IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 November 2023, accepted 28 January 2024, date of publication 1 February 2024, date of current version 7 February 2024.

*Digital Object Identifier 10.1109/ACCESS.2024.3361039*

TOPICAL REVIEW

# A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security

**NAVEEN TATIPATRI AND S. L. ARUN**
School of Electrical Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
Corresponding author: S. L. Arun (arun.sl@vit.ac.in)

This work was supported by the Office of Dean, Academic Research Velllore Institute of Technology (VIT), Vellore.

**ABSTRACT** Continuous communication and information technology advancements facilitate the modernization of the conventional energy grid into an integrated platform. Internet-of-Things (IoT) incorporates power systems, particularly smart grid features and the delivery of new services from the utility side to the end user over a two-way communication channel. However, severe security vulnerabilities have been created due to over-dependency on IoT based communication systems. In addition, critical information exchange between any two entities or devices is always an appealing target for cyber-attackers, especially with financial interest motive by damaging integrity, confidentiality and authenticity in a communication channel. Maintaining data security and preserving privacy in between two entities during the transmission or any data distribution are essential. The potential attacks and impacts of those attacks need to be investigated to develop an effective cyber security infrastructure. Thus, considerable researchers focused on detection and mitigation of these vulnerable cyber-attacks using advanced computation tools. This review article thoroughly investigated possible ways to address cyber security challenges such as smart meter security, end-users privacy, electricity theft cyber-attacks using blockchain and cryptography against communication attacks in smart grid. The operational impacts of cyber-attacks on power system security, as well as the economic impact on deregulated energy markets, have been extensively explored. In addition, the robustness of security features and cryptographic methods against various cyber-attacks is investigated to suggest unexplored cyber-attacks for future scope. Specially, the study of real-world cyber security events, case studies, new findings and new scopes in diverse power industries are carried out. More than 135 research articles has been examined for this review article. This paper mainly concentrates on distribution-side cyber-attacks with impact analysis, detection and protection techniques.

**INDEX TERMS** Cyber attacks, cyber security, cryptography, Internet of Things, power systems, smart grid.

## I. INTRODUCTION

In recent accomplishments, integration based on Machine-to-Machine (M2M) communication and widespread application of IoT communication technology played a vital role in smart grid. Incorporating IoT into a smart grid enables seamless interactions throughout all energy sectors such as generation, transmission and distribution, [1]. A traditional grid has a mechanized one-way communication infrastructure with fewer sensors. In contrast, a smart grid has digital two-way communication with more sensors. While adopting a future power system incorporating IoT provides effective billing, improved corrective capabilities during failures and enhanced operational efficiency [2].

Using a two-way communication channel, consumers and service providers communicate via smart meters, sensors, Advanced Metering Infrastructure (AMI), meter data management systems, and utility servers [4]. A smart grid includes an intelligent monitoring system that monitors all electricity flowing through the system which can more

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

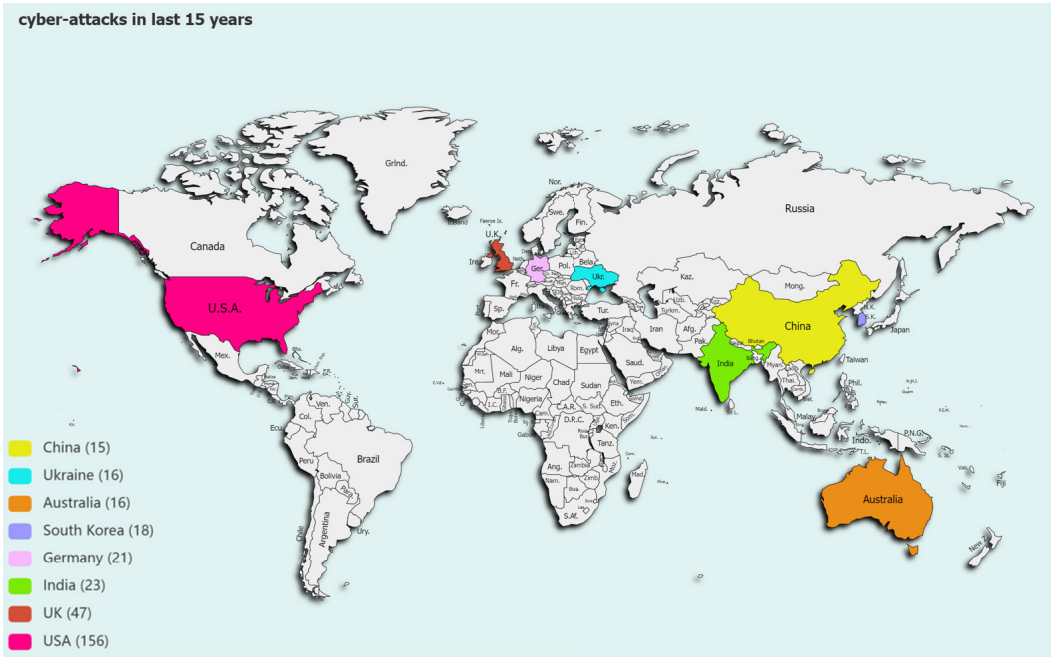



**FIGURE 1.** Reported cyber-attack incidence in last 15 years around the world [3].

efficiently balance the power flow, detect surges, outages and technical energy losses. In addition, smart grid technology also reduces operational costs, saves energy by using demand side management, demand response and Transactive Energy Management (TEM) technologies.

Through internet-based communications, public solutions on control and monitor the smart grid and high dependency could cause disaster due to vulnerabilities. Further, attackers could find infrastructure desirable [5]. Hence, increased connectivity and digitalisation pose new security challenges. For instance, an attacker can attack electronic devices by corrupting state estimation readings to maintain im-balance in between demand, supply in real time due to device data falsification [6]. Then, the smart grid's sensitivity could make it a cyber-terrorism target [7]. As a result, it is crucial to examine smart grid components and identify past flaws and cyber security problems. It can even cause plant failure and subsequent physical damage. Virtual networks of the power sector are essential, and attacks on them can impact a country's prosperity, public safety, and national defense. According to a survey by United Nations, most of the world's population already lives in cities (55 % in 2018), and by 2050, that figure will be closer to 68% [8]. These people rely heavily on reliable electricity distribution. Brownouts or blackouts can significantly impact safety and security in such urban settings. Since the last few decades, cyber security attacks have been the most serious concern. According to specops sources [3], the USA has witnessed the most cyber-attacks in the recent decade, followed by the United Kingdom, India, Germany, and South Korea as shown in Fig. 1. The simple fact is that most urban electric infrastructures are ageing and pushed to their breaking points. As mentioned earlier, the urban population data highlights the critical need to secure the utility operations. Deploying an Intrusion Detection System (IDS) and firewalls to secure power grid data, account management, non-segregated networks are necessary.

In recent years, cryptographic primitives are becoming essential solution to provide security for critical information transfer in communication channel by using message authentication codes, hash functions for authentication and Authenticated Key Agreement (AKA) schemes to encrypt messages while maintaining privacy and confidentiality in smart meters to the divisional network [9]. Therefore, this review paper aims to analyze the cyber-attack vulnerabilities and suggests research aspects to meet smart grid security requirements and fulfil security objectives by using detection and mitigation techniques such as cryptography, artificial intelligence, and blockchain. Meanwhile, study how security criteria affect data security, privacy, and cyber threats during data transmission. In [10], researchers have discussed deep learning and machine learning with different network operations, algorithms, and datasets to create a functional IDS which provides cyber security to the system. Arezoo Hasankhani et al., identified the following primary areas for blockchain technology applications in smart grids: demand response, EVs, IoT technology, decentralized energy balance, energy marketing [11]. In addition, a realistic aspect of the main advantages and disadvantages of using blockchain technology in smart grids have been discussed. In [12] authors reviewed about different cyber-attacks, strategies, and approaches for providing cyber security in energy systems. In [13], authors discussed cryptographic approaches as well

as key management techniques. In addition, discussed the security and integrity verification tools for communication protocols.

IoT incorporated power systems, particularly smart grid features posing cyber security vulnerabilities due to over dependency on communication systems. Therefore, the ideal approach for protecting smart grids and energy systems from cyber attacks is to provide accurate, up-to-date, and efficient overviews and details regarding identifying and dealing to cyber-attacks. As of now, researchers have put together several review articles in the literature on block chain, machine learning and deep learning based techniques for cyber security in power systems. However, prior work has not been done in power systems on communication attacks such as Denial of Service (DoS), Man-In-The-Middle (MITM), replay attacks, and so on. This review article assesses the feasibility of identifying the primary fields for cryptographic technology applications in smart grid sectors such as energy marketing systems, M2M and substation communications.

