Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

IAM based Audit Framework to enhance and protect the Critical Infrastructure for Distributed System

Saikrishna Tipparapu
Windows Engineer, University of the Cumberlands, Williamsburg, Kentucky, USA.
Lewis Center, OHIO, infosectsk@gmail.com

ARTICLE INFO

Received: 20 Dec 2024

Revised: 01 Feb 2025

Accepted: 19 Feb 2025

ABSTRACT

Manufacturing facilities, transportation networks, energy distribution networks, and power plants are all examples of Critical Infrastructure (CI) that modern communities depend on to provide goods and services. Due to their size, complexity, and unique features, these CIs frequently require the assistance of Industrial Automation and Control Systems (IACS). IACS manages assets and administers day-to-day activities. With additional processes and networked monitoring and controlling devices, the attack surface of the underlying CIs grows in these increasingly complex IACS. To establish and discern the correlation between worldwide concerns concerning Critical Infrastructure Protection (CIP) and cybersecurity. In order to support the economy and security interests, it is necessary to guarantee that systems, goods, and services are sufficiently reliable and resilient. This circumstance necessitates the development of new ways based on advanced data analytics techniques that can extract insights from the CI to enhance Critical Infrastructure Protection (CIP) frameworks. This paper introduces a proposed IAM-based audit framework that integrates capabilities for forensic investigation and audit compliance through effective architectural functions within security systems. The framework incorporates algorithms such as data acquisition and domain processors. The data acquisition algorithm processes a substantial dataset, comprising organized data for cloud identity and access management systems, including AWS, Azure, and Google Cloud datasets. It employs a DMA process to evaluate system performance metrics such as perceived data rate, ingested rate, and consumed rate. Afterward, the domain processor computes the data event by utilizing the determined ingested event as input. By changing the number of nodes or clients from 3 to 10, the suggested framework can help find the biggest event that is ingested, the longest time it takes to compute, and the shortest time it takes to compute. This article also introduces the Interruption and Abnormality-based Identification System (IAIS), a novel architecture designed to enhance Critical Infrastructure Protection (CIP) globally. By integrating forensic readiness and compliance auditing, IAIS addresses challenges in post-incident investigation and real-time monitoring. Its cloud-native design ensures scalability, making it a vital tool for safeguarding critical systems against evolving cyber threats Furthermore, this experimental evaluation also demonstrated the utility of the suggested framework in detecting common sequences of attacks.

Keywords: Critical Infrastructure Protection; Identity and Access Management; Industrial Automation; Authentication.

I. INTRODUCTION

Critical infrastructures, like power production and distribution networks, transportation systems, and industrial plants, provide more and more of the goods and services that make modern life possible. This means that any problems or downtime in these situations could have terrible results, including service delays, big financial losses, damage to valuable goods, or even death. Because of these and other reasons, these kinds of systems are becoming more and more appealing to hackers [1]. Concerns about security have the potential to impact both service availability and user safety. However, things aren't looking good either because the CI model is always expanding.

In reality, CIs are getting more complicated because sensors, actuators, and other related devices are becoming more popular and are often spread out in the field. Also, more and different kinds of information are being sent between system parts within the network. A number of developments, such as smart grids, transportation networks, oil and gas distribution, and Industry4.0, are posing threats to the conventional infrastructure paradigm [2]. This is giving rise to a new wave of Industrial Automation and Control Systems. The IIoT's (Industrial Internet of Things) slow but steady rollout is adding weight to this trend.

As CIs get more complicated and linked to their surroundings, the need to guarantee higher levels of availability and dependability grows. This is because tools, infrastructures, and services are more dependent on and linked to each other. Because of this change in thinking, the needed protected infrastructures need to get bigger and more complicated. There is an increasing number of dangers to these systems, and they must be able to identify and thwart them before catastrophes strike.

All of these things need the right security measures. Most people in the ecosystem think that making the right CIP mechanisms is important. However, a lot of work has been put into making tools and procedures for prevention, detection, and mitigation, and not much has been done on other things like forensics support or compliance audits. It would be a mistake to disregard the second part, though, since it is supported by numerous compelling arguments. In order to determine what went wrong and collect evidence, a postmortem trace analysis is necessary during the "lessons learnt" stage of best practices for incident handling.

• Extensive knowledge supports the definition of secure and safe systems and the rules over CI operation, management, and maintenance. Effective rules rely on ongoing monitoring, which becomes more challenging as infrastructure size and complexity increase.

This paper presents an IAM based Audit Framework that offers explicit assistance for these operations within the context of protect the Critical Infrastructure. This enhanced flight recorder is designed for a particular domain and includes compliance auditing, support for CI security policies, and forensics for analyzing events after the fact. A cloud-based method can be used to make it bigger. A unified security solution for distributed IACS can be more easily created with the design of the proposed framework.

The tools it provides are simple to implement, navigate, modify, and expand upon.

This method promises the gathering of forensic data and helps stop unexpected events from happening again by using categorization tools when checking for deviations from normal behaviors. This will help lower the risks that come with cyberattacks and operational breakdowns.

Checking that the CI security rules are being followed also helps to prevent future security problems.

Forensic research results can be used to audit regulatory compliance, allowing for the reuse of methods.

- IAM based Audit framework is proposed as it helps to incorporate the capabilities for forensic investigation and audit compliance with effective architecture functions with security systems.
- The framework integrates algorithms like data Acquisition and domain processors. The data Acquisition algorithm takes the input of large dataset, which is a collection of organized data for cloud identity and access management systems, which includes AWS, Azure, and Google Cloud datasets and it performs through DMA process to determine the system performance like perceived data rate, Ingested and consumed rates.
- Then determined ingested event is taken as the input into the process of domain processor to calculate the data event. In the performance analysis, proposed framework helps to generate the max ingestion event, maximum computational time and minimum computational time based on the number of nodes / clients from 3 to 10.

II. RELATED WORKS

Forensic science is the study, investigation, and interpretation of facts, documents, and other pertinent evidence that can be utilized to piece together the details of historical occurrences or happenings and, ultimately, be lawfully employed for criminal prosecution [3].

[4] In situations involving cybercrime or fraud, such as security breaches or targeted attacks, computer forensics is applied to discover, extract, preserve, and describe digital content in a manner that can be utilized as evidence.

According to [5], digital forensics is a methodical way of finding, collecting, inspecting, and studying data while making sure it is correct and safe and keeping a strict record of who has the data.

