IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 3, 2020, accepted October 7, 2020, date of publication October 20, 2020, date of current version October 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3032436

Context-Aware Autonomous Security Assertion for Industrial IoT

USMAN TARIQ[1], AHMAD O. ASEERI[2], (Member, IEEE), MOHAMMED SAEED ALKATHEIRI[3], AND YU ZHUANG[4]

[1]Department of Information Systems, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[2]Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[3]College of Computer Science and Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia
[4]Department of Computer Science, Texas Tech University, Lubbock, TX 79409, USA

Corresponding author: Usman Tariq (u.tariq@psau.edu.sa)

This work was supported by the Deputyship for Research and Innovation, Ministry of Education, Saudi Arabia under Project 383.

ABSTRACT The Industrial Internet of Things (IIoT) platform consists of purpose-driven communication controllers, enterprise-grade modems (routers and gateways), and edge computing systems that require integrated software and sensing capability in mission-critical environments. Extensible purpose-built industrial supervisory control and data acquisition networks are prone to numerous cybersecurity threats. In this paper, the historical databased qualitative threat assessment was part of the comprehensive risk breakdown (i.e., to quantify assessment and remediation) of the practicing industry (i.e., systems that rely on robotics, big data & analytics). Furthermore, a risk and operability (HAZOP & convolution neural-network) evaluation was proved to be the paramount study for autonomous vulnerability assessment. Through autonomous network management, continuous software monitoring, data-driven device insights, and integrated content filtering, the proposed endpoint protection scheme shows significant improvement in preventing data breaches, denial of service (DoS), and malware detection. A distinctive computational methodology to determine the cyber risk for industrial structures with IoT-explicit control factors has been programmed and elucidated in the perspective of IIoT systems. Firmware driven emulation (integrated and optimized) outcome aided to reduce breach ratio, better incident detection, and enhanced protection of confidential data.

INDEX TERMS Industrial Internet of Things, HAZOP analysis, hybrid integrity model, multicriteria decision analysis, convolution neural-network.

I. INTRODUCTION

Mission-critical industrial IoT (IIoT) has become increasingly a leading system paradigm in the IIoT realm whose failure can result in significant economic and operational costs. It is simply a network of intelligent devices that are pre-designed and pre-configured with a target to perform automated, repeatable, scalable, real-time, and reliable tasks by benefiting from sensed data collection and dissemination protocols, such as CoAP, MQTT, Mihini/M3DA & HTTP. Goal-oriented quantifiable critical insight (related to gateway management, communications (RFID, Wi-Fi or a mobile network), device scalability, and regulatory compliance) generated by the IIoT platform can increase enterprise operational efficiency. However, the current state-of-the-art IIoT solutions, which have generally emerged from the traditional wireless sensor network architecture, fall short in providing imperative requirements for mission-critical IIoT applications, imposing a different level of challenges on underlying communication infrastructures. System implementation using agile modus in IIoT guarantees expandable skills to operate, learn, discover, envision, and reason, that desirably fuels the right outcome.

IIoT infrastructure progression demands effective defense against cyber threats in the context of insight, visibility, detection, investigation & response to diminishing the vulnerability's impact. Furthermore, well-orchestrated and self-propagating advanced persistent threats (APT) are hard to detect due to adversaries' adopted concealment techniques, e.g., register reassignment subroutine recording, instruction subroutines, code transportation, and code integration. Broadly speaking, APT is a smart code that can mimic IoT

The associate editor coordinating the review of this manuscript and approving it for publication was Chunhua Su.

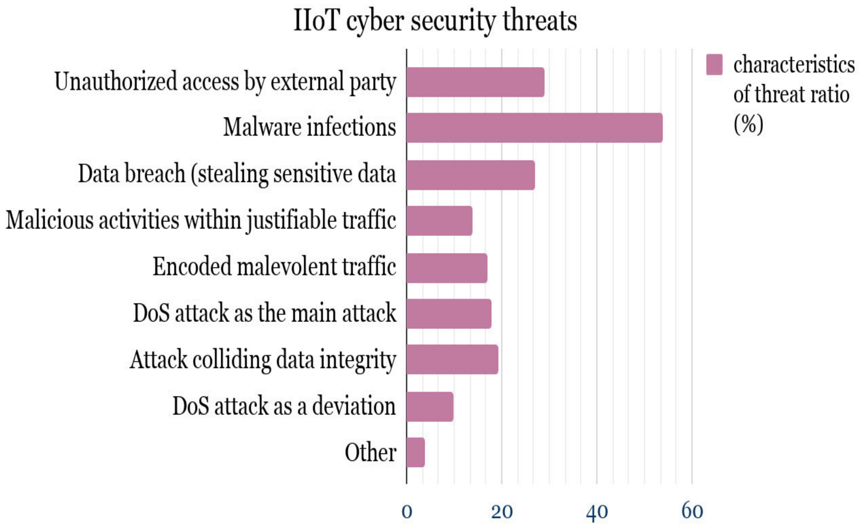


FIGURE 1. Weighted Factor Ratio of advanced IIoT cybersecurity threats.

device capability, including energy consumption patterns, available memory, etc.

Process mapping and optimization to keep a unique data source can be achieved by intelligent security concerning data extraction, both in structured and unstructured mode. Managing the data through 'hypervisor' can help to identify malicious and/or unintended activities by insider edge nodes. Hypervisor helps update pre-installed software and help distribute computing resources (e.g., processing power & data buffering), which can later be used by required interconnected devices. Industrial IoT enabled cloud is currently protected by deploying techniques, e.g., 'controlled access privileges', 'restricting unnecessary micro-processing services', and limiting virtualized stack.

Factors such as (a) lack of security-aware data, (b) misuse of insider device privileges, (c) unable to aggregate and filter cybersecurity-aware alerts, (d) inability to blacklist unauthorized event/access, (e) poorly configured interconnected IIoT infrastructure, (f) improper utilization sensitive information by legitimate or adversary controlled applications, (g) lack of realization regarding flash crowd or denial of service (DoS) in context of data and application can result in a devastating impact on efficient industrial automation endeavor.