### A. ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| AMI - | Advanced Metering Infrastructure |
| AKA - | Authenticated Key Agreement |
| AVISPA - | Automated Validation of Internet Security Protocols and Application |
| BAN logic - | Burrows-Abadi-Needham logic |
| CK - | Canetti and Krawczyk |
| CPS - | Cyber Physical Security |
| DoS - | Denial of Service |
| DER - | Distributed Energy Resources |
| ECC - | Elliptic Curve Cryptography |
| ECQV - | Elliptic Curve Qu-Vanstone |
| FDIA - | False Data Injection Attack |
| GNY - | Gong, Needham and Yahalom logic |
| GOOSE - | Generic Object-Oriented Substation Event |
| IoT - | Internet of Things |
| IDS - | Intrusion Detection System |
| MITM - | Man-In-The-Middle |
| M2M - | Machine-To-Machine |
| NPP - | Nuclear Power Plant |
| PMU - | Phasor Measurement Unit |
| PLC - | Programmable Logic Controller |
| PMAKE - | Privacy-preserving Multi-factor Authenticated Key Establishment |
| PF-DA - | Pairing Free-Data Aggregation |
| PUF - | Physical Unclonable Function |
| PIDMS - | Proactive Intrusion Detection and Mitigation System |
| RES - | Renewable Energy Sources |
| ROM - | Random Oracle Model |
| SCADA - | Supervisory Control And Data Acquisition |
| SVM - | Support Vector Machine |
| TEM - | Transactive Energy Management |
| TES - | Transactive Energy System |
| TESP - | Transactive Energy Simulation Platform |

## II. TAXONOMY OF CYBER ATTACKS IN POWER SYSTEMS

Taxonomy is the structured classification of things or concepts. Our proposed taxonomies aim to classify various types of vulnerabilities or cyber attacks across the generation, transmission, and distribution sectors. The damages incurred through cyber attacks and the vulnerabilities of attacks on power grids will vary based on the field and strategies employed by the attackers. The majority of cyber-attack exploitation is directly or inversely associated with grid instability. While cyber attacks on the generation sector have primarily relied on False Data Injection Attacks (FDIA) [20], the transmission sector has become a victim of physical access-based attack vectors such as time delay attacks [21], load redistribution attacks, time synchronisation attacks [22], load altering attacks [23], false command injection attacks,and cyber-physical attacks [24]. Most cyber attack vulnerabilities in the distribution sector are network access-based, including MITM attacks [25], DoS attacks [26], Replay attacks [27],and malware attacks. In addition, taxonomy of cyber attacks to power grid with impacts on power systems is presented in fig. 2.

## III. RESEARCH MOTIVATION AND CONTRIBUTIONS

The motivation for this survey arises from the quote, ''wherever IoTs are present, cyber-attack vulnerabilities are also present''. IoT applications include intelligent information transfer, monitoring of pollution, green infrastructure, smart homes, and connected healthcare. Smart grid is the major IoT application, which provides the structure sensing, communication and processing methods necessary for a smart energy systems. The rapid improvements in IoT technology give the new potential for the seamless operation of the smart grid systems. On the other hand, IoTs are becoming cyber-attack vulnerabilities like critical information leakage, and infrastructure damage.

Furthermore, IoT vulnerabilities may leads to grid blackouts like Ukraine's electricity grid attacks in 2015 and 2016 where attackers try to open circuit breakers to stop the electricity supply by using malicious bad firmware injection. In addition to that attackers implemented DoS attack on telecommunication system to block the communication in between consumers and grid. This study describes a public network-based smart grid defensive mechanism, opened possibilities of cyber attacks on smart grids and assists potential researchers and participants in this field in understanding the structure of an IoT-enabled smart grid system, as well as security breaches, prevention, and detection of those security breaches in smart energy systems. The significant contributions of the article are as follows:

1) A thorough examination of random cyber risks across various power sectors such as generation, transmission, distribution, and consumption have been conducted.
2) Detection techniques for various cyber-attacks such as impersonation, replay, privileged insider, man-in-the-middle, denial of service, ephemeral secret leakage,

**TABLE 1.** Comparison of proposed work with Existing Literature.

| Ref.no | Year | A | B | C | D | E | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [14] | 2023 | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ |
| [15] | 2023 | ✔ | ✘ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ |
| [13] | 2023 | ✔ | ✘ | ✔ | ✔ | ✘ | ✘ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ |
| [16] | 2023 | ✔ | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✘ | ✘ | ✔ | ✘ |
| [17] | 2023 | ✔ | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ | ✔ | ✘ |
| [18] | 2023 | ✔ | ✘ | ✔ | ✘ | ✔ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ | ✔ |
| [19] | 2023 | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ | ✔ | ✘ | ✘ | ✘ | ✔ | ✘ |
| Proposed Work | - | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

✔ - Assessment existing literature provided ;
✘ - Assessment existing literature didn't provided
**A** - Cyber-attacks in Power Grid ; **B** - Energy Marketing System ; **C** - AI based Detection and Protection scheme; **D** - Smart Meters Security ; **E** - Case study ; **F** - Real-world Cyber-attacks ; **G** - Cryptography Algorithms in Power Grid ; **H** - Verification Tool ; **I** - Cyber-attack Robustness Assessment ; **J** - Security features Assessment ; **K** - Block chain ; **L** - Cyber-attack impact Assessment

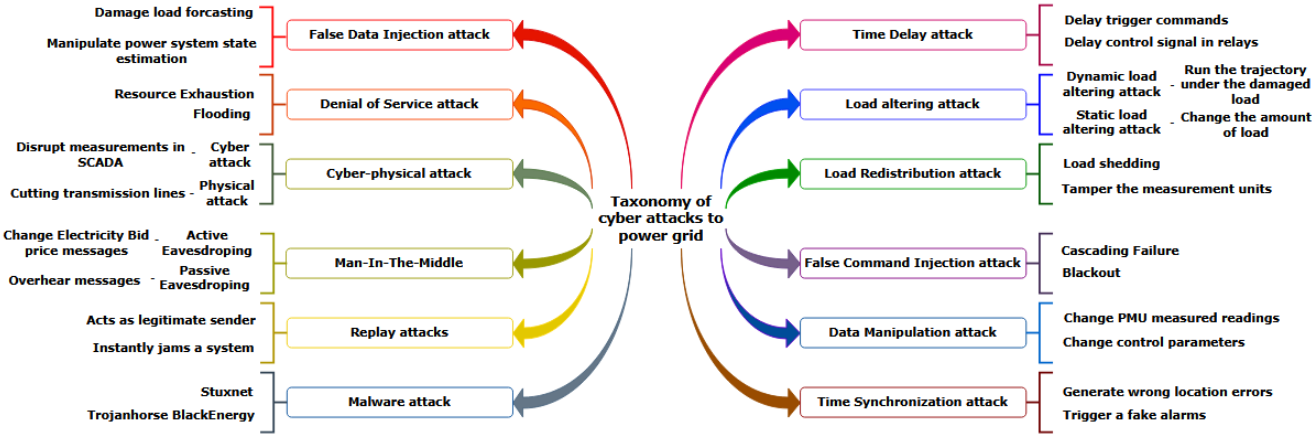



**FIGURE 2.** Possible Cyber attacks Impact on Power systems.

resending, masquerade and device stolen have been investigated. Furthermore, cyber security strategies against these threats have been examined.

3) The significance of different cryptographic algorithms in data privacy and protection while sharing data between two entities has been analyzed.
4) The study of real-world cyber security events and case studies in diverse power industries are carried out. Further, research gaps in smart grid cyber security are identified and highlighted.

The organization of this paper is as follows: section IV provides a review of cyber-attacks in power generation systems. Section V addresses a review of cyber-attacks in power transmission systems. Section VI presents a review of cyber-attacks in power distribution systems consists impact analysis, detection and security using various advanced methods. Section VII provides case studies and addresses real-world cyber-attack incidences on power systems. Finally, section VIII concludes, highlighting the findings, future directions and suggesting possible future research perspectives.

## IV. REVIEW ON CYBER-ATTACKS IN POWER GENERATION SYSTEM

Electricity generation mainly depends upon Nuclear Power Plant's (NPP), hydroelectric, and thermal power plants. Based on the present literature survey, power sectors are changing their approaches to sustainable energy by increasing the integration of renewables even though they have meteorological origins of variability in energy generation [28]. In addition, Renewable Energy Sources (RES) locations are decentralized, which may require fewer employees to report updates in person, which can become a time-consuming process for grid operators and leads to the installation of remote operation tools and IoT devices in power generation systems. In [29], researchers have reviewed wind farm threats, security, unauthorized wind turbine control, disruption and mitigation techniques used to improve confidentiality in the system. In addition, the researchers highlighted future work focused on understanding and combating persistent threats which will increasingly target wind farm assets. The authors of [30] provided a comprehensive review of Cyber Physical Security (CPS), particularly FDIA, in power generation

systems based on the national institute of standards and technology security framework. In [31], the authors have discussed the CPS of photo-voltaic systems and vulnerabilities under various cyber-attacks, such as replay attacks, FDIA, and infrastructure tampering attacks. Furthermore, challenges and opportunities in creating cyber-secure power electronics systems for the next generation have been addressed to assist readers with future research paths. In [32], using real network data and energy generation measurements collected by a wind turbine at Lancaster University, the researchers investigated the amount of malicious scans carried out by Mirai-infected bots in order to penetrate the wind turbine. Furthermore, ping to death with big ICMP packets was investigated.

### A. CYBER-ATTACKS DETECTION IN POWER GENERATION SYSTEM

Cyber-attacks, such as FDIA and MITM, are becoming significant threats in power systems, intending to modify the power system condition, which may lead to improper control actions. Fayha almutairy et al., have developed deep learning models such as Wavelet and Temporal convolutional network to detect FDIA in power systems with high RES penetration. In addition, the performance of the developed models has been evaluated on IEEE 14 bus system with an detection rate of more than 99% and 118-bus system with an detection rate of 97% [33]. In [34], researchers have developed a hybrid deep convolution–recurrent neural network to detect electricity theft in renewable energy-based distributed generation-units with detection rate of 99.3% and low false alarm rate of 0.22%. In [35], the authors have implemented a novel distribution algorithm for detecting cyber-attacks such as adversary manipulation of wind farms turbine-specific control logic parameters. In addition, the implemented algorithm has been tested at the Horns Rev wind farm in Denmark. The presented work shows that the implemented algorithm can also provide cyber security for wind farms. In [36], Huang et al. have developed an online platform to detect cyber-attacks in automated generation control using dynamic watermarking techniques without hardware upgrades on generation units. In addition, the developed technique can also be used for large-scale power systems.

### B. CYBER-SECURITY IN POWER GENERATION SYSTEM

Cyber security is an essential countermeasure to mitigate cyber-attacks and protect critical infrastructure in power generation systems. In [37], researchers have presented a protection approach using a digital frequency relay to protect equipment from large power fluctuations for longer duration in wind energy systems. In [38], authors have implemented an operating reliability evaluation mechanism for multi-state power systems to achieve dynamic system reliability by considering cyber malfunctions. In [39], researchers have implemented a comprehensive algorithm with the help of the proportional fairness index to coordinate defence countermeasures of microgrids during any cyber-attack. Furthermore, it analyzed cyber defence based on coalitional game theory.