It should be guaranteed that no digital evidence that is accessible is altered during a forensic inquiry without the proper authorization [6]. When concerns arise following an accident, a forensic investigation can help shed light on the situation.

[7] says that the goal of collecting forensically sound data is to find out where an intrusion or data transfer came from, what services and tools were used, and what security measures can't do. Usually, forensic data comes from two places: computer files, like logs and code, and network traffic that has been seen. When investigating SCADA and IACS systems, it is important to adhere to the five steps laid out by the European Union Agency for Network and Information Security (ENISA) [10–17].

- Looking through the system to find potential sources of evidence,
- Determining the impact components,
- Gathering raw data (in its original format),
- Analyzing the evidence, and
- Documenting.

They investigated computer forensics extensively in [18]. The writers start by talking about the different areas of computer forensics and the tools that are used in this field. After that, they use the properties of the forensic tools to do a comparison study.

Ultimately, they provide a concise overview of the present obstacles and forthcoming avenues of investigation in the field of computer forensics. [19] Have also done a study in the area of computer crime investigations.

Initially, the writers ascertained the primary subjects of digital forensics and discerned the key obstacles associated with them. Subsequently, they emphasized procedural concerns regarding preparedness, reporting, presentation, and ethical considerations. Furthermore, they emphasized the European viewpoint on privacy.

New developments in network forensics, as well as the various applications of expert systems, ML, DL, and ensemble/hybrid approaches, were discussed in this article [20]. Network traffic analysis, intrusion detection systems, cloud forensics, domain name system tunnels, smart grid forensics, and automobile forensics were some of the methods that were utilised. Blockchain, the IoT, and cloud computing were the subjects of a literature analysis on AI forensics in [21].

To maximise the performance advantages of distributed computing, it is crucial to employ distributed forensic methodologies, as highlighted in [22]. The team came up with the idea of a digital investigative tool that could centralise data while allowing users to access it from any device. If this were to happen, preparation could continue in the background even as multiple searches were underway.

In forensic analysis, new methods are required, as highlighted in [7], for example, specialised engines that employ parallel processing and adaptable, tailored evidence analysis. But they don't offer any concrete recommendations for satisfying this requirement. In order to establish connections and gather evidence, the investigation process weaves together the events that transpired. [23] proposed a different approach to finding and analysing breaches: using provenance instead of system calls. The provenance of corrupted files reveals the chain of events that led to their incursion.

Valli, who is 24 years old, created a structure for the Snort Intrusion Detection System (IDS) that creates forensically proven signatures. These signatures go after known weaknesses in SCADA and control systems that have been made public. This makes it easier for scientists to find and study exploits [25–32].

In the context of CI, [33] introduced an architecture that aims to enhance situational awareness, detect cyber intrusions promptly, and gather relevant forensic evidence to safeguard Smart Grids (SG). This requires the ability to visualise cybersecurity incidents, a forensic ready framework, a repository for forensic evidence, and methods to strengthen the reputation of certain assets. Also, the researchers suggested an Intrusion Detection System (IDS) with many variables that uses algorithms for outlier detection and access limitation [34]. Immediate detection of any discrepancies with respect to IEC-104 was their goal. Electrical engineers and power system automators must adhere to this standard while implementing SCADA systems.

Existing Auditing Strategies

By following a structured, objective, official, well-organised, and meticulously recorded method, a compliance audit can confirm that internal policies, external formal standards, and legal requirements have been met [35]. Certified specialists that serve as independent contractors do this work most of the time. Some examples of external elements that could impact how a company uses rules and criteria are laws, policies, processes, customer requests, and international regulations.

Compliance auditing operations serve to detect and evaluate risks as a means of mitigating threats. Additionally, they can aid in detecting security violations by analyzing security properties, such as misconfigurations, vulnerability exploits, and attacks/intrusions [35-38]. Some studies use formal reasoning tools, like XACML, to make sure that access policies are correct and to dynamically apply authorization by putting access controls outside of the application [39–41]. [42] Binary Decision Diagrams (BDD) and special methods were added to check access-control rules. [43] validated the policy using answer set programming (ASP) and expanded upon preexisting ASP thought models.

[44] and [45] Created a framework for policy research based on Satisfiability Modulo Theory. More research looked into how compliance tracking methods can be used to make the cloud safer. in the 45th Put in place a mechanism to automatically create security compliance solutions for cloud computing platforms. Their system is built to provide clock synchronisation, port security, and remote administration. Software agents were developed by Doelitzscher [46] to search for and inspect issues in Infrastructure as a Service (IaaS) clouds in an on-demand audit design. When asked about reviewing the network policies in Azure datacenters, Microsoft brought up SecGuru [47]. In a similar vein, IBM set up the QRadar [48] SIEM to collect and evaluate events in the cloud by means of a multitude of tracking technologies. According to Amazon, the best reporting tools are AWS CloudWatch and CloudTrail [49].

Customers can get logs and metrics info from these web APIs. Even with these business and academic attempts [50], there are still no standards for how to do compliance audits in the cloud.

Compliance auditing is closely connected to forensic procedures since forensic methods and techniques can frequently be utilized for evaluating compliance [51]. Data acquired during forensics operations is frequently the most useful source for compliance audits due to the thorough and time-stamped information it provides regarding inspected procedures. By establishing audit regulations and automatically implementing them on forensic data, it becomes feasible to carry out more comprehensive audits to identify probable instances of non-compliance. Auditing and compliance methods can make CI safer by making sure that laws, rules, regulations, and standards are followed. The big difference between the general rules and ideas in security standards and the detailed logs that modern systems make is a big problem for compliance auditing. SEM watches over networks, security devices, systems, and apps in real time and handles incidents related to security. SIM, on the other hand, manages logs, analyzes them, and sends compliance reports. SIEM technologies are mostly used for three main things: finding advanced threats, basic security tracking (which includes things like managing logs, reporting on compliance, and watching certain security controls in real time), and forensics and responding to incidents. Common elements of a SIEM system were covered in their study [52]. These components include source devices, processing and normalisation of logs, storage of logs, monitoring, rule engines, and correlation engines.

The study by [53] showed that modern SIEM systems don't have enough digital forensics and network forensics features. The study also found that many organizations did not have the ability to do safety audits. The poll also shows a lack of proficiency in the following areas:

(i) Add new event or data collectors or connections; and
(ii) Give data collection tools like web APIs or RESTful interfaces.