Necessary data for figure 1 was aggregated by analyzing audit logs obtained from (a) network access devices (e.g., EAGLE30 firewall, IEEE 802.15.4 nodes, and cloud-enabled proxy servers), (b) unified threat management (Barracuda) system, (c) network access control (NAC (FortiNAC)), (d) transaction logs and (e) Hadoop (an unstructured data source).

A. PROGRAMMATIC CHALLENGES

To attain an applicable secure framework, the system should be able to identify gaps between best practices (i.e., enhanced IT complexity, device harmonization, continuous threat assessment, an actionable audit of delegated nodes, application/process dependent level of security, and verification of standard procedure). A few considered programmatic security concerned challenges in IIoT are:

- Identify and cope with uttermost severe established and unfamiliar vulnerabilities;
- Location-aware applications, hardware and benchmarked network testing (i.e., design, integration, liability, APIs, electronics, & communications (Bluetooth, Wi-Fi, etc.)) mechanism;
- Establishment of identified risk/threat/malware repository for effective and efficient defense;
- Real-time data visualization of systematic security-driven testing outcomes;
- Automated asset aware vulnerability (such as brute forcing, malware and ransomware, stealth attacks that evade detection and untrustworthy communication) ranking system.

B. INDUSTRY DRIVEN MODULAR NODE FORMULATION

IIoT architecture can be divided into three sub-units (a) things (i.e., Wind River Linux, microcontrollers and microprocessor), (b) gateway devices (network), and (c) cloud (servers, storage, API's management). Considering this setting, the security layer is dependent on (1) control layer, (2) data layer, and (3) communication and connectivity layer. Layer structure will guarantee tier-based end-to-end security. It is worth mentioning that connectivity for devices (sensors and actuators) can be achieved by various protocols/solutions such as WiFi, Bluetooth, Ethernet, and RFID. Such offering necessitates that middleware and software should manage security parameters (i.e., (a) confidentiality of data, (b) discovery, registry, and permitting new devices, (c) allow I/O

TABLE 1. IIoT industry standards (devices & protocols).

Microprocessors	IntelAtom, ARM Cortex-M73, ESXi 6.7
Chip	Ultra-wide Band (UWB) i.e. very efficient for event detection and pattern recognition
Protocol	Constrained Application Protocol (i.e. runs over User Datagram Protocol)
Protocol Evaluation	6TiSCH Performance Estimator [1]
Communication Stack	Mulle (based on IEEE 802.15.4 and 6LowPAN)
Data Encoding	Sensor Markup Language (SenML) using JSON (compressed encoding size 206 bits), XML (compressed encoding size 235 bits), CBOR (compressed encoding size 196 bits), EXI (compressed encoding size 184 bits)
Localhost Port	5683
Connected Device Platform	Contiki OS [2]
Connectivity Software Platform	CoAP framework [3] for Contiki OS
Cloud Application Platform	Isidorey (mesh systems)

data streams, (d) storage policy identification, (e) remote blacklisting and rebooting of a specific device, (f) script-based device capability upgrade, etc.) for sensing nodes and gateways deployed on premises and in cloud-oriented infrastructure paradigm.

HYPER-AUTONOMOUS (LEMMA)

IIoT produces gigantic data; it prompts numerous issues to the next generation network. Hence, the IIoT framework must aim in terms of tractability and scalability. Furthermore, fog computing and passive data analytics require integration. It permits the network to adjust itself much quicker to service necessities with improved functioning effectiveness and intelligence. Thus, hyper-autonomous skill is a course of technology that can proactively answer back to real-world disorders without assistance.

Upon fulfillment of the lemma, the mechanism will (a) advances equipment trustworthiness, (b) lessens the rate of device failures, (c) diminishes the time disbursed on maintenance caused by security risk, (d) reduces the unprepared interruption due to disastrous failure (e) condenses the likelihoods of collateral destruction to the arrangement by obeying guidelines defined by existing and developing standards such as: IEC 62264, ISO 15745, MIMOSA IEEE 1232, ISO13374 and EN/IEC 60204-1

II. RELATED WORK

Boyes *et al.* [4] developed an IIoT analysis framework on the bases of well-defined categories: industry division, node location, connectivity, node features, node technology, and user type. Set out framework aid in establishing a methodical assembly of information about IIoT nodes, which permits the evaluation of threats and malicious exposures between different sectors. The manuscript concluded that imminent cyber-physical system security over the lens of spirit would empower the use of both assimilated & directed IIoT system defense procedures and strategies that safeguard the persistent functionality of required amenities delivered by proposed cyber infrastructure.

Sengupta *et al.* [5] proposed a classification of the IIoT security study and bind the cyber-defense with (1) security-and-latency-aware cloud/fog oriented IIoT architecture, (2) requiring all industrial sensing nodes to relay and store data in in-house cloud, (3) provision any reliance on necessary third party cloud service provider, and (4) get equipped with industrial domain specific vulnerability prevention scheme which should be led by organization wide standardized security policy.

Wu *et al.* [6] examined the vulnerabilities in SCF-MCLPEKS [7] scheme and offered a corrective solution. The authors projected a novel vulnerability-aware channel-free certificate-less searchable public key encryption with manifold keywords system for IIoT utilization specifically for the environments where one malicious node is empowered to select arbitrary public key as an alternative of opting for any device's public key. Enhanced scheme (SCF-MCLPEKS$^+$) gratifies indistinguishability and is secure against externally propelled off-line keyword guessing attacks as successful cryptanalysis launched by the server is nearly impossible in the absence of data owner's secret key.

Al-Aqrabi *et al.* [8] presented a multi-layer security mechanism to protect IIoT infrastructure against adversarial attacks, which (i.e., countermeasure) had the ability to react without affecting network latency, imposing higher data rates among IoT devices and enhancing the impact of power demand. Researchers established secure communication by utilizing public-key infrastructure. Moreover, to avoid hidden executable code, an anti-malware layer was enhanced which did not challenge resource abstraction. Ultimately, periodic scanning (i.e., side-channel parameters) of each IIoT device provided an effective defensive shield against malicious signature and adversarial behavior.