In [40], Lee and Huh have presented the system information and event management analysis method to prevent the leakage of peak information and hackings through insecure web services in NPPs. In [41], researchers have developed a framework using knowledge-based hidden makrove modelling to analyze the integrative cyber-attack reaction in NPPs. In addition, researchers have developed a security state estimation method utilizing online updated hidden Markov models to analyze the functional impact. Poong Hyun Seong et al., have designed a cyber-attack reaction planning approach based on Markov decision process model and the Monte-Carlo tree search algorithm to develop optimal reaction plans that improve response margin time and conserve time essential to secure NPPs safety [42].

FDIAs are becoming a primary threat to the generation system, causing disruptions in control logic parameters and state estimation readings to damage the electricity generation quantity, power market by maintaining imbalance in power generation. It is necessary for power plants to provide security for equipment and critical information with improved marginal time and a low false alarm rate against FDIA.

## V. REVIEW ON CYBER-ATTACKS IN POWER TRANSMISSION SYSTEM

Because of its size and the need for high system availability, the energy sector has adapted to digital technology, leading to cyber-attack or cyber-physical attack vulnerabilities to the transmission system. Attackers can use various attack vectors, such as malicious activities, malware injections, and viruses, to compromise the networks, measurements and also changes power flow of the transmission system which can cause a blackout or significant disruption in the power grid [43]. In addition, several sensors have been deployed to analyse the real-time operation of a power system by monitoring bus injection powers, bus voltages, and line currents. The control center assesses the stability of the grid based on redundant measures transmitted through the Supervisory Control And Data Acquisition (SCADA) system. Transferring measured data can also lead to cyber-attacks vulnerabilities. Power systems security threats have been classified into three types:

1) Physical attacks on networks can be considered as terrorist attacks, which may cause disrupting substation operations, cutting transmission lines, or generator units to fail.
2) Cyber-attacks that disrupt measurements or data transmission in SCADA systems.
3) Cyber-physical or coordinated attacks, such as the tripping of transmission lines are the consequence of FDIA's capabilities [24].

In [44], Hossein Rahimpour et al., presented a potential cyber attack vulnerabilities and their risks pertaining to power transformers in power networks. In [45], researchers have considered timing attacks, replay attacks and FDIA to analyze the impact of cyber-attacks on High Voltage Direct Current transmission-based oscillation damping control. In addition, the implementation of cyber-attack preventive measures for Alternative Current-High Voltage Direct Current systems, which have strong, robust control schemes and accurate detection algorithms considered for future scope. Habib Rajabi Mashhadi et al., have proposed an analytical method to analyse the influence of renewable energy power plants on transmission network congestion [46]. In [24], researchers have developed mixed integer linear program model to implement load transmission attacks via FDIAs, which may cause many transmission lines to overflow. The developed model established a standard to analyze realistic cyber-attacks that may disrupt transmissions and cause a blackout. In addition, developing a detection strategy for cyber-attacks aimed at transmission line congestions in Direct Current state estimation is considered for future studies. In [47], Yury Dvorkin et al., have implemented a bi-level optimization model to analyze the impact of distributed cyber-attacks on the distribution and transmission electrical grid. In addition, future research is projected into how attackers can use publicly available grid sources to create more harmful attack strategies.

### A. CYBER-ATTACKS DETECTION IN POWER TRANSMISSION SYSTEM

Mohsen ghafouri et al., have implemented a new detection scheme based on thevenin equivalent system parameters, which performs fast and accurate detection of possible cyber-physical attacks on the voltage stability monitoring of transmission system [48]. In addition, the implemented scheme has been utilized to calculate an indicator that detects Phasor Measurement Unit (PMU) data attacks. In [49], Wilson et al. proposed a deep-learning based stacked autoencoder framework for developing machine-learning features against transmission SCADA attacks. Also, presented unsupervised learning framework to detect automatic and adaptive attacks in the transmission SCADA system. Furthermore, the framework can also be improved so that it not only detects but also locates the event on each line planned. In [50], researchers have presented a cyber-physical data analysis using a deep-autoencoder to monitor transmission protection systems. A ridge regression-based classifier has been deployed to identify cyber anomalies. In addition, the outcomes of the presented models can be investigated as the underlying cause of reported incidents with the aid of cyber log data from protection equipment.

Transformer taps have mostly been used in transmission networks to manage bus voltages. Therefore, tap change commands carried across the SCADA network are always appealing targets for attackers to disrupt system operation. To address the issue, the authors have developed an algorithm that detects the presence of a concealed misleading tap change command in the on-load tap changer [51]. In [22], the authors have proposed a detection technique for cyber-attacks against line current differential relay by using a learning-based framework which employs a multi-layer perceptron model to detect FDIAs, and time synchronization attacks and to divide them from faults. In [52], Pal et al. proposed a mechanism for detecting PMU data manipulation attacks by using that mechanism which continuously monitors the equivalent impedance of transmission lines and divides observed anomalies to detect the presence and location of attacks.

### B. CYBER-SECURITY IN POWER TRANSMISSION SYSTEM

Security systems are one of the most crucial components for transmission system. With ongoing automation, they are becoming more digital and more efficient at delivering electricity which exposing them to cyber-attack vulnerabilities and generating many challenges. In [53], researchers have proposed an algorithm to detect the additional placement of PMUs for maximum security against FDIAs. The algorithm has been evaluated for a range of IEEE-30, 57 and 118 bus-based electric transmission network models. Future research analyze the impact of cyber-attacks on PMU placement strategies in realistic transmission networks. In [21], Lou et al. designed a time delay attack, which delays the delivery of system control commands and a recurrent neural network is used to predict delay values from input traces. The results demonstrated that long short-term memory-based deep learning approach could work well in power plant control systems based on data traces from three sensor measurements such as pressure, temperature, and power generation. In [54], Dehghani et al. launched an FDIA on the information exchange between independent system operator and under-operating agents in the power transmission system to evaluate system security levels. Blockchain has developed to increase the data confidentiality between independent system operator and under-operating agents.

The transmission system is more vulnerable to time delay and PMU data manipulation attacks. Due to a time delay attack, a delay in trigger commands can cause critical infrastructure damage or cascade failure, and PMU data manipulation may lead to load shedding or power overflow in a transmission system. Late detection of FDIA can cause power transmission lines tripping, change in power flow, and large-scale cascade failure [55], some defences against power transmission line attacks include maintaining PMU placement strategies, implementing fast key agreement protocols for secure communication and using blockchain to maintain confidentiality while sending commands.

## VI. REVIEW ON CYBER-ATTACKS IN POWER DISTRIBUTION SYSTEM

Distribution networks are more susceptible to cyberattacks due to their vast size and decentralized nature. In addition,

IoT applications become integral part in distribution system components such as electricity marketing, substations, smart meters as shown in the Fig. 2. As a result, they are exposed to major cyber-security risks, such as attacks, vulnerabilities, and consequences. Due to their control and communication requirements, even Distributed Energy Resources (DER) and battery storage installation may pose negative impact on the grid. In [5], the authors have reviewed the threats and potential cyber-security vulnerabilities, attack countermeasures, and security requirements in IoT-based smart grids. The below mentioned literature evaluated impact analysis of cyber attacks in smart distribution system.

In [56], Ma explained the cyber security challenges in smart cities, such as critical information leakage and intentional cyber-attacks by considering four essential components in smart cities such as smart grid, the smart homes, the smart transmission system, and the smart healthcare system. Furthermore, future research focus on cyber security challenges, threats to user privacy, and relevant authorities and policymakers. Researchers utilized the observer-based method and the decomposition form of the system matrices to analyze the impact of DoS attacks on state estimation in [26]. In addition, the detection and estimation of distributed attacks have been considered for future study. Researchers have implemented a game theory model for power plants, transmission lines, and distribution networks to analyze cyber-attacks and defence probability [57]. In addition, it allows decentralized defence strategies to make defenders separate decision-makers planned for future studies.

In [58], researchers have analyzed the security and privacy of emerging peer-to-peer electricity trading markets. Further, designing privacy-preserving protocols for the defined scenarios using the specified requirements as a guideline is proposed for future studies. In [59], Marufu et al. proposed a strategy for determining how successful cheating attacks on power marketing schemes can be executed in resource-constrained smart microgrids. In addition, mitigation techniques are implemented to prevent cheating attacks. The authors have presented a systematic detection of possible cyber-attacks and examined the influence of attacks on power market operation in association with TEM–based power systems [60]. Furthermore, intend to examine and analyze the impact of additional attacks, such as DoS and replay attacks, on the microgrid's peer-to-peer markets, as well as deploy detection schemes in the microgrid considered for future work. In [61], researchers have presented an ensemble decision tree approach based on the bagging technique to find possible anomalies in the electricity market and physical measurements within the Transactive Energy System (TES), which can reduce the impact of outliers. In addition, the presented approach may be tested on advanced use scenarios to depict a few realistic TES behaviors. In [62], Zhang et al. implemented a deep-stacked autoencoder algorithm to identify possible anomalies in the electricity market and physical measurements with an accuracy rate of 96.9%. The proposed algorithm analyzed the main cause and provide appropriate control actions to protect utilities and prosumers from cyber intrusion. In [63], Wang et al. detected possible anomalies in TES by considering zero-mean FDIA and analyzed cyber-attacks impact on price, quantity and market clearing price. In [64], researchers build a electrical trading protocol in the java programming language to maintain privacy preserve in between prosumers and utility by using blockchain and Elliptic Curve Cryptography (ECC). Pal et al. analyzed the influence of data integrity attacks on electricity pricing exchange in between distribution system operator and price-responsive loads in TES [65]. The system performance is evaluated using four metrics such as operational, financial, comfort, and reliability metrics under data integrity attack by using a 240-bus western electric co-ordinating council transmission model with modeling of the distribution system at specific buses. In [66], researchers have analyzed the impact of manipulated malicious bid prices and quantity cyber-attacks in TEM. Moreover, the TEM operation has been studied through proxy attacks simulated on the TE30 test system. In [67], the authors have created a comprehensive simulation-based transactive energy valuation method to systematically assess the system value, process, object, and design. In addition, a co-simulation-based Transactive Energy Simulation Platform (TESP) has been developed based on the valuation method to perform marketing operations. The work remarks that can deploy agents and market mechanisms without reprogramming any simulators.