III. PROBLEM STATEMENT

Forensics and compliance auditing may not have the same ultimate goal, but they do have numerous similarities, such as using similar data sources and techniques to extract pertinent information and context for evidence gathering and analysis. Building these capabilities on top of a shared infrastructure that includes persistence capabilities, data collecting, transport, and processing pipelines is feasible because of these similarities. This study's primary finding lends credence to the idea that the FCA framework can be useful in bolstering such endeavours via a convergent strategy. Due to the increasing size and complexity of current distributed CIs that require protection, it is becoming more and more problematic to meet the increased demand for effective security data gathering and processing.

Horizontal scalability, elasticity, adaptability, resilience, and fault tolerance are all essential qualities in a security framework for continuous integration (CI).

Achieving varying degrees of granularity in the information presented to auditors and examiners is also imperative due to the concerns surrounding cognitive friction. Depending on the specific forensics or compliance audit tasks, there are situations where it is advisable to present only general information to avoid overwhelming the analyst. However, in other cases, it is essential to delve into highly detailed data, such as when identifying the underlying reasons for failures in complex scenarios. In some cases, optimizing storage resources may sacrifice granularity on behalf of later analysis, but in anybody, permanent retention of low-level data is necessary.

By examining FCA tasks in many contexts, we may find the best data sources to profile and monitor activities and processes. Forensics often need operational data from the ICT infrastructure to create user behaviour profiles.

All relevant evidence, such as historical data on service usage, network flows, and system-level logs detailing ongoing processes, service events, file modifications, and more, should be included. Compliance auditing, which involves regularly monitoring adherence to set standards and procedures, can also make use of the same data sources. This should come as no surprise. Standardised platforms are essential for the integration of financial crime research's numerous data sources. There is more to standardisation than just adopting similar formats; for example, data events can still be correctly sequenced in the timeline even when non-synchronized data sources (such clock skews) are properly regulated.

Identity and Access Management (IAM) is a vital cyber security discipline that revolves around how individuals access digital resources and what activities they can execute with those resources. The key Components of IAM are:

- Digital Resources: These encompass a wide range of applications and data within a computer system. Examples include web applications, APIs, platforms, devices, and databases.
- Identity and Identity Cube: At the core of IAM lies identity. When someone seeks access to a resource, they become a digital identity. This could be a customer, employee, member, or even a non-human entity like software or IoT devices. The entity which unites all the Information and its resources in one is called Identity Cube.
- Authentication: The process of authenticating a user's digital identity. Authentication assures that the user is who they claim to be.
- Authorization: Determines what resources a user can access. Unlike authentication, which confirms identification, authorization provides or limits access to specified resources depending on that identity.

Identity and Access Management (IAM) is a vital cyber security discipline that revolves around how individuals access digital resources and what activities they can execute with those resources. The key Components of IAM are:

- Digital Resources: These comprise a wide range of applications and data within a computer system. Examples include online apps, APIs, platforms, devices, and databases.
- Identity and Identity Cube: At the basis of IAM resides identity. When someone requests access to a resource, they become a digital identity. This could be a customer, employee, member, or even a non-human entity like software or IoT devices. The entity which unites all the Information and its resources in one is called Identity Cube.
- Authentication: The procedure of validating a user's digital identity. Authentication verifies the user's claimed identity.
- Authorization: Specifies the resources accessible to a user. Authentication verifies identification, whereas authorization allocates or restricts access to particular resources depending on that identity.

Practical Illustrations

- Data Breach Mitigation: A major financial institution utilizes IAM to impose rigorous authentication and access restrictions, preventing unauthorized access to critical financial data and lowering the risk of data breaches.

- Healthcare organizations utilize IAM to adhere to regulations such as HIPAA by restricting access to patient records to authorized personnel, thereby safeguarding sensitive health information.
- Security of Remote Work: IAM solutions make it possible to access company resources securely from any location as remote work becomes more popular. Multi-factor authentication and ongoing surveillance guarantee the security of remote access.

Societal and Global benefits:

Cyber security and Critical Infrastructure Protection (CIP) plays a significant role as it helps to carry out the various challenges in various domain such as, healthcare, public safety, etc. As public safety is concerned, it takes up the responsibility of required components required for the various sectors related to system and networks, which are threat as cyber sector. Safety makes to ensure to perform the operations repeatedly or continuously and makes data resilience while the cyber-attacks are performed, and those attacks make critical problems to the society. To eradicate / mitigate the challenges, collaborative approach is applied among the private, government organization and international organizations as it brings to identify the threat vulnerabilities and make to improve the data robustness based on the various security metrics and response measures among various sectors in coordinative manner.

To create and identify the relationship on global challenges based on CIP and cybersecurity. Today's goal is to ensure sufficient trustworthiness of systems, products, and services, as well as the resilience required to support the economy and security interests. Nations must acknowledge the significance of safeguarding critical infrastructures from natural disasters, terrorist actions, and emerging cyber threats. The CIP enhances all critical infrastructure sectors to optimal standards, facilitating disaster preparedness, response, and recovery efforts. U.S. is known as the world's richest country, but its infrastructure safety ranks 13th in the world, according to a White House fact sheet1. In general, each country identified its most important infrastructure areas. However, the four most important ones were identified as transportation, water, energy, and communication. Disruption or loss in any of these sectors will directly impact the security and resilience of multiple sectors, resulting in significant harm and catastrophic consequences.

The five key elements of UNSC resolution 2341, shown in Figure 10, are

- Awareness, which strengthens and reinforces knowledge and recognizes critical infrastructure threat and threats,
- Abilities, which assess states' serves and private-public partnerships to reduce cyberattack risk,
- Resilience, which promotes preparation.

The UNSC acknowledged the susceptibility of key infrastructures to cyberattacks by terrorists and the existence of three essential infrastructure sectors:

- Energy,
- Healthcare, and
- Public Safety

UNSC resolution 2341 said that terrorist attacks are a unique threat to critical infrastructures and urged all states to work together to make people more aware of the threat, learn more about it, and understand it better so that everyone can be better prepared. It is also acknowledged that there are several different types of risks to vital infrastructures. The purpose of hard targets is to make it more difficult for terrorists to attack, in contrast to soft targets, which are areas or locations that are more susceptible to assaults because of their lack of security and unfettered access. Such risks posed by these targets are categorized according to their type, place of origin, and circumstances. The UK's National Security Strategy acknowledged that the country's Critical National Infrastructures (CNI), which include those related to energy, water, transportation, health, and telecommunication, are vital to the country's ability to function. The UK National Cyber Security Centre (NCSC) created the NCSC CAF collection, a set of fourteen cybersecurity and resilience principles for defending critical infrastructure sectors. NCSC CAF collection accepted the EU Security of Networks & Information networks (NIS) Directive to improve cybersecurity and resilience of critical EU networks. Any organizations that are a part of the UK Critical National Infrastructures (CNI) or in charge of providing services to CNI sectors are welcome to use the CAF collection.