Raptis *et al.* [9] comprehensively discussed data management in 'industrial 4.0' environments. Data were prioritized based on characteristics such as criticality, variety, volume and transmission requirements. Paper advised enabling remote monitoring in actuator networks to identify potential misbehavior of industrial devices, transceivers and cluster-based adopted network protocols. Proper data management facilitates information-automation that affects fast control cycles and secure data sharing among nemours stakeholders. Due to the rapid requirement of node engagement, a routine inspection of process logs was advised. Overtime, the system will require diminished actionable tasks/processes, thus will reduce process log volume.

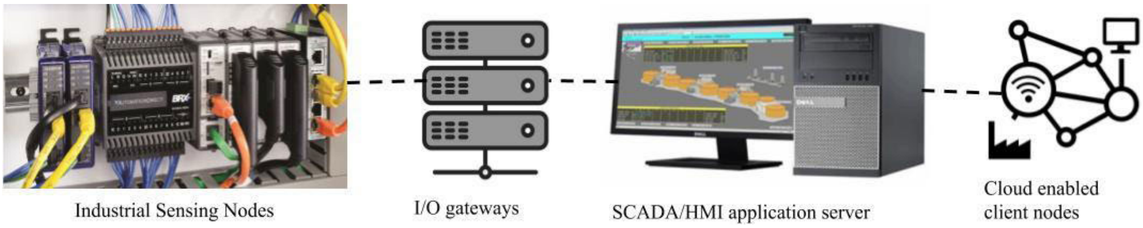


FIGURE 2. Sample representative architecture.

Laszka *et al.* [10] quantified risks associated with cybersecurity and IIoT design optimization and proposed a secure and resilient IIoT System. Numerous instances of similar components were deployed to model redundancy to identify deliberate vulnerability and tested the system with an assumption when most instances were compromised. Loop to identify malfunctions continues until there are no further compromised components. To find the optimum design, an NP-hard problem was applied in polynomial time. Numerical evaluation of the model portrayed diminishing security threat if diversity and integrity duplication were applied.

Geonwoo *et al.* [17] offered a design to deliver an arrangement tool using the MQTT to issue/contribute messaging configuration. Handlers were able to distinguish the provision and admittance route of each node by means of the provision encounter. When the node is linked to the LAN, the gateway routinely accumulates node data and stores it so that the node is capable of being organized over the gateway access. The operator authorized the node data aggregated via the service detection and established the "IF" and the "THEN" condition. The state assessment of the handler-distinct rule was executed according to three states of higher, lower, and equal. The provision detection time processes the interruption from when the operator and the node issue the provision discovery request by means of MQTT to when the outcome was acknowledged. Through the performance investigation, it was established that the provision discovery and rule matching are promising with inadequate overhead.

Sikder *et al.* [18] presented Aegis, a unique context-aware security outline to sense malicious behavior in IoT enabled environments. The method was based on four main components: (a) data accumulator, (b) situation initiator, (c) data exploration, and (d) action administration. Aegis takes the sensor information, produces the settings of the sensors, and outlines malevolent node behavior based on operator actions. For evaluation of the proposed scheme, the malevolent dataset consisted of fifty-five thousand events observed and stored in a ten-day span. To evaluate, methodology applied six diverse performance metrics: True Positive Ratio (TPR), False Negative Ratio (FNR), True Negative Ratio (TNR), False Positive Ratio (FPR), Precision, and F-score (i.e. harmonic mean of precision). Thorough assessment demonstrates that Aegis can accomplish over 95% of precision and F-score in dissimilar smart settings.

Wang and Su [23] projected a system called CCBRSN, which profits Blockchain as a hidden interaction network and set in ciphered communication. In this prototypical, handlers can convey hidden communications via Blockchain communally and fast. For communication confidentiality, the scheme used DES symmetric encryption that is secure and efficient in processing. CCBRSN only guarantees security on a local network with a limited number of transactions to avoid the delay caused due to block generation, which may belong to a public network.

III. PROPOSED METHOD (ZERO TRUST SECURITY)

While designing novel defense mechanism for our IIoT networked devices, we had focused on (a) bandwidth (in terms of capacity, quality of experience (QoE), quality of service (QoS) and flexibility, (b) Time (in terms of synchronization, scheduling, node localization accuracy and coordination), (c) security (in terms of node and data reliability, resilience, and traceability), (d) data computation and storage modeling in the context of node mobility and static deployment. Ultimately, the proposed scheme (that is hinged on 'peer-to-peer distributed control') emphasizes on deploying nodes in such a manner that offers a network with highly synchronized devices with bounded jitter and reliable security. The main reason to program distributed control is to avoid complete platform/framework instant failures. Non-redundant communication nodes (i.e., edge and intermediate routers and switches) can disengage the entire industrial operation at once. Moreover, we have registered / setup protocol stack (i.e., security layer, storage layer, preprocessing layer and monitoring layer) with the purpose of cross-layer optimization that was utilized by all the related nodes.

A. HEALTHY DEVICES REDUCE SECURITY RISK

Industrial internet applications can minimize unexpected interruption, condense obligatory portfolios (within linked zones) and increase throughput. A linked zone means having the information for domain-specific engineering to stay viable and endure to mature. Eradicating cyber-attacks is perhaps an idealistic objective. As an alternative, practicalities require to be as fortified as possible to prevent and diminish the unavoidable. Quantification of associated system risk is:

$$Risk = \sum\nolimits_{resultant} Probability[resultant].Impact(resultant)$$

In the proposed model, the resultant is signified as a set of modules that have been cooperated by an adversary. It enumerates the probability that an adversary compromises a set of modules, which defines a probabilistic procedure about how a malicious entity can deregulate the method components one-by-one. To govern the number of reiterations that are obligatory to discover a good solution in training, we concentrated on the resulting quality (i.e., security hazard) as a utility of the number of looping.