### A. CYBER-ATTACKS THROUGH DEVICES

AMI is a catch-all word for whole infrastructure, from smart meters to control center equipments which establish communication between two-entities or devices. The purposes of AMI can include remote meter reading for error-free data, identifying network problems, load profiling, and energy audits by sending energy usage data in near real-time. Unfortunately, sophisticated cyber-attacks on AMI are an open and apparent vulnerability. Attackers typically target less secure system elements such as AMIs to manipulate energy and consumption reports based on financial motives. When the system is heavily loaded, the failure of a single critical component can cause a chain reaction of component failures, eventually leading to blackout. To safeguard the necessary infrastructure from cyber-attacks several researchers analyzed attack detection and protection techniques.

#### 1) DETECTION OF DEVICES THROUGH CYBER-ATTACKS

Energy theft has become one of the most concerning attacks in electricity distribution system. In [68], researchers utilized support vector regression and impact difference to detect possible anomaly pricing cyber-attacks that influence the guidelines of smart meter electricity rates in smart home systems. Bhattacharjee and Das implemented a two-tier approach to detect the FDIA in data consumption without increasing the false alarms in smart meters by using

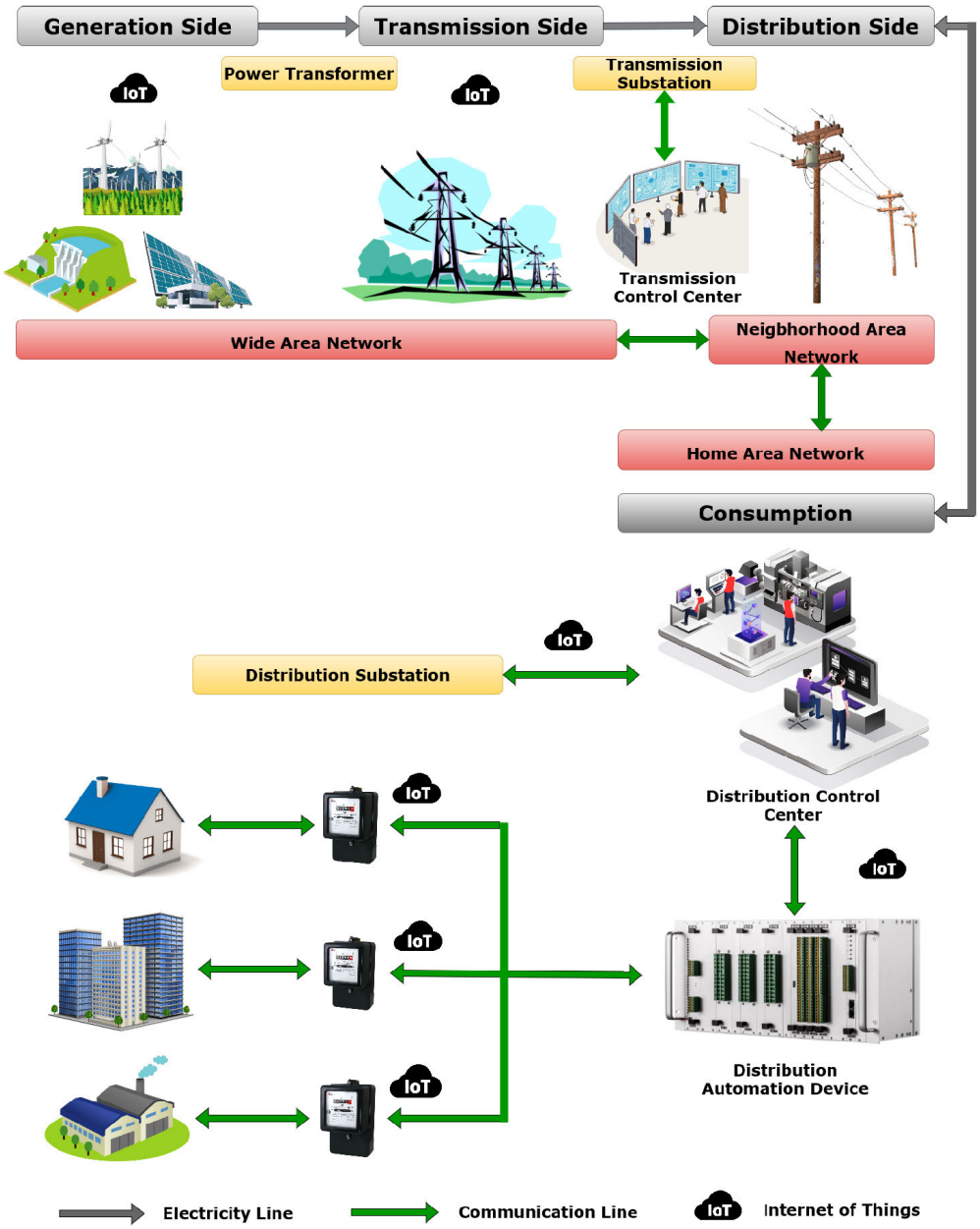



**FIGURE 3.** Advanced Communication Infrastructure for Power network.

harmonic - arithmetic mean ratio as tier-1 and residential under the curve as tier-2 [20]. The work highlights that the analysis on ON-OFF and data omission attacks with minor modifications to the tier-2 detection level approach can also be considered for future studies. In [69], researchers have developed an isolation forest-based detection method to detect FDIA without a pre-training procedure for detection labels in a power system with an fast detection accuracy rate 96.3% at time 1.944 sec. In [70], the authors have developed a highly randomized tree algorithm to detect FDIA, which jeopardizes power system state estimation by applying FDIA into smart meter measurements. The developed algorithm has achieved detection accuracy of 99.76% with IEEE-118 bus, 99.39% with IEEE-57 bus and 97.8% with IEEE-14 bus systems respectively. Furthermore, developed algorithm showed more accurate results than Support Vector Machine (SVM), k-nearest neighbor and random forest. Furthermore, a stacked autoencoder has been used in co-ordination with a highly randomized tree classifier to deal with dimensionality. In [71], researchers have developed multiple-stage IDS techniques, such as temporal failure propagation graph, SVM, for intrusion detection and generating attack pathways for recognizing attack events in smart meters.

### 2) CYBER-SECURITY FOR DEVICES THROUGH CYBER-ATTACKS

Yankson and Ghamkhari developed an attack-thwarting technique for preventing load-altering attacks, which can rectify

frequency disturbances in power grids [23]. Furthermore, the developed technique has given effective results when tested on IEEE 33-bus power distribution system. In [72], the authors presented a bi-level optimization strategy for determining the most compromised and effective attacks as well as independent system operators effective response. Besides that, a defense strategy has been developed to reduce network losses and maintain rated voltage and current values.

### B. CYBER-ATTACKS THROUGH ADVERSAL USERS

Adversary users may act maliciously by tampering their meters to decrease the electricity consumption, resulting in financial losses to utility companies or service providers and grid instability. Researchers proposed various detection and mitigation techniques in the existing literature.

In [73], Ahmadian et al. incorporated FDIA into the measurement system, in which the attacker acts as a virtual bidder in the day-ahead and real-time markets to maximize its profit by trading and proposed the mathematical programming equilibrium constraint-based single-level optimization problem to determine the optimal cyber-attacks against state estimation. In [74], researchers designed a easy-to-implement detection algorithm based on a co-variance estimator to detect and identify coordinated electricity theft incidence by evaluating both dependent & independent smart meter data generation process.

In [75], Yang et al. described a resilience technique for defending Programmable Logic Controller's (PLC) from critical information tampering attacks. In addition, generated a data authentication mechanism with an accuracy of 97.4% for the message digest in PLC-to-PLC communication. In [76], researchers have developed a privacy-aware AKA scheme to provide secure communication in between smart meters and service providers. Moreover, the developed scheme ensures the physical security of smart meters by utilizing light-weight cryptographic primitives such as one-way hash functions and PUF. Gope, implemented an efficient Privacy-preserving Multi-factor Authenticated Key Establishment (PMAKE) scheme based on reverse fuzzy extractor, one-way hash function and PUF to achieve secure smart grid communication [77]. Furthermore, the implemented scheme can guarantee the physical security for smart meters. The Table 2 and 3, presented the simulation platforms used to evaluate the performance of proposed techniques or algorithms against cyber-attacks.