For necessities like clean water, electricity, transportation, and communications, the United States depends on dependable key infrastructures. Critical infrastructures were characterized as a collection of assets, systems, operational technologies, and other essential components in both the physical and cyber environments by the Patriot Act of 2001 [7]. As protecting the United States' critical infrastructure became a top concern for the country, Executive Order 13,636 [8] was made to work on making critical infrastructure safer. It guides U.S. policy "to maintain a cyber environment that promotes efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties, and to enhance the security and resilience of the Nation's critical infrastructures." [8]. In the United States, the private sector, federal, state, or regional governments own and operate essential physical and cyber infrastructure. Following Executive Order 13,636, the Cybersecurity Increase Act 2014 (CEA) [9] was authorized through the National Institute of Standards and Technology (NIST) to facilitate and develop a framework for reducing risk to critical infrastructures by

- Collaboration of public-private on cybersecurity.
- Cybersecurity Research and Development.
- Education and Workforce Development.
- Cybersecurity Awareness and Preparedness; and
- Advancement of Cybersecurity.

"A prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructures to help them identify, assess, and manage cyber risks" is what the framework promises to identify.

Overcoming Obstacles with CIP:

- Risk Assessment and Vulnerability Management: Consistently detecting any weaknesses in critical infrastructure systems and setting mitigation priorities to successfully resolve them.
- Network segmentation separates operational technology (OT) and information technology (IT) networks to prevent cyber threats.
- Implement strong authentication methods for essential systems to prevent unwanted access.
- Creating thorough preparations for identifying, containing, and recovering from cyber disasters is known as incident response planning.
- Information Exchange and Cooperation: Encouraging cooperation between government organizations, operators of vital infrastructure, and cybersecurity specialists in order to exchange threat intelligence and best practices.

IV. PROPOSED IAM BASED AUDIT FRAMEWORK

Here, we introduce the suggested FCA framework. Section 3.1 provides an overview of the reference architecture. Now we will take a close look at each important part of the system:

- Collecting Information
- Domain Processor,
- Cyber-physical Intrusion Detection Systems,
- Data Lake,
- Continuous Integration Business Rules,
- Monitoring, Data Visualisation,
- Analytics,
- Players/Roles,
- Orchestration, and
- Trust/Reputation Indicators.

The proposed platform's structure is shown in Figure 1. By incorporating capabilities for forensic investigation and audit compliance, this architecture effectively functions as a specialised flight recorder that augments conventional security systems.

This software facilitates forensic investigations by enabling the identification, extraction, preservation, and highlighting of digital evidence. When it comes to compliance audits, it makes it possible to evaluate adherence to policies, corporate regulations, and standards. To help FCAs become more proficient, the platform compiles data from several sources and makes it easier to understand, especially when it comes to digital evidence extraction.

- Collecting Information
- Domain Processor,
- Cyber-physical Intrusion Detection Systems,
- Data Lake,
- Continuous Integration Business Rules,
- Monitoring, Data Visualisation,
- Analytics,
- Players/Roles,
- Orchestration, and
- Trust/Reputation Indicators.

The same kinds of data are used for auditing compliance and fraud detection in AAA sessions, network traces, service and device logs, physical access control systems, and physical process logs. For a fuller view, the system can process massive volumes of data, both organised and unstructured, from internal and external sources.

An organized correlation of collected data is utilized by the Analytics component to spot outliers and cases of non-compliance. These results will be useful for highlighting important facts and improving the process of identifying security issues after the fact so that evidence can be extracted.

Continuous auditing against preset policies helps discover and prevent potential vulnerabilities.

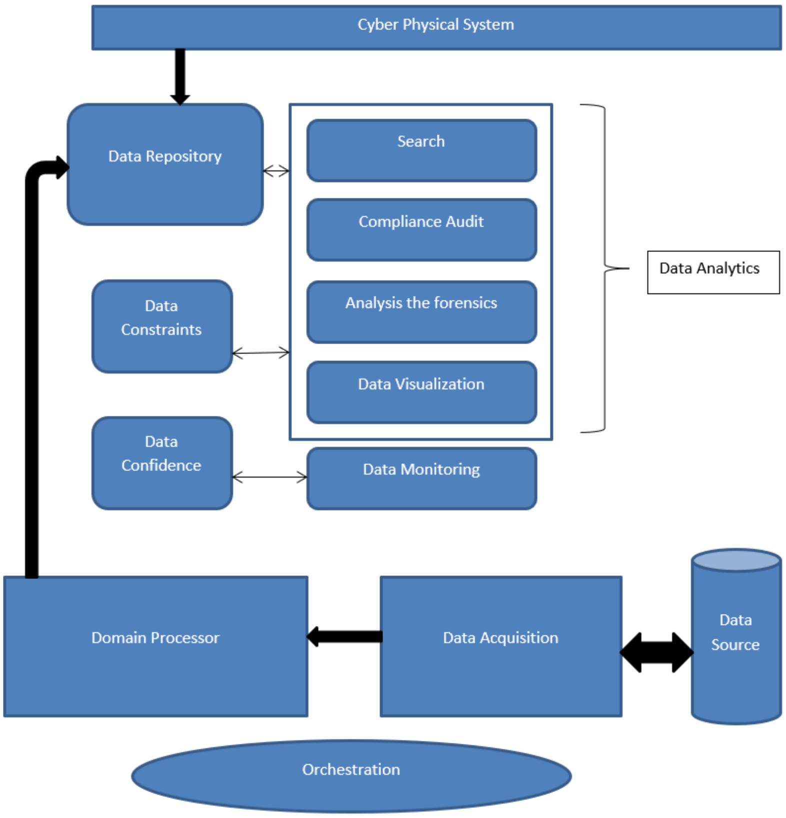

Figure 1. IAM-Based Audit Framework Architecture: This diagram illustrates the interaction between the framework's components, including Data Acquisition, Domain Processor, and Data Analytics. The framework integrates forensic investigation and compliance auditing to enhance Critical Infrastructure Protection (CIP).

In the proposed IAM-Based Audit Framework, there are 3 main components as mentioned below,

1. Data Source:

- Role: Originates raw data streams, including logs and telemetry.

- Text Addition: "The framework begins by acquiring data from diverse sources such as sensor logs, network traces, and physical device outputs."