1) NODE SECURITY USING BLOCKCHAIN

An IoT security system interacts with numerous internal and external devices that can be a proxy for intruder driven vulnerability. We have adopted a decentralized peer-to-peer network-oriented private blockchain [11] because it permits one institute to administer the network. That establishes controls about who is permissible to contribute to the network, implement a unanimity protocol and sustain the pooled ledger. In proposed emulation, Blockchain is used to track the device-initiated information and avert replication with any added malevolent records. The 'distributed' characteristic of Blockchain empowers data auditing on a comprehensive scale, and it is this advantage that makes Blockchain unsettling and innovatory. The 'chain' of proceedings in Blockchain software generated data guarantees a conscious, regular simplified assembly of pooled records in real-time that tolerates communications corroborated by several nodes across a dispersed network, guaranteeing the correctness of information. In the context of node security, it is difficult to factotum, falsify, or corrupt a distinct information-set for a particular setback because proceedings are buffered and corroborated autonomously by interconnected ledgers. Moreover, Blockchain empowers planted IIoT nodes with self-governance, discrete characteristics, reliability of information, and provisions of peer-to-peer packet exchange by eradicating procedural bottlenecks and ineffectiveness.

We preferred blockchain to database because all proceedings available on a database are federal; each contributor on a blockchain has a protected copy of all proceedings and all deviations, so every participant can outlook the derivation of the data. Once data can routinely recognize and filter itself based on defined smart contracts and pre-agreed settlement, accomplices are inherently able to rely on it. Blockchain ultimately exhibits ease of data retrieval, improved transparency, better security, decentralization, and true traceability with efficiency.

In our scenario, Blockchain is buffered locally in each node, which will have periodic provisional updates. Devices that accept a transaction (a) will first corroborate its legitimacy (i.e., whether it is harmonious with all prior communications); (b) if the transaction is found to be usable, at that point it is inserted into the blockchain, and (c) directed to all connected devices. Specific reasons for preferring Blockchain to a relational database is specified in table.2.

TABLE 2. Difference between blockchain & relational database (RDB).

	Blockchain	RDB
Expert witness	Decentralized	Centralized
Data Handling	read & write	Create, Read, Update, Delete
Transparency	Transparent	Non-transparent
Cryptography	Yes	No

2) HYBRID INTEGRITY (WHIRLPOOL CRYPTOGRAPHIC HASH AND RSA-AES CRYPTO)

For node/data integrity, we had decided to choose the secure 'Whirlpool Cryptographic Hash [12], [13]'. We implemented Whirlpool because (a) the anticipated capability of producing an impact was of the mandate of $2^{x/2}$ performances of Whirlpool; (b) Specified an n-bit rate, the predictable capability of discovering a communicated/buffered data that jumbles to that value is of the mandate of 2^{x} performances of Whirlpool; and (c) assumed a communication and its n-bit hash outcome, the anticipated capacity of discovering a subsequent data that hashes to the identical value is of the order of 2^{x} implementations of Whirlpool.

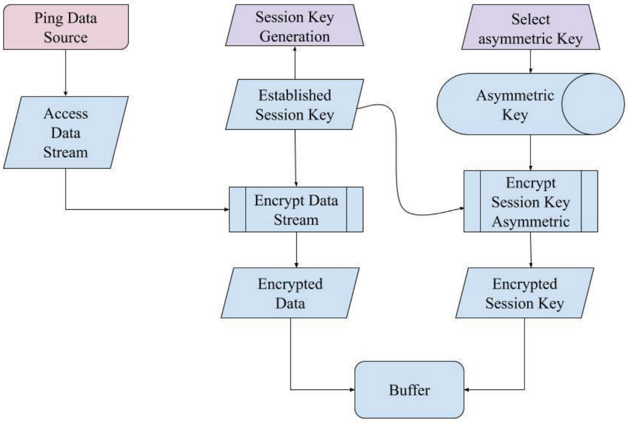
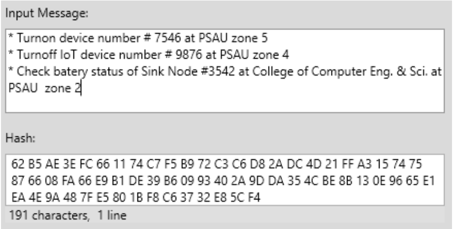
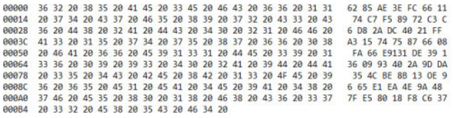


FIGURE 3. Hybrid encryption flowchart (RSA-AES).

Figure 3 illustrates the proposed scheme that utilizes 'hybrid encryption (RSA-AES) [14], [24]. It integrates a blend of asymmetric and symmetric encoding/decoding to profit from the vitality of each arrangement of encryption. The grouping of encryption procedures produces a number of benefits. An association channel is recognized among two or more device groups of the IIoT ecosystem. Nodes then partake in the facility to interconnect over hybrid encryption. Asymmetric encryption can establish a deliberate/desired bottleneck in the encoding progression, but with the synchronized practice of symmetric encoding, both methods of encryption are augmented. The outcome is improved security

TABLE 3. Whirlpool hashing-to-encoding (RSA-AES) specifications.

Block size (bits)	512 bits message digest
Message length	Less than 2^256 bits
Key Size (bits)	512
Number of rounds	10 (input is mapped row-wise, derived by '*' symbol)
Substitution-Box	Recursive structure
Memory Requirement	2^{16}
Computational Complexity	2^{128}
Input / Hash (Sample)	 Input Message: * Turnon device number # 7546 at PSAU zone 5 * Turnoff IoT device number # 9876 at PSAU zone 4 * Check batery status of Sink Node #3542 at College of Computer Eng. & Sci. at PSAU zone 2 Hash: 62 B5 AE 3E FC 66 11 74 C7 F5 B9 72 C3 C6 D8 2A DC 4D 21 FF A3 15 74 75 87 66 08 FA 66 E9 B1 DE 39 B6 09 93 40 2A 9D DA 35 4C BE 8B 13 0E 96 65 E1 EA 4E 9A 48 7F E5 80 1B F8 C6 37 32 E8 5C F4 191 characters, 1 line
Hash to Encoding (RSA-AES)	 00000 36 32 20 38 35 20 41 45 20 33 45 20 46 43 20 36 36 20 31 31 62 85 AE 3E FC 66 11 00014 20 37 34 20 43 37 20 46 35 20 38 39 20 37 32 20 43 33 20 43 74 C7 F5 89 72 C3 C 00028 36 20 44 38 20 32 41 20 44 43 20 34 30 20 32 31 20 46 46 20 6 D8 2A DC 40 21 FF 0003C 41 33 20 31 35 20 37 34 20 37 35 20 38 37 20 36 36 20 30 38 A3 15 74 75 87 66 08 00050 20 46 41 20 36 36 20 45 39 31 33 31 20 44 45 20 33 39 20 31 FA 66 E9131 DE 39 1 00064 33 36 20 30 39 20 39 33 20 34 30 20 32 41 20 39 44 20 44 41 36 09 93 40 2A 9D DA 00078 20 33 35 20 34 43 20 42 45 20 38 42 20 31 33 20 4F 45 20 39 35 4C BE 8B 13 0E 9 0008C 36 20 36 35 20 45 31 20 45 41 20 34 45 20 39 41 20 34 38 20 6 65 E1 EA 4E 9A 48 000A0 37 46 20 45 35 20 38 30 20 31 38 20 46 38 20 43 36 20 33 37 7F E5 80 18 F8 C6 37 000B4 20 33 32 20 45 38 20 35 43 20 46 34 20