**TABLE 2.** Proposed schemes with analyzed IEEE-bus Networks.

| Ref.no | IEEE Buses |
|---|---|
| [78] | IEEE 37 - Bus |
| [34] | IEEE 123 - Bus Test System |
| [38] | IEEE RTS ( Reliability Test System ) |
| [45] | IEEE New England 39 - Bus AC-HVDC |
| [24] | IEEE 118 - Bus |
| [47] | IEEE RTS & IEEE 13 - Bus Distribution feeder |
| [48] | IEEE New England 39 - Bus & IEEE 118 – Bus |
| [51] | IEEE 118 - Bus |
| [22] | IEEE 39 - Bus |
| [53] | IEEE 14 - Bus for impact analysis & IEEE - 14, 30, 57, 118 |
| [54] | IEEE 14 - Bus Network |
| [79] | IEEE 14 - Bus |
| [69] | IEEE 118 - Bus |
| [70] | IEEE 14, 30, 57, 118 - Bus |
| [23] | IEEE 33 - Bus Power Distribution System |
| [72] | IEEE 94 - Bus |
| [80] | IEEE 57 & 118 - Bus |
| [81] | IEEE 9 - Bus |
| [82] | IEEE 57 - Bus |
| [83] | IEEE 33 - Bus |
| [33] | IEEE 14 & 118 - Bus |

**TABLE 3.** Proposed schemes with analyzed Simulation Networks.

| Ref.no | Different Simulation Scenarios |
|---|---|
| [65] | Western Electric Co-ordinating Council 240 - Bus model |
| [35] | High Fidelity Simulation Test - Bed |
| [36] | NPCC 140 - Bus System |
| [62] | TESP & IEEE 9 - Bus System |
| [66] | TESP & IEEE 9 - Bus System |
| [67] | TESP & IEEE 9 - Bus System |
| [61] | TESP & IEEE 9 - Bus System |
| [84] | OPNET Simulator |
| [85] | SUMO & OMNET ++ |
| [86] | Speed Goat Real-Time Digital Simulator |
| [87] | Power World Transient Simulation Tool |
| [73] | 5 - Bus PJM( Pennsylvania-Jersey-Maryland ) System |
| [88] | Xilinx ISE 14.7 |

### C. ATTACKS THROUGH COMMUNICATION CHANNELS

A smart grid is an IoT-based application that allows energy providers to exchange electricity information with their customers or devices. However, the distribution systems reliance on communication networks makes it highly vulnerable to cyber-attacks. Attackers exploit this by attempting to steal information transferring through communication lines via DoS attacks and MITM, which can result in service interruption, energy theft or critical data theft. In addition, an attacker may try to eavesdrop on crucial messages transmit to the market operator. As a result, the attacker could know the identities of users, smart meter readings, bidding-offer information, electricity supply and demand information from these critical messages. Any drawback happen while providing security may leads to grid instability, AMI damage, and blackouts. Many researchers published various analysis methods, detection, and protection techniques in the literature to control the communication attacks. In [89], researchers reviewed about cyber systems and cyber physical systems, as well as the communication standards and protocols utilized in smart grids. In [90], authors presented a trust-based multi-path routing protocol for secure communication in the Mobile ad hoc network by minimising packet losses and detecting malicious nodes. In addition, cryptography and block chain approaches for providing high security to Mobile ad hoc network are being considered for future scope.

#### 1) DETECTION OF COMMUNICATION CHANNEL CYBER-ATTACKS

In [80], the researchers proposed a cyber-attack detection scheme based on kernel principal component analysis

and randomized trees algorithm for dimensional reduction between the sensor and gathered measurements in smart grid networks. The performance of proposed scheme has been evaluated using standard IEEE 57 and 118 bus systems. In [91], researchers have proposed an artificial feed-forward network using a true data integrity agent-based model to detect false data cyber-attacks in smart grid systems for security assessment. The proposed model has detection accuracy of 98.91% through replay cyber-attacks. The proposed model can also be used in intelligent transportation systems for cyber-security.

In [81], the authors have considered the cosine similarity matching and chi square detector approach for use to detect cyber-attack in smart grid. In addition, the Kalman filter estimation method has been utilized to measure the divergence between actual and estimated data in order to detect attacks. In [84], researchers have developed supervised machine learning algorithms such as tree classification, naive bayes, multilayered perceptron, and multinomial logistic regression algorithms for classification tasks between network abnormality effects such as cyber-attacks and faults on energy-aware smart home systems. In [92], the authors have presented an IoT micro-security add-on that leverages a convolution neural network model to identify phishing attacks on IoT devices. In addition, the recurrent neural network-long short-term memory model has been hosted on back-end services to identify botnet attacks on IoT devices. In [93], researchers have developed an attack detection technique based on a deep belief network and interval state estimator to detect malicious attacks and electrical load forecasting. Moreover, the proposed mechanisms been evaluated on IEEE 14 and 118-bus systems. In [94], the authors have presented an adaptive and resilient N-IDS model using deep learning architectures to monitor network traffic, detect and classify network attacks such as jamming attacks, DoS attacks, and MITM attacks.

In [95], the authors have proposed a data integrity-based effective IDS with two phases: data sampling and selecting features to protect the network with accurate detection rate of 0.936 sec and false alarm rates of 0.33%. Even though the proposed system performs better in unstable conditions, it only detects data integrity-based attacks. In [79], researchers have developed an IDS architecture to monitor and detect lethal attacks such as price manipulation attacks, DoS attacks with detection rate of more than 95% and false positive rate is below 5% using a cumulative sum algorithm in smart grid. In [96], the authors have proposed an SVM algorithm to detect active eavesdropping attacks with detection probability of 95% using artificial training data in the wireless communication channel. From the presented work, adding more hidden features to the proposed algorithms can improve detection performance.

In [97], Sahoo et al. presented a cooperative mechanism based on the cooperative vulnerability factor to detect potential deceptive cyber-attacks in cyber-physical Direct Current microgrids. Furthermore, the proposed mechanism performance has been examined in MATLAB environment. In [85], authors developed a cross-layer IDS based on random forest and k-nearest neighbor to detect spoofing attacks in inter-vehicle communications. Based on the results of the IDS, attackers have been barred from using the wireless charging mechanism.

#### 2) COMMUNICATION CHANNEL CYBER-ATTACKS DETECTION AND CYBER-SECURITY

The use of the internet for data communication between building controllers, such as smart meters and the electric grid, renders the system susceptible to cyber-attacks. A skilled adversary may be able to manipulate the exchanged data which will harm the system. In [98], researchers designed, implemented, and evaluated a monitoring system for open-flow networks and injected proxy attack in between open-flow controller and open-flow switches to capture messages and monitor traffic data. From the presented work, it is to be noted that they can deploy multiple monitoring systems for load balancing and upgrade open-flow versions from 1.0 to 1.1. The authors of [99] created a singular value decomposition technique and private pilot to identify active attacks by authenticating the sender based on the wireless channel. Furthermore, passive eavesdropping and active attacks have been defended using the concept of one-time pad by encrypting wireless channels with a private plot. In [100], researchers have proposed an authentication method to overcome false data flow and improve false data detection with less detection time 4.67 sec without increasing end-user overload in smart grid communication. In [82], the authors have proposed a deep learning-based dual denoising auto-encoder and unified scheme to protect the cyber physical system from eavesdropping attacks and to detect typical cyber-attacks, such as FDIA, DoS, and relay attacks. The proposed scheme performance has been evaluated on IEEE-57 bus system. In [86], researchers have presented a dynamic state estimation technique based on an unknown input observer to estimate the presence of unknown inputs in the microgrid communication channel for stable operation. In addition, a residual function has been generated that detects the presence of FDIA and triggers a detection alarm for attack isolation and mitigation.

#### 3) CYBER-SECURITY FOR COMMUNICATION CHANNEL ATTACKS

A smart meter is an essential component of the smart grid and transmits real-time data to a utility centre. According to the united nation-national institute of standards and technology, bi-directional communication between the two parties opens doors for cyber-attack vulnerabilities. Implementing security for that kind of attack is one of the challenging tasks. Cryptography is one of the efficient technique to provide security against communication channel attacks such as DoS, MITM, jamming attacks, replay attacks, impersonation attacks not only in smart grid but also in health care purpose. In [101], authors proposed a logistic map based

key generation for secure communication by maintaining confidentiality and authenticity in Mobile ad hoc based health care network. Fig. 4. express the structure of cryptography primitive.

In [102], researchers presented an AKA scheme with privacy preservation for smart grid communication. When an adversary compromises a smart meter device, this scheme considers reducing the possibility of a critical leakage attack. In addition, the work highlights that blockchain technology can be used to better authentication schemes for privacy protection in smart grid.

In [103] and [104], Abbasinezhad-Mood and Nikooghadam proposed an ECC-based self-certified key distribution mechanism to address the issue of public key infrastructure maintenance in between smart meters and service providers in smart grid. However, Khan et al. discovered security problems such as the inability to provide security against DoS attacks, insider attacks, anonymity and failure to update the identity and keys from Mood and Nikooohadam's work. Therefore, the design of an authentication scheme to mitigate the flaws mentioned above has been considered for future work. In [105], Ashok Kumar Das et al., proposed a new anonymous signature-based authenticated key exchange scheme for IoT-enabled smart grid, called AAS-IoTSG which allows a smart meter to establish a session key for encrypted communication by mutually authenticating with a service provider. From the presented work, the proposed method can be tested on a Raspberry Pi to demonstrate its viability for IoT-enabled devices with limited resources such as smart meters. In [106], researchers proposed identity-based signature to demonstrate an anonymous key agreement methodology for smart grid system. Moreover, the proposed protocol not only provides authentication but also provides smart meter anonymity. In [107], the authors have presented a novel symmetric homo-morphic scheme to achieve lightweight aggregation for encryption which can provide secure and efficient authentication in smart grids. In [108], Braeken et al. presented a Elliptic Curve Qu-Vanstone (ECQV) certificate-based key agreement paradigm for smart metering communications, which does not require a secure network during entity registration and is resistant to key escrow. Furthermore, the proposed scheme can also be secure under Random Oracle Model (ROM). In [109], researchers have developed a key management scheme based on ECC to mitigate MITM and re-transmission attacks between smart meters and power companies (outside the HAN). The results revealed that the false factor is directly proportional to detection time. For example, the identification time increases by 1.4 seconds as the false factor rises from 0.1 to 0.3.