2. Data Acquisition:

- Role: Collects, validates, and normalizes input data.

- Text Addition: "Data Acquisition integrates and normalizes input from various CI components, forming the foundation for subsequent analysis."

3. Domain Processor:

- Role: Processes ingested data using filtering and enrichment techniques.

- Text Addition: "The Domain Processor refines the ingested data, extracting meaningful insights to support compliance and forensic tasks."

From the domain processor, it is stored in the data repository as the data analytics operations are performed as it makes data search, auditing the data through compliance, data forensics is performed based on the data analysis and visualization is done based on bar, line, graph plots. These visualizations are made with the analysis based on the set of rules and constraints through data. The above activities are performed and monitored as it results in data confidence and data's are related to the cyber physical system.

Algorithm 1: Data Acquisition:

Input: Large Data

Output: System Performance

```
Integrating the data source
Managing the data from various sources through DMA
Event → Set of independent feature attributes
Event Creation 'E(i)'
    E(i) = {Set of tuples} i=1 to n
Parsing Function P(i) as P(i): E(i)
    Processing the Event E(i) based on,
        Parsed 'P'
        Validation 'V'
        Normalization 'N'
System Performance:
    Received Data rate (RDr)
    Output Rate
        Ingested (In)
        Consumed rates (Cr)
```

Algorithm 2: Domain Processor

Input: Ingested Event

Output: Data Event

```
Optimize the load distribution based on distributed environment
Processing Function P={Aggregate (A); Filtering (F); Enrich (E); Indexing (I)}
        P: Input Event I($E_1$)
        F: Event Domain {0,1}
        R: Combine{Positive and Negative}
        'S' Subset Attributes
```

7. Disjunction Level
8. Negating the disjunction level
9. F: {Define the Event filter (or) Event blocked}
10. I: Ingested Event Improvement
11. E: Attribute to the normalized event
12. A: Set of grouping attributes
13. Number of events created per second

V. PERFORMANCE ANALYSIS

Within this part, we will assess and deliberate on the IAM based Audit Framework framework. The suggested IAM based Audit Framework framework is designed to be neutral concerning the use of analytics algorithms. Indeed, each unique deployment scenario will likely require distinct algorithms. Therefore, this assessment prioritizes performance over accuracy. But in the field of Formal Concept Analysis (FCA), we have already assessed the accuracy of various ML techniques, and K-means with XGBoost [63] are two examples.

Table 1: Max Ingestion Vs. Number of Nodes

Nodes	10 Primary Shades/1 replica	5 Primary Shades/3 replica	5 Primary Shades/2 replica	5 Primary Shades/1 replica
3	0.30	0.21	0.24	0.32
4	0.48	0.53	0.57	0.59
5	1.41	1.45	1.48	1.52
6	1.31	1.35	1.38	1.40
7	1.23	1.26	1.28	1.32
8	1.18	1.21	1.23	1.26
9	1.09	1.13	1.16	1.19
10	0.97	0.99	1.03	1.06

Table 2: Max Computation Time Vs. Number of Nodes

Nodes	10 Primary Shades/1 replica	5 Primary Shades/3 replica	5 Primary Shades/2 replica	5 Primary Shades/1 replica
3	110	96	84	78
4	71	62	55	48
5	68	52	45	38
6	56	45	36	28
7	48	31	24	19
8	46	37	21	17
9	37	26	15	13
10	36	23	11	09

Table 3: Min Computation Time Vs. Number of Nodes

Nodes	10 Primary Shades/1 replica	5 Primary Shades/3 replica	5 Primary Shades/2 replica	5 Primary Shades/1 replica
3	10.25	8.65	6.85	4.56
4	16.74	14.23	12.58	8.95
5	17.96	15.25	13.56	9.15
6	18.25	16.95	14.85	11.5
7	20.15	18.45	16.25	14.5
8	16.37	14.74	12.96	10.9
9	15.65	13.45	11.25	9.7
10	14.85	12.65	10.96	8.9

Table 4: Average Computation Time Vs. Number of Nodes

Nodes	10 Primary Shades/1 replica	5 Primary Shades/3 replica	5 Primary Shades/2 replica	5 Primary Shades/1 replica
3	50.6	45.3	33.2	34.5
4	150.0	39.5	38.2	28.5
5	210.2	19.5	39.6	24.6
6	265.0	17.6	41.6	22.1
7	310.5	14.5	28.5	19.6
8	320.6	12.6	35.6	17.3
9	345.2	10.9	26.9	15.8
10	365.2	8.50	23.6	11.6

Based on the primary shard/replica configurations and cluster size, Table 1 shows the maximum ingestion time (in milliseconds) for 10 clients. I should note that in this specific experiment, the minimum, average, and maximum timings were not significantly different from one another.

The computation times for each arrangement are displayed in Tables 2, 3, and 4, together with their maximum and minimum values. In other instances, there were more noticeable variations than in the previous experiment; this was especially true when working with primary shards and replicas that maintained a low minimum computation time over a range of cluster sizes.

Use case Study of IAM with Amazon EC2:

A web service called AWS Identity and Access Management (IAM) is used to safely manage who can access AWS resources. It lets you design and manage services for user authentication or restrict access to your AWS resources to a specific group of users. An entity that can act on an AWS resource is called a principal. Principals can be users, roles, or applications. Verifying the identity of the principal attempting to access an AWS product is known as authentication. The principal must supply its credentials or needed keys for authentication.

- Request: The action and the resource that should carry it out are specified in a request sent by a principal to AWS.
- Authorization: All resources are blocked by default. Only when all the request's components are permitted by a matching policy does IAM approve it. AWS authorizes the activity after authenticating and authorizing the request. Resource creation, editing, deletion, and viewing are accomplished using actions.
- Resources: A collection of steps that can be carried out on an AWS account-related resource. Access to AWS resources is managed and permissions are specified by an IAM policy.

AWS stores policies as JSON documents. Permissions define the resources' users and the actions they are permitted to take. A policy might, for instance, let an IAM user to access one of the Amazon S3 buckets.

Information like this would be included in the policy:

- Who has access to it?
- What the user can do?
- Which AWS resources are available to users?
- When are they available?

A. Initial Setup Configuration:

1. Create an AWS account and set up AWS IAM Identity Centre to create administrative accounts for AWS resources.
2. When you set up account access for the administrative user, IAM Identity Centre creates a matching IAM role.
3. The policies defined in the Administrator Access permission set are associated to this role, which is generated in the applicable AWS account and administered by IAM Identity Centre.