of the transfer of data procedure along with general upgraded network performance.

Furthermore, we have evaluated hybrid encryption against "related-key" attacks. This category of cryptanalysis tries to pop a cryptogram by perceiving how it functions using diverse keys. After correcting the INGRES mechanism of AES encryption configuration, we successfully overcame the related-key anomaly.

Our optimum configuration for client (AES-RSA) was as followed:

a) Type = private / global (protocol: TCP/IP)
b) Evaluated host = 127.0.0.1 localhost
c) enabled = true
d) module = iiot_aes
e) aes-key-size = 128
f) rsa-key-size = 1024
g) rsa-key-scope = process

It is worth highlighting here that exhausting the "*rsa_key_scope = process*" selection can lessen the expanse of time for launching succeeding acquaintances when a progression makes more than one association. Cumulating "*rsa_key_size*" did escalate the data security but also caused extensive association times since bigger RSA keys take extended time to produce.

RSA-AES algorithm was utilized because the S-box is beneficial for the encryption of the data for the validation process. This method diminishes the risk of adversary intrusion. Furthermore, the system provisions any grouping of data key size of 128, 192, and 256 bits.

B. SECURITY ANALYSIS

To attain the 'zero trust security' objective, we perform (1) Hazard and Operability (HAZOP) Analysis and (2) Fault Analysis using Convolution Neural Network, which are elaborated below.

Hazard and Operability (HAZOP) Analysis: HAZOP [15] is a structured checksum technique to validate the probability of interferences/hazards of IIoT nodes/platforms. We have stored data related to operational normality as a whitelist of executable routines to flag the abnormal event/occurrence. We merged qualitative (i.e., data flow, node pressure, startup, and shutdown status, timestamping, device vibration and DCS (distributed control system) failure) HAZOP with FMEA (failure mode effect analysis) for cybersecurity assessment of utilized & integrated information systems. During the evaluation process, we benchmarked system-related feedbacks (such as statistics related to node usability, symantec modeled IIoT platform, and API generated data) which was originated by system applications/gateway services, node identity management, resource sharing, proxy services and programmatic integrations.

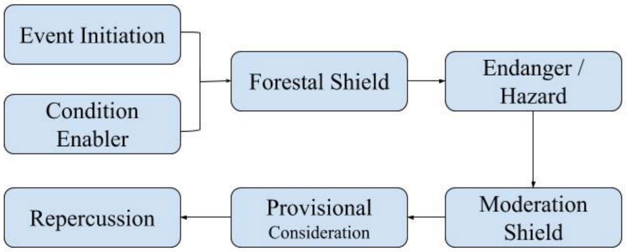


FIGURE 4. HAZOP breakdown evolution.

As per figure 4, adopted HAZOP progression is as followed:

1. Choose the suitable segment of the IIoT enabled plant (devices);
2. Outline the device's policy commitment and procedure settings;
3. Relate the primary/subsequent consideration;
4. Apply constraint (if any) that will contribute the abnormality;
5. Regulate (by contextual data) all the probable foundations of the abnormality;
6. Settle the reliability of respective reason;
7. Calculate the significances of individual event;
8. Measure the security delivered counter to the event roots and its magnitudes;
9. Settle an endorsement for exploit or supplementary deliberation of the concerned issues;

TABLE 4. Assessment of the applicability of HAZOP analysis for the dissimilar IIoT platform categories.

Programmatic	Gateway/Proxy Service based Model
Suitable	Supported
For systems that can be programmatically protracted	For setup that is aligned with Proxy, provisions expanded accessibility
Examined serviceable opportunities were: 1. Resource exchange; 2. Service logic authentication; 3. Reliable and accessible node reputation management; 4. Execution of comprehensible queries (using GraphQL [16]) autonomously from the source node to aggregate and access core data. GraphQL helped propose a scheme to query multiple resource data with a single reference request.	

10. Relate the succeeding factor in anticipation until all events are accessed;
11. Move onto/select the succeeding device of the system until the inter-connected devices positioned in the zone have been scrutinized.

Using a concentrated and coordinated contribution, the proposed scheme handled the systematic process and node examination in consideration of different industrial operational aspects. Proposed scheme found HAZOP as a time deficient but appreciable solution.

FAULT ANALYSIS scheme uses convolutional neural-network (CNN) to analyze association among the aggregated information. To illustrate this scheme, assume that the source information is obtained from various channels and each channel-collected values are accurately timestamped. Now assume that the input data stream consists of ‘x’ bits, each bit is denoted by an N-dimension bit vector. The concatenated vector is converted into the yield for respective classification/set over the entirely associated layer and the dropout layer (i.e., comprises inserting junk-data while working out each core layer in the course of forward dissemination for training neural networks) was adopted to encounter data overflow. The dropout probability ‘p’ is applied as:

$$m' = \begin{cases} 0 & \textit{with probability } p \\ m/(1\text{-}p) & \textit{Otherwise} \end{cases}$$

CNN Training Process: For the duration of the all-inclusive CNN training progression, we ensure as many epochs as required to attain our preferred level of precision. With this, we execute succeeding steps:

a) Acquire collection from the preparation data set.
b) Authorize and relay adopted data set to network.
c) Analyze the loss (variance between the anticipated values and the factual values).
d) Determine the ascent of the risk function with respect to the interconnected industrial device operational requirements.
e) Update the ratios by means of the gradients to diminish the risk factors.
f) Repeat above mentioned steps, until system reach to optimum yield.