Cryptographic algorithms have been used to mitigate communication attacks between devices like smart meters and service providers in the power distribution system, which typically uses cryptographic keys to maintain perfect secrecy. Whenever cryptographic algorithms need to be strengthened, it is often possible to use larger keys or hybrid with two algorithms. In [110], researchers presented a defence strategy using event-based cryptography to keep attackers away from obtaining critical information in the sensor communication channel between the plant and the cyber physical system supervisor. In [111], the authors have developed a secure communication methodology using recursive inter-networking architecture, which addresses almost all communication attacks in a closed environment like LAN. Besides, recursive inter-networking architecture capabilities and features can replace existing communication technology while providing increased security. Furthermore, the work highlights that the developed method can be extended to open environments such as wide area networks and neighbourhood area networks. In [112], researchers have designed an Advanced Encryption Standard-512 bit algorithm for faster processing speed with a stable surface environment in web-based applications with more secure communication.

Elakrat and Jung developed a field-programmable gate array security mechanism to minimize information-gathering attacks based on a cryptographic approach to secure data confidentiality and prevent the injection of malware into the vital digital assets data communication system of NPP [113]. In [114], researchers have developed a secure access control scheme based on certificate-less signcryption with a proxy re-encryption scheme which can secure in ROM. The work remarks that the presented scheme can also be extended to merge attribute-based signcryption with proxy re-encryption schemes. In [115], the authors have implemented a lightweight privacy-preserving Q-learning (LiPSG) framework for smart grid energy monitoring. Moreover, four additive secret-sharing-based sub-protocols such as secure action selection, SMAX, SEle and SGry were developed to perform the atomic operations efficiently and securely. Kumar et al. developed a hardware chip integrated S-box advanced encryption standard algorithm to secure the smart grid SCADA system and chip performance is evaluated using field programmable gate array with different key sizes and grid sizes [88]. In [116], the authors present a lightweight fault-tolerant privacy-preserving data aggregation strategy using modified Paillier cryptosystem, ECC, Chinese-remainder theorem, and hash function technique. Furthermore, the proposed scheme robust against all security features. In [117], researchers have developed a novel Pairing Free-Data Aggregation (PF-DA) scheme based on certificate-based cryptography to reduce the impact of certificate pre-checking problems in the energy internet-based smart grid communication networks. Furthermore, designing the decentralised data aggregation scheme can be provided more security for smart grid communication.

In [25], the authors have presented single and multi-antenna models by applying the Stackelberg game with renewed intelligent simulated annealing algorithm and the stochastic algorithm with feedback to provide security

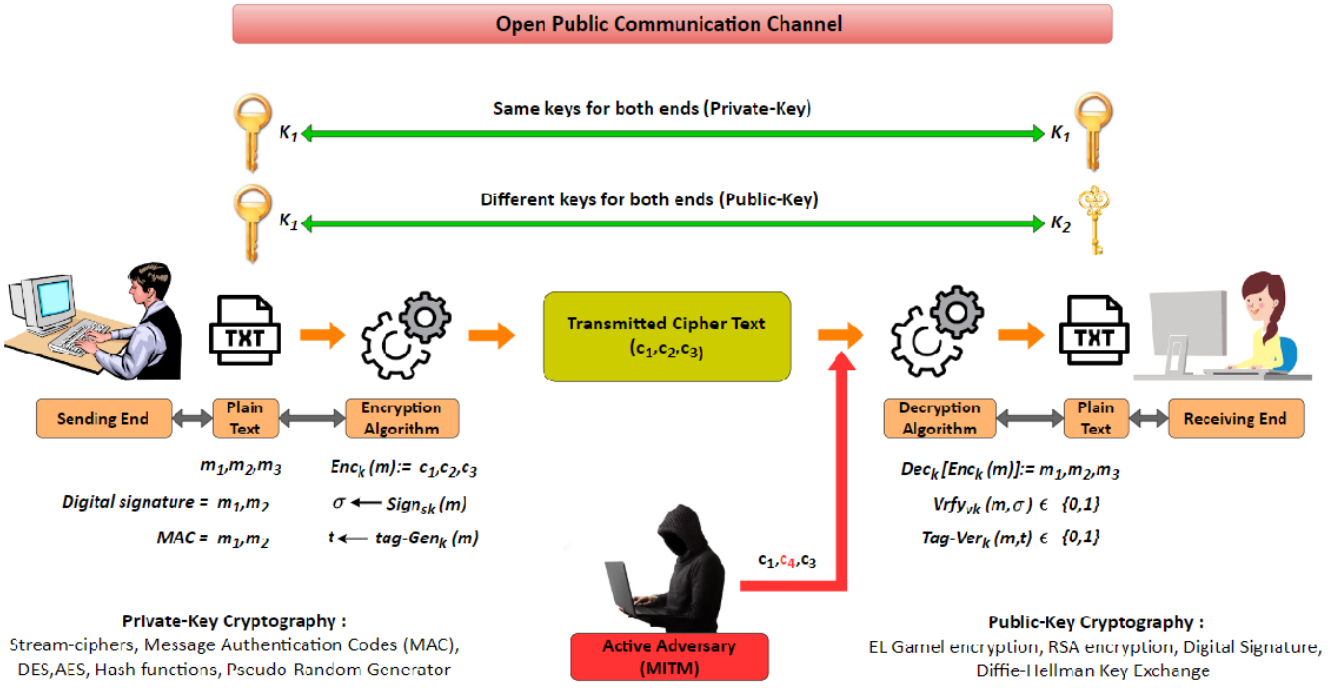



**FIGURE 4.** A Detailed Overview of Cryptographic Primitives in Communication Channel.

against jamming and MITM attacks in green cyber-physical communication systems. In [118], researchers have proposed a cyber-security architecture that integrates identity-based security mechanism and intelligent security system for energy management to provide appropriate security and privacy for components, data, and actions in the energy internet. The evaluated results of the proposed architecture expressed safety and efficiency for energy internet. Marcos Vicente Moreira et al., presented a security module to prevent MITM attacks between controller and sensor communication channel in cyber-physical systems. Furthermore, the extension of the security module offered NA-safe controllability [119]. In [120], researchers have developed a super-lightweight security protocol using a logical XOR and one-way hash function to secure the smart grid neighbourhood area network communications. The work highlights the implementation of a lightweight scalable blockchain-based multi-party computational protocol that can be employed for resource constraint networks. In [121], the authors have proposed a resilient scheduling strategy that uses additional metrics based on the difference between forecasted and actual bills to detect FDIA in interconnected multiple smart buildings. Besides, the support vector regression method has been used to calculate predicted bills.

Moghadam et al. developed a lightweight protocol based on hash and private key to mitigate IEC62351 security flaws while facilitating key agreement in smart grid [27]. The developed protocol can agree the session key within 0.057ms. Furthermore, it explored privacy, authentication, and private data transfer security between two entities and tested several sorts of cyber-attacks such as impersonation, replay, and MITM attacks. In [122], researchers have presented the timing performance of the RSASSA-probabilistic signature scheme digital signature algorithm to secure the Generic Object-Oriented Substation Event (GOOSE) messages in power system control operations. The work highlights the requirement of cyber-security and time domains that an authentication scheme can achieve.

In [123], [124], and [125], researchers have developed multiple techniques such as PUF- based AKA scheme and reconfigurable authenticated key exchange scheme to secure communication channels by mitigating energy theft attacks, such as ephemeral leakage attacks in between service providers and smart meters. In [126], researchers have developed a lightweight mutual authentication scheme based on PUF to encrypt communications in between smart meters and neighbourhood gateways. In [127], the authors have presented a novel authentication key exchange approach based on low-cost memristor-PUF to investigate security between the head-end system and smart meters. Furthermore, the work highlights that the presented scheme for analysing various other attack scenarios, such as replay attack, MITM,

and impersonation attack, has been considered as future scope.

In [128], researchers developed an anonymous authentication approach based on a group signature scheme with configurable linkability with tokens to reduce double spending and billing scam in the smart grid. In [129], the authors developed a hash function, ECC, and symmetric encryption-based anonymous and reliable authentication scheme for the smart grid to ensure the integrity of information transmitted between the smart meter and central service provider. Limbasiya and Arya have discussed various attacks, authentication schemes, and security parameters for secure communication in the smart grid system [130]. Researchers have presented a Diffie-hellman-based message authentication protocol for smart grid communications between the HAN-gateways and BAN-gate ways [131]. In [132], researchers have developed a lightweight ECC-based mutual authentication scheme with trifling operations to secure communication between consumers and substations for smart-grid environments. The presented work shows that the developed scheme can also analyze real-time data communications in smart grid. In [133], researchers have introduced a new AKA protocol using an ECQV implicit certificate to access data securely by providing mutual authentication in smart meters for smart grid environments. Aziz et al. implemented a lightweight authentication protocol based on the hash function with masked identity to secure information exchange between the control centre and smart breakers in a smart grid [83]. The work highlights that the proposed scheme injecting into the REF542plus controller using manufacturing software such as CAN open digital field bus can provide low computation and communication costs for real-time smart grid applications. Gope, proposed a lightweight authentication scheme, while ensuring strong user anonymity support to satisfy all the security features of M2M based home network services [134]. In [135], the authors have introduced mutually authenticated key establishment scheme to provide secure communication between the multiple smart meters and service providers in a cloud-enabled smart grid system. The work remarks the necessity to design two protocols to mitigate: one to store the gathered data in the cloud server and the other to obtain the processed data from the cloud server. In [136], [137], and [138], researchers have developed an ECC-based authentication protocol to mitigate considered communication attacks between smart grid devices and utility centres. Besides, another researcher proposed a privacy-preserving lightweight authentication scheme based on pseudo-identity and secret parameters to address the shortcomings of the ECC authentication protocol. Such shortcomings are the protocol insecurity against masquerade, smart grid device theft, and failure to ensure robust mutual authentication.

In [139], the authors have proposed a blockchain and homo-morphic encryption-based privacy-preserving data aggregate model to prevent internal and external attacks such as MITM, privileged-insider attacks, and impersonation attacks with low computational cost in a cloud computing-based smart grid system. In [140], the researchers have developed a blockchain-based secure and lightweight authentication protocol with centralized register authority to mitigate the majority of common attacks, such as replay attacks, jamming attacks, and DoS attacks in practical smart grid environments. In addition, the work highlights that the developed protocol can be used for batch verification and to evaluate dynamic issues. The Table 4. gives detailed view about the vital characteristics for cyber security against cyber attacks.