As administrators, Nikki and Mateo no longer need their root user to access their AWS account. They will only use the root user for root-only tasks. Based on security best practices, they configure Multi-Factor Authentication (MFA) for root user credentials and decide how to protect them. Their company hires developers, admins, testers, managers, and system administrators as it grows. Nikki runs operations, while Mateo leads engineering. An Active Directory Domain Server manages employee accounts and internal company resources.

To give employees access to AWS resources, they use IAM Identity Centre to connect their Active Directory to AWS. Since they linked Active Directory to IAM Identity Centre, all of the users, groups, and group memberships are defined and synchronized. To give users the right AWS resource access, they must assign permission sets and roles to groups. They construct permission sets using AWS managed policies for job functions in the AWS Management Console:

- Administrato0072
- Billing
- Developers
- Administrators of networks
- The database administrators
- System administrators

They then apply these permissions settings to Active Directory group roles.

B. Permissions for the user groups using Amazon EC2:

Nikki adds a policy to the AllUsers user group in order to enable "perimeter" management. Any AWS request from a user that originates from an IP address outside of Example Corp's corporate network is rejected by this policy. At Example Corp, different IAM groups need different permissions:

1. To create and manage AMIs, instances, snapshots, volumes, security groups, and other items, system administrators must have authorization.
2. By attaching the AmazonEC2FullAccess AWS managed policy to the SysAdmins user group, Nikki grants group members access to all Amazon EC2 actions.

3. Developers: You must be able to work with instances only. For this reason, Mateo makes a policy and adds it to the Developers user group, enabling developers to call Describe Instances, Run Instances, Stop Instances, Start Instances, and Terminate Instances.

To manage who has access to the operating system of Amazon EC2 instances, Amazon EC2 employs security groups, Windows passwords, and SSH keys. Access to the operating system of a particular instance cannot be granted or denied using the IAM system. Support users should not be able to perform any Amazon EC2 actions other than listing the resources that are currently available. In order to restrict the Support users group's ability to call Amazon EC2 "Describe" API operations, Nikki drafts and adds a policy to the group.

C. Changes in the user's job function

One of the developers, Paulo Santos, eventually transitions into a managerial role. Paulo joins the Support users network as a manager in order to open support issues for his developers. Paulo is transferred by Mateo from the Developers user group to the Support users group. This change limits his ability to communicate with Amazon EC2 instances. He is unable to start instances. Additionally, he is unable to stop or end instances that have already started, even if he was the one who initiated them. He can only display the instances that Example Corp users have launched.

D. Practical application of IAM in conjunction with Amazon S3

Additionally, organizations such as Example Corp would frequently implement IAM in conjunction with Amazon S3. John has made an Amazon S3 bucket named amzn-s3-demo-bucket for the business establishing additional users and user groups. Both Zhang Wei and Mary Major must be allowed to generate their own data in the business bucket as workers.

- Additionally, they must read and write shared data that is used by all developers. To do this, Mateo uses an Amazon S3 key prefix system to logically organize amzn-s3-demo-bucket data.
- The address is /amzn-s3-demo-bucket /home /zhang /major /share /developers /managers.
- Mateo divides the /amzn-s3-demo-bucket into personal folders for each employee, as well as a shared space for development and manager groups.
- At this point, Mateo develops a set of rules to provide users and user groups permission:
- Mateo attaches a policy to Wei that grants him permission to read, write, and list any items that have the Amazon S3 key prefix /amzn-s3-demo-bucket/home/zhang/. This policy grants Zhang access to the home directory.
- Mateo attaches a policy to Mary that allows her to read, write, and list any objects with the Amazon S3 key prefix /amzn-s3-demo-bucket/home/major.
- The developer's user group has shared directory access. Mateo adds a policy to the user group that permits developers to list, access, and edit everything in /amzn-s3-demo-bucket/share/developers/.
- Managers' user group has shared directory access; Mateo adds a policy to the group that permits managers to list, read, and write objects in /amzn-s3-demo-bucket/managements/

A user who creates a bucket or object on Amazon S3 may not have authority to conduct additional operations on it. IAM policies must clearly allow users to use the Amazon S3 resources they make. Examples of these policies can be found in the Amazon Simple Storage Service User Guide under the heading "Access Control." See Policy evaluation logic for details on how policies are assessed at runtime.

The AWS Solution Architect Certification goes thoroughly into the critical components of AWS Identity and Access Management (IAM), a vital service for managing security in AWS environments. This certification highlights how crucial it is to comprehend IAM's extensive features for safely managing access to AWS resources and services.

VI. CONCLUSION

An AM-based audit framework is offered as it integrates capabilities for forensic investigation and audit compliance with effective architectural functions and security mechanisms.

The framework incorporates algorithms such as data acquisition and domain processors. The data acquisition algorithm processes a substantial dataset, comprising organized data for cloud identity and access management systems, including AWS, Azure, and Google Cloud datasets. It employs the DMA process to evaluate system performance metrics such as perceived data rate, ingested rate, and consumed rate. The identified ingested event serves as the input for the domain processor to compute the data event. The proposed framework in the performance analysis facilitates the generation of the maximum ingestion event, maximum computational time, and minimum computational time, contingent upon the number of nodes/clients ranging from 3 to 10.

This project's goal is to lay the foundation for better solutions that will meet FCA's present and future demands. This framework specifies function blocks, functions, as well as internal, input, and output communications to enable IACS security, hence combining FCA capabilities. This platform handles vast volumes of heterogeneous data in real-time by utilizing distributed computing resources. We examined whether the system's essential elements could grow, especially to handle the volume and speed of data. According to the experimental evaluation, the suggested architecture can manage FCA requirements at scale. To evaluate a cluster's performance under different ingestion and compute demand situations, it involved several trials. Additionally, this empirical evaluation showed how useful the proposed framework is for recognizing typical assault sequences.

REFERENCES

[1] J. Henriques, F. Caldeira, T. Cruz and P. Simões, 'A forensics and compliance auditing framework for critical infrastructure protection,' International Journal of Critical Infrastructure Protection, Vol. 42, Sept. 2023. Doi.org/10.1016/j.ijcip.2023.100613.

[2] S. M. Ali, A. Razzaque, M. Yousaf and R.U. Shan, 'An Automated Compliance Framework for Critical Infrastructure Security Through Artificial Intelligence,' IEEE Access, Vol 13, pp. 4436 – 4459, Dec. 2024. Doi: 10.1109/ACCESS.2024.3524496.

