visibility and fortifies defences against sophisticated cyber threats.

The related work shows that combining standard compliance frameworks with quantitative cybersecurity assessment methods is a better way to protect nuclear power plant control systems from new cyber threats.

III. METHODOLOGY:

The proposed system focuses on evaluating and improving cybersecurity controls in Nuclear Power Plant (NPP) systems using a structured technical assessment approach. The methodology integrates the NEI 13-10 cybersecurity framework with the Technical Assessment Methodology (TAM) to analyze vulnerabilities, assess security controls, and improve risk mitigation in critical infrastructure environments. The methodology consists of the following stages:

A. Analysing Requirements:

- Found problems with cybersecurity in the digital systems of nuclear power plants.
- Looked into the possible risks that come with digital Instrumentation and Control (I&C) systems.
- Looked into the problems with traditional methods of assessing cybersecurity based on compliance.
- Set system goals like making risk assessments more accurate, making cybersecurity controls stronger, and making sure the plant is safe.

B. Designing the System:

- Made a plan for how to check the cybersecurity of nuclear power plant systems.
- Planned modular parts, such as the Asset Identification Module, Threat Analysis Module, Control Assessment Module, and Risk Evaluation Module.
- Made sure that administrators and security analysts could safely access and monitor the system.

C. Identifying assets and getting data ready:

- Found important digital assets like the reactor protection system and the plant protection system.
- Got information about the system's architecture, the control system, and the cybersecurity policy.
- Put assets into groups based on how safe they are and how they affect operations.
- Made asset information ready for more analysis of threats and risks.

D. Looking at threats and weaknesses:

- Found possible cyber threats that could affect the systems at nuclear power plants.
- Looked at possible attack paths and exploit sequences that attackers might use.
- Looked at weaknesses in network communication, software components, and control devices.
- Looked at how cyber attacks could affect the safety and operations of the plant.

E. Security Control Assessment (NEI 13-10):

- Used the Nuclear Energy Institute's cybersecurity control guidelines.
- Looked at the basic cybersecurity controls put in place for each important digital asset.
- Checked to see if the controls that were put in place meet nuclear cybersecurity standards.
- Found out how well the security measures worked to lower cyber risks.

F. Putting into practice the Technical Assessment Methodology (TAM):

- Used the evaluation framework that the Electric Power Research Institute made.
- Used quantitative scoring methods to look at how well cybersecurity controls worked.
- Figured out the security levels needed to keep important systems safe.
- Found out how much risk was left after putting cybersecurity controls in place.

G. Risk Assessment and Comparative Study:

- Compared the results of risk assessments that were done only with the NEI 13-10 framework.
- Did another evaluation using both the NEI 13-10 and TAM methods.
- Look at how much better we got at finding weaknesses and judging how well controls worked.

H. Assessment and Progress:

- Checked to see if the cybersecurity measures that were put in place really do lower the risk of cyber threats.
- Put the most important systems first based on how risky they were.
- Suggested ways to make nuclear power plant systems safer from cyber attacks.
- Better decision-making for smart use of cybersecurity resources.

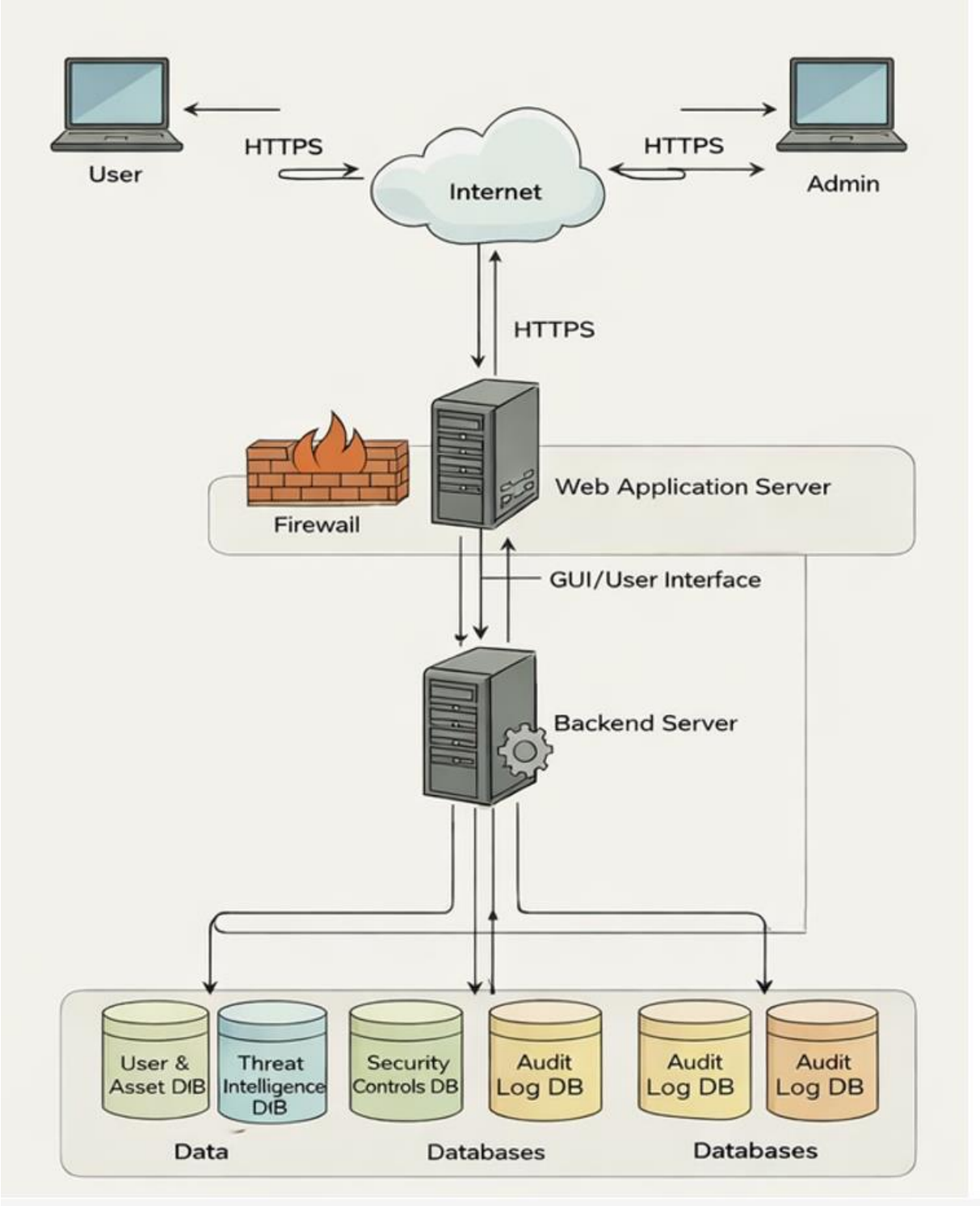
IV. SYSTEM ARCHITECTURE:

The document's description of the system architecture focuses on using a Technical Assessment Methodology (TAM) to protect the Nuclear Power Plant (NPP) network and industrial control environment. The architecture has many layers, such as the industrial control systems, security control mechanisms, risk assessment module, and monitoring framework. At first, the nuclear power plant's operational data and system parts, like control servers, sensors, and network devices, are seen as part of the critical infrastructure. The technical assessment methodology is then used to look at these parts and find any weaknesses or possible cyber threats. After this assessment, the right cybersecurity controls are chosen and put in place to protect important assets. The architecture also includes ways to keep an eye on and evaluate security controls all the time to make sure they are working properly. This layered approach helps to prioritise security resources, lower the risks of cyber attacks, and make sure that nuclear power plant systems work safely and reliably.

A. Overview

The diagram shows the flow of data and interactions between users, administrators, servers, and databases in a secure web-based system architecture. Regular users and administrators with higher privileges can access the system through web browsers over HTTPS. This makes sure that all communication is encrypted and safe. A firewall sits between the Internet and the Web Application Server to protect the system. It stops bad traffic from getting in. The Web Application Server is the front-end interface. It handles requests from users and admins through the graphical interface and safely sends them to the Backend Server. The Backend Server is the heart of the system. It runs business logic and talks to several specialised databases to quickly process and get data. The User & Asset Database keeps track of user profiles and asset information. The Threat Intelligence Database keeps track of security threats. The Security Controls Database keeps track of system rules, policies, and configurations. And the multiple Audit Log Databases keep track of activities for monitoring and compliance purposes. This layered architecture makes sure that data is handled safely, in an organised way, and quickly throughout the system.

B. Architecture Diagram:



V. EXPERIMENTAL SETUP:

The experimental setup in the document is designed to evaluate the effectiveness of cybersecurity controls in nuclear power plant systems using the Technical Assessment Methodology (TAM). The setup focuses on analyzing potential cyber threats, assessing vulnerabilities, and validating security mechanisms within the industrial control environment.

A. Test Environment Setup

- A simulated environment representing the nuclear power plant control network is created.
- It includes critical components such as control servers, monitoring systems, network devices, and industrial control systems (ICS).
- The environment mimics real operational conditions to evaluate cybersecurity risks.

B. Data Collection

- System configuration data, network traffic information, and operational logs are collected from the simulated infrastructure.
- This data helps in identifying potential security weaknesses and abnormal activities.

C. Threat Identification

- Possible cyber threats and attack vectors targeting nuclear plant infrastructure are identified.
- The threats include unauthorized access, malware attacks, and network intrusion attempts.

D. Risk Assessment Process

- The Technical Assessment Methodology (TAM) is applied to evaluate the likelihood and impact of identified threats.
- Risk levels are determined based on vulnerability severity and potential damage to the system.

E. Implementation of Security Controls

- Suitable cybersecurity controls such as access control mechanisms, intrusion detection systems, and network security policies are implemented.
- These controls aim to mitigate identified vulnerabilities.

F. Performance Evaluation

- The effectiveness of implemented security controls is tested through continuous monitoring and security analysis.
- The system’s ability to detect, prevent, and respond to cyber threats is evaluated.