As discussed earlier, the proposed schemes can withstand a wide range of attacks, which is critical for communication networks. The security of proposed schemes is evaluated both formally and informally depending on their robustness against major cyber-attacks. From the mentioned literature, the effectiveness of proposed schemes against all possible cyber-attacks are examined in Table 5. Furthermore, the proposed schemes are primarily focused on providing security against well-known attacks such as the replay attack, MITM, impersonation attack, and failing to provide security against insider attacks, which is very difficult to detect, as shown in Fig. 5.

The proposed schemes needs to meet common security requirements such as data integrity, privacy, confidentiality and availability in order to develop good security. Table 6 presented how well the proposed schemes are defended against all potential security vulnerabilities. From the discussed literature, un-tracebility is one of the important security feature, schemes are failing to provide strong security which will become a biggest concern as shown in Fig. 6.

## VII. CYBER-ATTACK INCIDENCE IN POWER SYSTEMS

### A. CASE-STUDIES

Based on 2015 Ukraine cyber-attack, the authors have implemented the cascading outage analysis to analyze the impact of various cyber-attacks by opening all devices, generators, and loads connected to the lines of every transmission and distribution system provider in the North American regional interconnection system [87]. In [141], the authors have implemented electrical power system analysis software in a petrochemical plant to analyze the influence of electrical parameters on modified remote data transmitted cyber-attacks in SCADA systems. Furthermore, the designed cyber-attacks can be mitigated by using cryptography. The authors looked into cyber terrorism in NPPs after the 2014 cyber-attack on the South Korean NPP [142]. In addition, GEN-4, radiation control, and secure information management have been explored as potential solutions to the problem of cyber terrorism in NPPs. In [143], the authors developed a multi-state markov model to analyse the impact of integrity attacks such as command messages for circuit breakers and modifying IED parameter. In [144], researchers analysed IoT-related vulnerabilities, potential mitigation, and prevention techniques for real-world cyber security incidents

**TABLE 4.** Vital characteristics to provide cyber-security against cyber-attacks.

| Ref.no | Year | Platform | Cryptographic Library | Verification Tool | Cryptographic Algorithm |
|---|---|---|---|---|---|
| [128] | 2017 | gcc Apple LLVM Version 8.0.0 | TEPLA 2.0 | - | Group Signature |
| [134] | 2017 | - | Crypto++ library | - | Light weight anonymous authentication & key agreement protocol |
| [131] | 2017 | - | - | proverif | Diffie-hellman based message authentication |
| [103] | 2018 | STM32 F4 DISCOVERY & Nano pi M3 board for to ends | Stm32 & open SSL | Proverif, ROM | ECC- based self-certified key distribution scheme |
| [83] | 2018 | MATLAB R2014a | Java class cryptosystem | - | Crypto hash function, SKA, SGMA |
| [106] | 2018 | - | - | Proverif, ROM | Identity based AKE protocol |
| [108] | 2018 | - | - | AVISPA | Secure key agreement model based on ECQV certificates |
| [27] | 2019 | LAN employed the switched Ethernet network | - | AVISPA | ECC based authentication |
| [76] | 2019 | Ubuntu 12.04 virtual machine | JPBC library Pbc 05.14 & JCE library | - | Privacy - preserving authentication protocol using PUF |
| [122] | 2019 | python | - | - | RSASSA-Probabilistic Signature Scheme |
| [138] | 2019 | Grid smart home hardware testbed, Pentium IV, Hiper smart card | - | AVISPA | ECC based authentication |
| [126] | 2020 | AT91SAM3X8E micro controller board | Arduino Libs as a cryptographic library | Mao, Boyd's logic | Light-weight mutual authentication protocol based on PUF |
| [137] | 2020 | Pentium IV, Hiper smart card | - | AVISPA, BAN logic, ROR | Light weight authentication using pseudo-identity and secret parameters |
| [125] | 2020 | - | - | Scythe, AVISPA | End-to-end PUF based AKE |
| [77] | 2020 | Ubuntu 12.04 virtual machine | JPBC library Pbc-05.14 | - | PMAKE scheme based on PUF |
| [102] | 2021 | NS-3 version 3.28 | C/C++ open SSL library | - | Authenticated Key Agreement |
| [109] | 2021 | Communication inside the network on IEEE 802-15-4 & network outside the building on IEEE 802-16 WiMAX | - | - | ECC based authentication |
| [132] | 2021 | NS – 2.35 | PBC library version 05.12 | AVISPA | ECC based authentication |
| [105] | 2021 | Philips Hiper smart card | - | AVISPA, ROR | ECC-based schnorr's signature based AKE |
| [136] | 2021 | Pentium IV, Hiper smart card | - | Proverif, BAN logic | Light weight authentication using pseudo-identity and secret parameters |
| [129] | 2021 | Pycrypto, Rasberry pi-3 | - | ROM, scythe based security | ECC-based AKE protocol (ARAP-SG) |
| [120] | 2021 | AT91SAM3X8E for smart meter & Intel® core™ i7- 3612QM CPU @ 2.10 GHz and 6GB-RAM for NG | Arduino Libs as a cryptographic library | Mao, Boyd's logic | Super light-weight secure protocol based on one-way hash function and logical XOR |
| [135] | 2021 | - | - | GNY logic, Proverif | Mutually authenticated key establishment protocol |
| [133] | 2021 | - | - | CK security model | Authenticated key agreement protocol based on ECQV implicit certificate |
| [117] | 2022 | Ubuntu 12.04 virtual machine | JPBC library Pbc-05.14 & JCE library | ROM | PF-DA designed by using certificate-based cryptography |
| [127] | 2022 | MATLAB (Mathworks) using okamoto protocol | - | NIST 800-22 statistical tests | Memristor based - PUF |

**TABLE 5.** Robustness of proposed schemes against Cyber-attacks.

| Ref.no | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| [105] | ✔ | ✔ | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ | ✔ |
| [102] | ✔ | ✔ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ |
| [131] | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ |
| [27] | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ |
| [109] | ✘ | ✘ | ✘ | ✔ | ✘ | ✘ | ✔ | ✘ | ✘ |
| [132] | ✔ | ✔ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ | ✔ |
| [76] | ✔ | ✔ | ✔ | ✔ | ✔ | ✘ | ✘ | ✘ | ✔ |
| [136] | ✔ | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ | ✔ |
| [137] | ✘ | ✔ | ✔ | ✔ | ✘ | ✘ | ✘ | ✔ | ✔ |
| [138] | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ | ✘ | ✔ |
| [129] | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ |
| [125] | ✔ | ✔ | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ | ✔ |
| [103] | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✘ | ✘ |
| [106] | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ |
| [83] | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ |
| [77] | ✘ | ✘ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ | ✔ |
| [117] | ✔ | ✔ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ |
| [134] | ✘ | ✔ | ✘ | ✘ | ✔ | ✘ | ✘ | ✔ | ✘ |
| [120] | ✔ | ✔ | ✘ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ |
| [126] | ✔ | ✔ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ | ✔ |
| [135] | ✔ | ✔ | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ |
| [133] | ✔ | ✔ | ✘ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ |
| [108] | ✔ | ✔ | ✘ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ |

✔ - proposed scheme is strong against specified attack ;
✘ - proposed scheme is not strong against specified attack
**A** - Impersonation Attack ; **B** - Replay attack ; **C** - Privileged insider attack ; **D** - MITM ; **E** - DoS attack ; **F** - Ephemeral secret leakage attack ; **G** - Resending attack ; **H** - Masquerade attack ; **I** - Device stolen attack

**TABLE 6.** Robustness of proposed schemes against security features.

| Ref.no | A | B | C | D |
|---|---|---|---|---|
| [103] | ✔ | ✔ | ✔ | ✘ |
| [106] | ✔ | ✔ | ✘ | ✔ |
| [83] | ✔ | ✘ | ✔ | ✘ |
| [125] | ✔ | ✔ | ✔ | ✔ |
| [105] | ✔ | ✘ | ✔ | ✔ |
| [102] | ✘ | ✔ | ✔ | ✔ |
| [131] | ✘ | ✔ | ✔ | ✘ |
| [27] | ✔ | ✔ | ✔ | ✘ |
| [109] | ✘ | ✘ | ✘ | ✘ |
| [132] | ✔ | ✔ | ✔ | ✘ |
| [76] | ✔ | ✔ | ✘ | ✘ |
| [136] | ✔ | ✘ | ✔ | ✔ |
| [137] | ✔ | ✘ | ✔ | ✘ |
| [138] | ✔ | ✔ | ✘ | ✔ |
| [129] | ✔ | ✘ | ✘ | ✔ |
| [77] | ✔ | ✔ | ✔ | ✔ |
| [117] | ✘ | ✘ | ✘ | ✘ |
| [134] | ✔ | ✔ | ✔ | ✔ |
| [120] | ✘ | ✔ | ✔ | ✘ |
| [126] | ✘ | ✘ | ✔ | ✘ |
| [135] | ✔ | ✔ | ✔ | ✔ |
| [133] | ✔ | ✔ | ✔ | ✔ |
| [108] | ✔ | ✘ | ✔ | ✘ |

✔ - proposed scheme is strong against security feature ;
✘ - proposed scheme is not strong against security feature
**A** - Anonymity; **B** - Perfect Forward Secrecy; **C** - Mutual Authentication; **D** - Untracebility

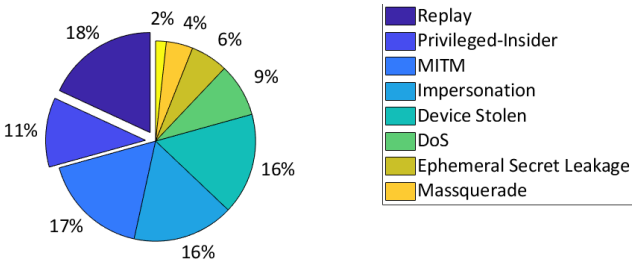



**FIGURE 5.** Percentage of cyber-attacks strong against proposed schemes.

affecting electricity consumers. In [145], researchers have proposed a generalized stochastic petri net to investigate the impact of integrating multi-level preventive, responsible measures on security indicators like mean-time-to-disrupt and system availability against cyber-attacks in NPPs. Furthermore, the proposed approach can also be extended to examine system dependability. In [146], the authors have provided a case study demonstration on the Proactive Intrusion Detection and Mitigation System (PIDMS) to examine the packet replay attack scenario in photo voltaic inverter communication. Moreover, PIDMS is extensible to other smart grid devices to send and receive cyber-physical data streams. In [78], researchers have presented tandem stability and machine learning-based classifiers to analyze the influence of time delay attacks on automatic generation control in the power grid. The presented approach has been evaluated and verified on the IEEE 37-bus system model.