Algorithm 1 When ‘Apache MXNet’ is not in Training Mode

```
net = neural_network.Successive()
net.add(neural_network.Compressed(‘n’, activation="Rectified Linear Unit"),
    # Augment a dropout layer subsequently the initial completely associated layer
    neural_network.Dropout (dropout1),
    neural_network.Dense (‘n’, activation=" Rectified Linear Unit "),
    # Enhance a dropout layer subsequently the succeeding fully associated layer
    neural_network.Dropout(dropout2),
    neural_network.Dense(0 - 9))
net.initialize(init.Normal($\sigma = 0.02$))
```

MXNet is an open source deep learning framework. Authors used Python language to simulate.

ERROR REPORTING ASPECT

Inadequate control of errors can lead to a range of cyber security complications for applications, devices, and networks. The proposed scheme examines conjoint issues in which comprehensive in-house error communications such as stack bits, database logs, and error cryptograms are exposed to manipulators. We have used distributed SQL “CrateDB” because it supports linear scalability for data ingestion. These data streams can disclose application specifics that should never be publicized. Such specifics can offer hackers opportunities to identify prospective imperfections in the systems. To address this issue, the projected system regularly partakes in a thorough code assessment that examines the program for error behavior logic. A code examination will disclose how the system is planned to handle numerous categories of errors.

TABLE 5. Feature selection during emulation testing.

Program Review #	Global Dataset		Time (ms)	# of features
	Detection Rate (%)	False Alarm Rate (%)		
1	95.03	19.53	14.78	3
2	91.84	16.34	12.53	6
3	89.12	15.97	11.87	8
4	88.01	15.01	11.98	10

Table 5 and Figure 5 list kernel density estimations, computationally efficiency of each white listed process, random variable of any data space, probing user-to-root, DoS (programed for Gafgyt malware, and Apache Struts vulnerability), and remote-to-local access. Overtime, the system gets mature and reduces false alarm rate with respect to adopted number of features.

Although the imperative used for analysis (i.e., pseudocode 1) is highly simple, it allows us to identify a

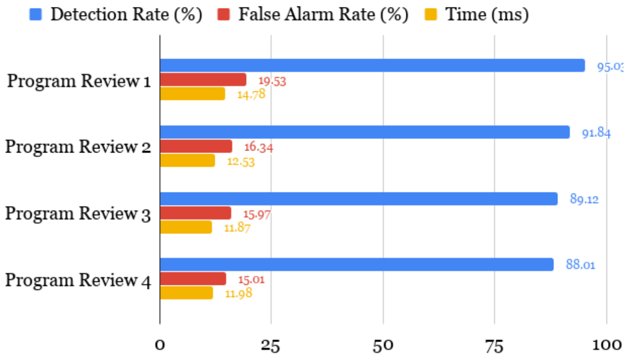


FIGURE 5. Feature selection during emulation testing.

Pseudocode 1 Rule to Check Malicious Software

```
Rule large_internet_protocol_expolit_
possibility:
Common_Vulnerabilities_and_Exposures_
AUG_2020_PSAU {
    String:
      $v = / \ / ( x | tm ) vm / \.{, 300
} \. \.; /
    Condition:
      $v
}
```

wide-ranging malware. For example, a basic outline with IIoT malicious software like Mirai discovers diverse files put on in one domain with dissimilar extensions destined to risk diverse architectures. Furthermore, our research has found that SORA malware used authorizations for exhaustive search attacks that are 'exclusive OR' ciphered with the key DEDEFBAF which were occasionally rapped using UPX-Fbot to condense the extent of the executable dualistic and avoid discovery.

Pseudocode 2 Creating CRON (time-based job scheduler)

```
Echo > /etc/cron.d/start
Echo "11 11 ** root
path="$path:/var/run/sysctl "" >
Echo >/etc/cron.hourly/dkpp
Echo "00 00 ** root
path="$path:/var/run/sysctl "" >
```

Pseudocode 2 may result in two unalike inferences: (a) no other malicious software will have undeviating admittance to open amenities in the infected node, and (b) the node holder will not be able to contact the administration interface by utilizing TCP port such as 443 when it transmits GET request towards victim device. Here, it is worth to mention that a GET invitation with a "command" parameter to *tmshCmd.jsp* would be sufficient to distantly execute a code/script in a zombie node if the ID route is acceptably injected to it.

Table 7 and figure 6 illustrate an assessment dataset that was generated by analyzing data sources, timestamped data, node monitoring, and error logs during the monitoring process, etc. Parameter sensitivity was validated against risks, e.g., cross-site scripting, misconfiguration of security policy, broken authentication, private/protected data exposure, and known vulnerability such as DoS against IIoT framework. It shows an inversely proportional relationship between smaller standard deviation and data / process accuracy rate (i.e. Precision = 1- (wrong value / collected values)).

TABLE 6. *Sample* (Indicators of Compromise).

File Name	Detection Name
MsdUpdate.exe	Trojan.Win32.NYMERIA.MLR
Win32.NYMERIA.MLR is a grayware that hash out on a system as a file downloaded by other anomaly or as a file transferred mistakenly by operator when installing / updating system from unverified source. Upon execution of this spyware, system registry can maliciously be modified.	
DysonPart.exe	Trojan.Win32.SCAR.AD
Win32.SCAR.AD is a trojan that readdresses web browser map reading away from definite online web interface to alternative IP address. This hazard may cause long-term deviations to a computer's operational policies that are *not* reinstated by sensing and eradicating this malware.	

TABLE 7. Guiding principle implementation framework assessment.