[3] J. Henriques, F. Caldeira, T. Cruz and P. Simões, 'A Survey on Forensics and Compliance Auditing for Critical Infrastructure Protection,' IEEE Access, Vol. 12, pp. 2409-2444, Jan. 2024. Doi: 10.1109/ACCESS.2023.3348552.

[4] A.S. George, T. Baskar and P.B. Srikaanth, 'Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors, Partners Universal International Innovation Journal, Vol. 2, No. 1, pp. 51-75, Jan – Feb. 2024. Doi: 10.5281/zenodo.10639463

[5] N. Chowdhury and V. Gkioulos, 'Key competencies for critical infrastructure cyber-security: a systematic literature review,' Information and Computer Security, Vol. 29, Issue. 5, Nov. 2021. Doi: 10.1108/ICS-07-2020-0121

[6] M.J. Haber, B. Chappell and C, Hills, Regulatory Compliance,' Cloud Attack Vectors. Apress, Berkeley, CA. July 2022. Doi: 10.1007/978-1-4842-8236-6_8

[7] E. Calandro, 'Observing Global Cyber Norms Nationally - The Case of Critical Infrastructure Protection in South Africa,' SSRN, Dec. 2020, Doi: 10.2139/ssrn.3895156

[8] M. Papamichael, C. Dimopoulos and G. Boustras, 'Performing risk assessment for critical infrastructure protection: an investigation of transnational challenges and human decision-making considerations,' Sustainable and Resilient Infrastructure, Vol. 9, Issue. 4, pp. 367-385, Apr. 2024. Doi: 10.1080/23789689.2024.2340368.

[9] O. Eltayeb, 'The Crucial Significance of Governance, Risk and Compliance in Identity and Access Management,' Transnational Press London, Issue. 3, pp. 2395-2405, 2024.

[10] H. A., Hussein, and Z. Razzaq, 'CFRP Retrofitting Schemes for Prestressed Concrete Box Beamsfor Highway Bridges,' Global Journal of Research In Engineering, Vol. 17, Issue. 1, Jan. 2017.

[11] H. A. Hussein, and Z. Razzaq, 'Prestressed Concrete Inverted Tee Beams with CFRP for Building Structures,' Global Journal of Research In Engineering, Vol. 17, Issue. 3, July 2017.

[12] H. A. Hussein, 'Effective CFRP Retrofitting Schemes for Prestressed Concrete Beams,' Doctoral dissertation, Old Dominion University, Dec. 2014, Doi: 10.13140/RG.2.2.33231.25764.

[13] Hussein, H. A. (2022). Effectiveness of Suspended Lead Dampers in Steel Buildings Under Localized Lateral Impact and Vertical Pulsating Load (Doctoral dissertation, Old Dominion University, Dec. 2014.

[14] H. A. Hussein, and Z. Razzaq, 'Strengthening Prestressed Concrete Bridge Girders and Building Beams with Carbon Fiber Reinforced Polymer Sheets,' European Journal of Engineering and Technology Research, Vol. 6, Issue. 1, pp. 55-57, Jan. 2021.

[15] A. Nazarian, R. Velayati, P. Foroudi, D. Edirisinghe, and P. Atkinson, 'Organizational justice in the hotel industry: revisiting GLOBE from a national culture perspective,' International Journal of Contemporary Hospitality Management, Vol. 33, Issue. 12, pp. 4418-4438, Nov. 2021

[16] G.-J. Ahn, H. Hu, J. Lee, Y. Meng, 'Representing and reasoning about web access control policies,' IEEE 34th Annual Computer Software and Applications Conference, IEEE, pp. 137–146, July 2010.

[17] K. Arkoudas, R. Chadha, J. Chiang, 'Sophisticated access control via SMT and logical frameworks,' ACM Trans. Inf. Syst. Security. Vol. 16, Issue. 4, pp. 1–31, 2014.

[18] K.W. Ullah, A.S. Ahmed, J. Ylitalo, 'Towards building an automated security compliance tool for the cloud,' 2th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1587–1593, July 2013.

[19] F. Doelitzscher, Security Audit Compliance for Cloud Computing, Ph.D. thesis, Plymouth University, 2014, Doi: 10.24382/3874.

[20] N. Bjørner, K. Jayaraman, 'Checking cloud contracts in Microsoft azure,' International Conference on Distributed Computing and Internet Technology,' Springer, Vol. 8956, pp. 21–32, 2015.

[21] S. Majumdar, T. Madi, Y. Wang, Y. Jarraya, M. Pourzandi, L. Wang, M. Debbabi, 'Security compliance auditing of identity and access management in the cloud Application to OpenStack,' IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 58–65, Dec. 2015.

[22] K. Kumar, and M. Zolkipli, 'A Review on Identity and Access Management (IAM) for Digital Environment Security,' Borneo International Journal EISSN, Vol. 7, Issue. 4, pp. 43-48, 2024. https://majmuah.com/journal/index.php/bij/article/view/666.

[23] L. D. Khare, 'Security and Integration in Business Intelligence Tools: A Comprehensive Study,' The University of Western Ontario (Canada) ProQuest Dissertations & Theses, 2024.

[24] M.T.H. Sarker and M.S. Rahman, 'Artificial Intelligence Enhanced Identity And Access Management Preventing Unauthorized Access In Modern Enterprises,' Vol. 1, Issue. 4, pp. 80-95, 2024. Doi: 10.62304/ijmisds.v1i04.202.

[25] G S. Nagaraj and Shankaramma, 'Framework Analysis and Zero Trust Security Issues in Contemporary Network Systems,' 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS), Nov. 2024, DOI: 10.1109/CSITSS64042.2024.10816783

[26] C. Singh, R. Thakkar and J. Warraich, 'IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations,' European Journal of Engineering and Technology Research, Vol. 8, No. 4, Aug. 2023. DOI: 10.24018/ejeng.2023.8.4.3074.

[27] M. Gordan, D.A. Kountche, D. McCrum, S.Schauer, S. König, S. Delannoy, L. Connolly, M. Iacob, N.G. Durante, Y. Shekhawat, C. Carrasco, T. Katsoulakos and P. Carroll, 'Protecting critical infrastructure against cascading effects: The PRECINCT approach,' Resilient Cities and Structures, Vol. 13, Issue.3, pp. 1-19, Sept. 2024. DOI: 10.1016/j.rcns.2024.04.001

[28] M. G. Cains, L. Flora, D. Taber, Z. King and D.S. Henshel, 'Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation,' Risk Analysis, Vol. 42, Issue. 8, pp. 1643-1669, Feb. 2021, DOI: 10.1111/risa.13687.