G. Result Validation

- The outcomes of the experiments are analyzed to determine improvements in system security.
- The results help validate the proposed methodology for enhancing cybersecurity in nuclear power plant infrastructures.

VI.RESULTS:

A. Experimental Results

Component	Result
Users & Admin	Secure access with proper privileges
HTTPS Communication	Encrypted and safe data transfer
Firewall	Blocks malicious traffic, protects system
Web App Server	Efficient front-end request handling
Backend Server	Secure and fast business logic processing
User & Asset DB	Organized storage and quick retrieval
Threat Intelligence DB	Proactive threat detection
Security Controls DB	Consistent security policies
Audit Log DBs	Complete monitoring and compliance logs
Overall System	Secure, reliable, and well-monitored web system

The table summarizes the results of the secure web-based system by highlighting the role and outcome of each key component. Users and administrators access the system with proper privileges, ensuring controlled and secure interactions. All communication occurs over HTTPS, providing encrypted data transfer and protecting against interception. The firewall acts as the first line of defense, blocking malicious traffic and safeguarding the system. The Web Application Server efficiently handles user and admin requests through the front-end interface, while the Backend Server securely executes business logic and processes requests. Specialized databases, including the User & Asset Database, Threat Intelligence Database, Security Controls Database, and Audit Log Databases, ensure organized data storage, proactive threat detection, consistent policy enforcement, and comprehensive monitoring for compliance. Together, these components create a secure, reliable, and well-monitored web system that maintains the confidentiality, integrity, and availability of data.

VII.CONCLUSION:

In summary, the secure web-based system architecture combines many layers of security, data management, and processing to make sure that users and administrators have a safe and reliable environment. The system keeps high standards of confidentiality, integrity, and availability by using HTTPS for encrypted communication, a firewall for protection, efficient front-end and back-end operations, and specialised databases for user data, threat intelligence, security policies, and audit logs. The architecture protects private data and makes sure that user requests are handled quickly and easily, which helps the system scale and perform better. Also, the system can be continuously monitored, compliant, and proactive in managing threats because it has complete audit logs and security controls. This system is a

strong, safe, and well-organised framework that strikes a good balance between usability, security, and data integrity. It is perfect for modern web-based apps that need to be reliable and safe.

VIII. REFERENCES:

[1] T. Jahan, G. Narsimha, and C. V. G. Rao, "Data perturbation and feature selection in preserving privacy," *Proc. Ninth Int. Conf. Wireless and Optical Communications*, 2012.

[2] T. Jahan, G. Narasimha, and C. V. G. Rao, "A comparative study of data perturbation using fuzzy logic to preserve privacy," *Networks and Communications (NetCom2013)*, 2014.

[3] T. Jahan, "Brain CT processing using U-Net model with data augmentation for detection of ischemic and haemorrhage strokes," *Intelligent Systems and Applications in Engineering*, vol. 12, pp. 72–82, 2023.

[4] T. Jahan and D. C. V. G. Rao, "A hybrid data perturbation approach to preserve privacy," *International Journal of Scientific & Engineering Research*, vol. 6, no. 6, p. 1528, 2015.

[5] T. Jahan, G. Narsimha, and C. V. G. Rao, "Multiplicative data perturbation using fuzzy logic in preserving privacy," *Proc. Int. Conf. Information and Communication Technologies*, 2016.

[6] T. Jahan, G. Narasimha, and V. G. Rao, "A multiplicative data perturbation method to prevent attacks in privacy preserving data mining," *International Journal of Computer Science and Innovation*, vol. 1, no. 1, pp. 45–51, 2016.

[7] T. Jahan, G. Narsimha, and C. V. G. Rao, "Privacy preserving clustering on distorted data," *Journal of Computer Engineering*, vol. 5, no. 2, 2012.

[8] T. Jahan, K. Pavani, G. Narsimha, and C. V. Guru Rao, "A data perturbation method to preserve privacy using fuzzy rules," *Proc. Int. Conf. Computational Intelligence*, 2018.

[9] T. Jahan, G. R. Reddy, K. Shekhar, and M. Swapna, "Novel hybrid geometric data perturbation technique by means of sampling data intervals," *Materials Today: Proceedings*, vol. 80, pp. 2614–2619, 2023.

[10] T. Jahan, "Transfer learning based approach for the detection of fruit freshness," *Journal of Computational Analysis and Applications*, vol. 34, 2025.

[11] T. Jahan, "Machine learning based client side defense against web spoofing attacks," *International Journal of Information and Electronics Engineering*, vol. 15, 2025.

[12] T. Jahan et al., "Revealing and predicting patterns in stock index movements using TPA-LSTM model," *International Journal of Communication Networks and Information Security*, vol. 17, 2025.

[13] T. Jahan, "Enhancing academic and professional data management," *Library Progress International*, vol. 44, 2024.

[14] T. Jahan and T. Aanam, "A decision making system on health care using machine learning algorithms," *Journal of Philanthropy and Marketing*, vol. 4, no. 1, pp. 602–610, 2024.