Parameters	Prog. review 1	Prog. review 2	Prog. review 3	Prog. review 4
Precision	0.8	0.7	0.3	0.4
Accuracy	0.8	0.6	0.4	0.5
Completeness	0.8	0.9	0.7	0.5
Relevance	0.8	0.7	0.6	0.2
Confidentiality Representation Score	0.9	0.5	0.1	0.5
Security Schema Score	0.9	0.6	0.1	0.1
Sync. Validation	0.7	0.34	0.1	0.1

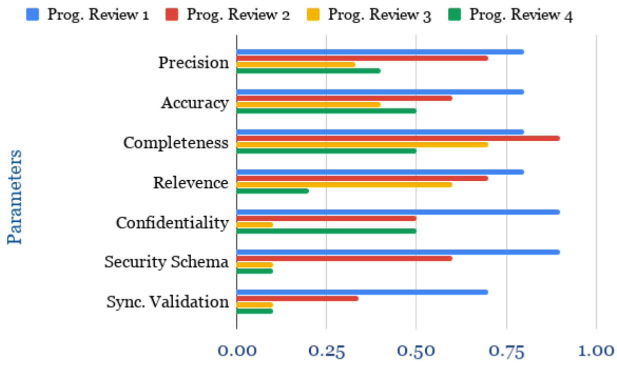


FIGURE 6. Guiding principle implementation framework assessment.

TABLE 8. Evaluated dataset (External).

Parameters	*TUIDS*	*UNSW-NB15*	*UNIBS*
configuration	True	True	True
traffic	True	True	True
data	True	True	True
traces	False	False	False
attack scenarios	True	True	False
Evaluated flow features (sample listing)			
• Aggregate Total of bytes per source & destination IP • Aggregate Number of packets per source & destination IP • Aggregate Number of packets per protocol (TCP, ARP, RARP, IGMP) • Number of incoming connections per source & destination IP • Attacks (probing attacks, DoS (TCP), Data Integrity and theft, etc.)			

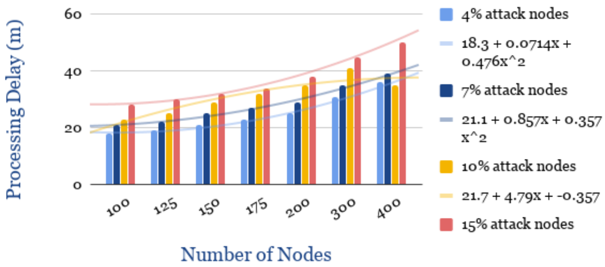


FIGURE 7. Node density vs. processing delay.

Scheme supervisors can safeguard IIoT nodes from malwares with some of embedded superlative practices:

a) Guarantee that IoT nodes' firmware execute on the up-to-date versions by regularly checking policy rules;
b) Adoption of network breakdown to perimeter the extent of contagions and tailor the security parameters of nodes;
c) Deploy strong *EventFilter* to organize tasks and consistent launch strings.

To strengthen proposed scheme, we have also analyzed our framework with publically available TUIDS [19], UNSW-NB15 [20], [22] and UNIBS datasets [21].

Figure 7 illustrates the impact of processing delay with respect to node density in presence of insider malicious adversaries. The scheme calculates delays in terms of transmission (Data size / available bandwidth), propagation (distance to sink node / transceiver transmission speed), data queuing (((number of packets − 1) ∗ size of packet) / (2 ∗ bandwidth)) and general active processing. Emulation has found that attack node density has directly proportional relationship with increased processing delay. Overtime, the system trains itself, and identifies malicious actors inside the network, which ultimately reduces the adversary activity.

IV. CONCLUSION

The Industrial internet of things is now used in business around the world. Wide adaptability and strong operational requirements of IIoT raises challenges related to network reliability, data latency, and cyber-security. Proposed scheme proactively overcame risks by (a) determining and categorizing all nodes involved in the network and (b) screening uninterruptedly to classify compromised nodes and apply a desired policy enforcement to isolate them. Method embraces critical proficiencies in the provision of asset administration, IoT node amenability, network admission mechanism, network subdivision, and incident response initiatives.

We aggregate and analyze approximately one million network statistics and sensory logs, including network connectivity traces, node density behavior (i.e., variation over time) with respect to data generation and aggregation. To evaluate the performance of adopted protocols, '6TiSCH Performance Estimator' was utilized. In summary, the work presented in this article is a step in the direction of the enactment of an abundantly linked world, where respective nodes are securely reachable and open for communication.

DECLARATION OF COMPETING INTEREST

The authors declared that they had no conflicts of interest with respect to their authorship or the publication of this article.

DATA AVAILABILITY STATEMENT

The [Simulation / Experimental Code and Quantitative Analysis Outcome] data used to support the findings of this study are currently under embargo while the research findings are commercialized. Requests for data, [01/03 months] after publication of this article, will be considered by the corresponding author.

ETHICAL APPROVAL

All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

REFERENCES

[1] N. Accettura, E. Vogli, M. R. Palattella, L. A. Grieco, G. Boggia, and M. Dohler, "Decentralized traffic aware scheduling in 6TiSCH networks: Design and experimental evaluation," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 455–470, Dec. 2015.
[2] Y. B. Zikria, S. W. Kim, O. Hahm, M. K. Afzal, and M. Y. Aalsalem, "Internet of Things (IoT) operating systems management: Opportunities, challenges, and solutions," *Sensors*, vol. 19, no. 8, p. 1793, 2019.
[3] M. Iglesias-Urkia, A. Orive, and A. Urbieta, "Analysis of CoAP implementations for industrial Internet of Things: A survey," in *Proc. ANT/SEIT*, Jan. 2017, pp. 188–195.
[4] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, 101, pp. 1–12, Oct. 2018.
[5] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.

[6] T.-Y. Wu, C.-M. Chen, K.-H. Wang, and J. M.-T. Wu, "Security analysis and enhancement of a certificateless searchable public key encryption scheme for IIoT environments," *IEEE Access*, vol. 7, pp. 49232–49239, 2019.

[7] M. Ma, D. He, N. Kumar, K.-K.-R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 759–767, Feb. 2018.

[8] H. Al-Aqrabi, A. P. Johnson, R. Hill, P. Lane, and T. Alsboui, "Hardware-intrinsic multi-layer security: A new frontier for 5G enabled IIoT," *Sensors*, vol. 20, no. 7, p. 1963, Mar. 2020.