[29] H. Riggs, S. Tufail, I. Parvez, M. Tariq, M.A. Khan, A. Amir, K. V. Vuda and A. I. Sarwat, 'Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure,' Sensors, MDPI, Vol. 23, Issue, 8, April 2023, DOI: 10.3390/s23084060.

[30] H.E. Amin, A.E. Samhat, M. Chamoun, L. Oueidat, and A. Feghali, 'An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure,' Journal of Cyber Security Privacy, MDPI, Vol. 4, Issue. 2, pp. 357-381, June 2024. DOI: 10.3390/jcp4020018.

[31] H. Taherdoost, 'Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview,' Electronics, MDPI, Vol.11, Issue. 14, July 2022, DOI: 10.3390/electronics11142181.

[32] A. Devipriya; R. Anto Arockia Rosaline; M. R. Prabhu; P. Nancy; V. Karthick; V. Kadumbadi, 'Algorithmic Approaches to Securing Cloud Environments in the Realm of Cybersecurity,' 10th International Conference on Communication and Signal Processing (ICCSP), Apr. 2014, DOI: 10.1109/ICCSP60870.2024.10543914.

[33] IEC, IEC 62443 - IEC technical specification - industrial communication networks - network and system security - Part 1-1: Terminology, concepts and models, 2017, https://webstore.iec.ch/preview/info_iec62443-1-17Bed1.07Den.pdf.

[34] J. Henriques, F. Caldeira, T. Cruz, P. Simes, 'Combining K-means and xgboost models for anomaly detection using log datasets,' Electronics, MDPI, Vol. 9, Issue. 7, July 2020. http://dx.doi.org/10.3390/electronics9071164.

[35] J. Henriques, F. Caldeira, T. Cruz, P. Simes, 'An automated closed-loop framework to enforce security policies from anomaly detection,' Computer. Security. Vol. 123, pp. 102949, Dec. 2022, Doi: 10.1016/j.cose.2022.

[36] F. Caldeira, S. T., M.E. Varrette S., S. P., B. K. D., 'Trust based interdependency weighting for on-line risk monitoring in interdependent critical infrastructures,' International Journal of Secure Software Engineering,' Vol. 4, Issue. 4, pp. 40-46, Sept. 2011, DOI: 10.1109/CRiSIS.2011.6061545.

[37] L. Rosa, T. Cruz, M.B. de Freitas, P. Quitério, J. Henriques, F. Caldeira, E. Monteiro, P. Simões, 'Intrusion and anomaly detection for the next generation of industrial automation and control systems,' Future Gener. Comput. Syst. Vol. 119, pp. 50–67, June. 2021. DOI: 10.1016/j.future.2021.01.033.

[38] L. Rosa, M.B. de Freitas, J. Henriques, P. Quitério, F. Caldeira, T. Cruz, P. Simões, Evolving the security paradigm for industrial IoT environments, in: Cyber Security of Industrial Control Systems in the Future Internet Environment, IGI Global, pp. 69–90, 2020. DOI: 10.4018/978-1-7998-2910-2.ch004.

[39] B.N. Levine, M. Liberatore, DEX: 'Digital evidence provenance supporting reproducibility and comparison,' Digit. Investigation, Vol. 6, pp. S48 – S56, 2009, http://dx.doi.org/10.1016/j.diin.2009.06.011.

[40] E. Casey, G. Back, S. Barnum, 'Leveraging cybox™ to standardize representation and exchange of digital forensic information,' Digit. Investig. Vol. 12 pp. S, 02–S110, 2015. DOI: 10.1016/j.diin.2015.01.014

[41] A. Aminnezhad, A. Dehghantanha, M.T. Abdullah, 'A survey on privacy issues in digital forensics,' Int. J. Cyber-Secur. Digit. Forensics, Vol. 1, Issue. 4, pp. 311–324, 2012.

[42] R. Verma, J. Govindaraj, G. Gupta, 'Data privacy perceptions about digital forensic investigations in india,' International Conference on Digital Forensics, Springer, pp. 25–45, 2016. DOI: 10.1007/978-3-319-46279-0_2.

[43] P.R. Grammatikis, P. Sarigiannidis, E. Iturbe, E. Rios, A. Sarigiannidis, O. Nikolis, D. Ioannidis, V. Machamint, M. Tzifas, A. Giannakoulias, 'Secure and private smart grid: The spear architecture,' 6th IEEE Conference on Network Softwarization (NetSoft), IEEE, pp. 450–456, 2020. DOI: 10.1109/NetSoft48620.2020.9165420

[44] P.R. Grammatikis, P. Sarigiannidis, A. Sarigiannidis, D. Margounakis, A. Tsiakalos, G. Efstathopoulos, 'An anomaly detection mechanism for IEC 60870-5-104,' 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), IEEE, pp. 1–4, 2020. DOI: 10.1109/MOCAST49295.2020.9200285.

[45] ISO/IEC, ISO/IEC 27002:2022 – 'Information security, cybersecurity and privacy protection,' Information security controls, 2022, https://www.iso.org/standard/75652.html.

[46] P. Mell, T. Grance, 'NIST definition of cloud computing (NIST SP 800-145),' 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[47] ISO/IEC, ISO/IEC 27019:2017. 'Information technology—Security techniques— Information security controls for the energy utility industry,' 2017, https://www.iso.org/standard/68091.html

[48] ISA SECURE, Establishment of isasecure Japanese scheme and publication of isasecure embedded device security assurance certification program specifications in Japan, 2013, http://www.isasecure.org/en-US/News-Events/Establishment-of-ISASecure-Japanese-Scheme-and-Pub.

[49] S. Majumdar, T. Madi, Y. Wang, Y. Jarraya, M, Pourzandi and L. Wang, 'Security Compliance Auditing of Identity and Access Management in the Cloud: Application to OpenStack,' IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), Dec. 2015, DOI: 10.1109/CloudCom.2015.80.

[50] J. Henriques, F. Caldeira,T. Cruz and P. Simões, 'Combining K-Means and XGBoost Models for Anomaly Detection Using Log Datasets,' Electronics, MDPI, Vol. 9, Issue. 7, 2020. Doi: 10.3390/electronics9071164.

[51] K. Kent, S. Chevalier, T. Grance and H. Dang, 'Guide to Integrating Forensic Techniques into Incident Response,' Information Technology Laboratory, Computer Security Resource Center, NIST, Aug. 2006.