[9] T. P. Raptis, A. Passarella, and M. Conti, "Data management in industry 4.0: State of the art and open challenges," *IEEE Access*, vol. 7, pp. 97052–97093, 2019.

[10] A. Laszka, W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Integrating redundancy, diversity, and hardening to improve security of industrial Internet of Things," *Cyber-Phys. Syst.*, vol. 6, no. 1, pp. 1–32, Jan. 2020.

[11] K. Brünnler, D. Flumini, and T. Studer, "A logic of blockchain updates," in *Proc. Int. Symp. Log. Found. Comput. Sci.*, Cham, Switzerland: Springe, Jan. 2018, pp. 107–119.

[12] C. Wentz, "Systems, devices, and methods for signal localization and verification of sensor data," U.S. Patent Appl. 16460724, Jan. 2, 2020. [Online]. Available: https://patents.google.com/patent/US20200007331A1/en

[13] W. Stallings, "The whirlpool secure hash function," *Cryptologia*, vol. 30, no. 1, pp. 55–67, Jan. 2006.

[14] S. Sridhar and S. Smys, "Hybrid RSAECC based secure communication in mobile cloud environment," *Wireless Pers. Commun.*, vol. 111, no. 1, pp. 429–442, Mar. 2020.

[15] V. A. Ciliberti, R. Østebø, J. T. Selvik, and F. J. S. Alhanati, "Optimize safety and profitability by use of the ISO 14224 standard and big data analytics," in *Proc. Offshore Technol. Conf.*, Apr. 2019, pp. 1–20. [Online]. Available: https://www.onepetro.org/conference-paper/OTC-29634-MS

[16] R. Khan and A. N. Mian, "Sustainable IoT sensing applications development through GraphQL-based abstraction layer," *Electronics*, vol. 9, no. 4, p. 564, 2020.

[17] G. Kim, S. Kang, J. Park, and K. Chung, "An MQTT-based context-aware autonomous system in oneM2M architecture," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8519–8528, Oct. 2019.

[18] A. K. Sikder, L. Babun, H. Aksu, and A. S. Uluagac, "Aegis: A context-aware security framework for smart home systems," in *Proc. 35th Annu. Comput. Secur. Appl. Conf.*, 2019, pp. 28–41.

[19] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Towards generating real-life datasets for network intrusion detection," *IJ Netw. Secur*, vol. 17, no. 6, pp. 683–701, 2015.

[20] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6.

[21] L. Vigoya, D. Fernandez, V. Carneiro, and F. Cacheda, "Annotated dataset for anomaly detection in a data center with IoT sensors," *Sensors*, vol. 20, no. 13, p. 3745, Jul. 2020.

[22] S. Rajagopal, P. P. Kundapur, and K. S. Hareesha, "A stacking ensemble for network intrusion detection using heterogeneous datasets," *Secur. Commun. Netw.*, vol. 2020, pp. 1–9, Jan. 2020.

[23] W. Wang and C. Su, "CCBRSN: A system with high embedding capacity for covert communication in Bitcoin," in *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*, Cham, Switzerland: Springer, Sep. 2020, pp. 324–337.

[24] J. K. P. Alegro, E. R. Arboleda, M. R. Pereña, and R. M. Dellosa, "Hybrid Schnorr, RSA, and AES cryptosystem," *Int. J. Sci. Technol. Res*, vol. 8, no. 10, pp. 1777–1781, 2019.

USMAN TARIQ received the Ph.D. degree from Ajou University, South Korea. He led the design of a global data infrastructure simulator modeling, to evaluate the impact of competing architectures on the performance, availability, and reliability of the system for industrial IoT infrastructure. He is currently an Associate Professor with the College of Computer Engineering and Sciences, PSAU. His international collaborations/collaborators include, but not limited to, NYIT, Ajou University, PSU, University of Sherbrooke, COMSATS, NUST, UET, National Security Research Institute (NSR), Embry-Riddle Aeronautical University, Korea University, Manchester Metropolitan University, University of Bremen, and Virginia Commonwealth University.

AHMAD O. ASEERI (Member, IEEE) received the bachelor's degree in computing from King Saud University, Saudi Arabia, the master's degree in computer science from the University of Wisconsin-Madison, USA, through a Full Scholarship, and the Ph.D. degree in computer science from Texas Tech University, USA, through a Government Scholarship. He is currently an Assistant Professor with the Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Saudi Arabia. His main research interests include the field of artificial intelligence (AI), having the main focus in the area of deep learning: with application to neural network-based risk analysis in physical unclonable functions for resource-constraint IoTs, natural language processing (NLP), and computer vision, data mining: with application to clustering techniques, including bisecting K-means clustering (BKM), limited-iteration bisecting K-means (LIBKM), and memory-aware clustering algorithms, and applied deep learning for medical applications.

MOHAMMED SAEED ALKATHEIRI received the bachelor's degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, the master's degree in communication network security from the Beijing University of Aeronautics and Astronautics (Beihang), China, and the Ph.D. degree in computer science from Texas Tech University, USA, through a Full Scholarship. He was a Researcher with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. He is currently an Assistant Professor with the Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia, where he is also the Vice-Dean of Graduate Studies and Scientific Research. His current research interests include the area of cybersecurity, digital authentication, machine learning and pattern recognition, security in resource-constrained devices, and technological innovation management. He served as a Consultant for national projects and joined the Prince Muqrin Chair for Information Security Technology (PMC) along with government departments on National Information Security Strategy project as a Security Consultant.

YU ZHUANG received the Ph.D. degree in mathematics and computer science from Louisiana State University, in 2000. He is currently an Associate Professor with the Department of Computer Science, Texas Tech University, USA. His research interests include parallel computing, high performance memory systems, and large-scale computing. He has also research works in deep learning with application to neural network-based risk analysis and data mining with application to clustering techniques, including bisecting K-means clustering (BKM), limited-iteration bisecting K-means (LIBKM), and memory-aware clustering algorithms. He has a considerable contribution to the IEEE and ACM communities as a committee member of respectful journals, conferences, and workshops around the world.