### *B. REAL-WORLD CYBER-ATTACK INCIDENCES ON POWER SYSTEMS*

#### 1) ZERO-DAY ATTACK ON DAVIS-BESSE NPP, 2003

By injecting a zero-day attack into a micro-soft SQL server, attackers gained access to the secret and control

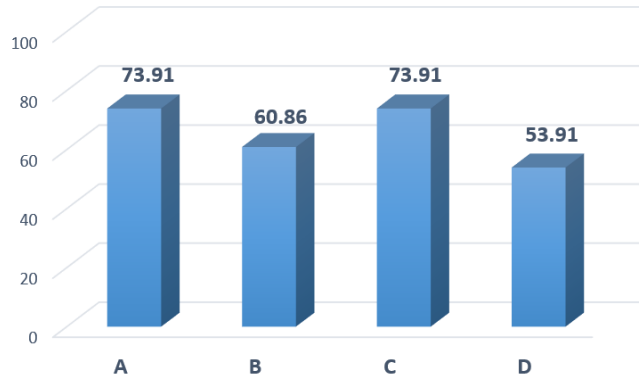



**FIGURE 6.** Percentage of proposed schemes strong against specified security features.

networks of Davis-Besse NPP in Ohio. The injected malware generated a massive amount of traffic in order to disrupt communication networks between corporate and control networks. In addition, the worm had left a safety monitoring system inoperable for more than five hours. Employees were unable to monitor the core temperature sensors at the plant.

#### 2) STUXNET ATTACK ON NUCLEAR PROGRAM OF IRAN, 2010

On November 29, 2010, the Iranian president stated that the stuxnet virus had destroyed hundreds of centrifuges used to enrich uranium at Natanz nuclear enrichment. According to estimates, the stuxnet worm destroyed Nine Eighty-four uranium enrichment centrifuges and destroyed enrichment efficiency by thirty percent. Another virus corrupted government computers at nuclear plants and stolen data in 2012.

#### 3) CYBER-ATTACK ON KOREA HYDRO AND NUCLEAR POWER, 2014

On December 23, 2014, Korea Hydro and Nuclear Power announced that their computer systems had been hacked. ''Unless you stop operating the nuclear power plants until Christmas and give us $1 billion, we will continue to release the facility's secret data'', the hackers posted on their twitter page. Furthermore, two nuclear reactor manuals from Korea Hydro and Nuclear Power were posted online, exposed ten thousand employee's personal data.

#### 4) SANDWORM ATTACK ON UKRAINE ELECTRICITY COMPANY, 2015

On December 23, 2015, remote cyber intrusions at three electric power distribution companies caused a blackout that left over 2,25,000 customers without power for 16 hours in Prykarpattyaoblenergo, Ukraine. The attackers injected malware through spear phishing emails with malicious attachments, gaining access to the SCADA control and then opened breakers at over 30 substations. Furthermore, serial-to-ethernet servers, backup power was disabled with bad firmware, and a DoS attack on the utility telephone system was also carried out.

#### 5) INDUSTROYER ATTACK ON UKRAINE ELECTRICITY COMPANY, 2016

On December 17, 2016, a remote cyber intrusion occurred at a local substation that supplies power to the capital city of Kyiv. Attackers opened breakers at a substation again. However, this time they attempted to compromise the relays.

#### 6) DTRACK ATTACK ON KUDANKULAM NPP, 2019

On September 4, 2019, malware was discovered on a personal computer belonging to a user who was connected to an administrative internet network. The nuclear power corporation of India limited issued an official statement confirming the incident. ''This PC has been disconnected from the critical internal network and networks are constantly monitored.''

#### 7) REVIL RANDSOMWARE ATTACK ON UK ELECTRICITY MARKET, 2020

On May 12, 2020, hackers attacked internal IT systems at Elexon, which is center of balancing and settlement system, works for the energy system operators of Great Britain's national grid. Elexon's official response to this incident was as follows: ''the attack is to our internal IT systems and ELEXON's laptops only. Electricity supply is not affected.''

#### 8) CYBER-ATTACK ON LADAKH ELECTRICITY DISTRIBUTION CENTER, 2022

On March 2022, unknown hackers attempted but failed to hack into an electricity distribution center. ''two attempts by the hackers to target electricity distribution centers near Ladakh were unsuccessful. We have already strengthened our defenses to counter such attacks,'' said India's minister of power and renewable energy.

## VIII. CONCLUSION

This paper reviewed various approaches for cyber-attacks detection, protection and impact analysis in multiple areas such as wind farms, PV systems, transmission systems, smart meters and communication channels. A need of cyber security for IoT-based smart grid systems has been examined. This review article analyzed the literature to provide an overview of the need and potential methods for detecting and mitigating cyber attacks, particularly communication attacks, using artificial intelligence, block chain and cryptographic primitives. When it comes to the analysis of proposed literature, it suggested vital characteristics, simulation platform, libraries to do practical design, simulation and verification of cryptographic primitives for secure communication between two endpoints in a smart grid system. and Furthermore, the robustness of security properties, cryptographic algorithms against various cyber attacks was analyzed to suggest an unexplored attack.

### A. FINDINGS

Based to the literature, FDIA is the most serious concern in the power system. The authors presented unique detection strategies for FDIA by employing thevenins equivalent parameters [48], an extremely randomised tree algorithm [70], and auto regressive models such as wavelet and TCN instead of the recurrent family model [33]. Not only FDIA, eavesdropping attack also one of the cyber security vulnerable attacks in smart communication system. Researchers developed a deep learning architecture [94], SVM [96], decomposition form of the system matrices [26], dual denoising auto-encoder based encryptor [82] and a certificate-less signcryption [114] to analyse impact and detect DoS, eavesdropping attacks. Furthermore, researchers utilised a zero-knowledge proofs & the pailiers crypto system [102], as well as a blockchain & homomorphic encryption based aggregation architecture [139], to minimise smart meter data manipulation attacks.

Based on presented literature, the following new findings are highlighted in the field of power systems cyber-attacks:

- FDIA's is one of the concerned attacks in power systems. Machine learning-based techniques such as extremely randomized tree and isolation forest could deliver accurate and fast detection of FDIAs with an accuracy of more than 99.75% and a detection time of less than 1.944 seconds, respectively. Because, false factor increases then detection time also increases.
- Cryptographic algorithms such as elliptic curve-based encryption incorporated with block chain, will facilitate electricity trading without the mediator as well as provide low computation cost for data aggregation. In addition, the kind of approach will provide authenticated security for deregulation energy markets such as TEMS, Demand Response.
- To satisfy the IEC 61850 protocols in the standard of IEC 62351, the control commands must transmit within 4ms between substation to circuit breakers. Hash function and private key based protocol can agree on the session key within 0.057ms, which satisfies the time restrictions of GOOSE and sampled value protocols and will provide private key privacy and session key security against communication attacks such as MITM, replay attack and DoS attack. Furthermore, RSASSA-PKCS-V1_5 fails to meet the timing standards of GOOSE messages, which may leads to revisit the IEC 62351-6 standard with new considerations for better cyber security.

### B. FUTURE DIRECTIONS

The comprehensive review has opened up new scopes in power systems cyber securities.

- Establishment of a detection approach based on dynamic watermarking to detect sophisticated adversaries that can be scaled up to large-scale power systems [36].
- A deep stacking auto-encoder technique can also be used to identify the root cause and implement appropriate control measures to prevent cyber intrusion between utilities and consumers in smart grid [62].
- Despite FDIA detection in smart grid, artificial feed-forward networks based on a true-data integrity agent model can be employed for cyber security in intelligent transportation systems [91].
- Merging of attributed-based signcryption with proxy re-encryption scheme to secure data from communication attacks in smart grid [114].
- A lightweight multiparty computation protocol based on blockchain that can also be suitable for resource-constrained networks like the smart grid [120].
- Blockchain technology can also provide better authentication protocols for the smart grid privacy protection [102].

The following research areas are suggested in the field of cyber-attacks in power systems based on existing research:

1) Development of decentralized defense system to identify and mitigate threats in renewable energies such as wind and photo-voltaic systems, based control networks using artificial intelligent control techniques that can be extend to large-scale power systems. Furthermore, evaluation of the impact of renewable energy power plants temporal characteristics and participation in power markets.
2) Development of effective strategies for analyzing the impact, detecting and protecting against cyber-attacks on state estimation (PMU, Direct Current, Alternative Current -High Voltage Direct Current) in transmission lines, as well as improving a framework for locating the events at each line.
3) Implementation of a framework to analyze a few realistic behaviours of agents, operators and electricity market mechanisms and the development of cyber security actions for data manipulation attacks and energy theft attacks using intelligent transportation in TES.
4) There is a need to analyze the impact of cyber-attacks such as DoS and MITM in various environments like peer-to-peer energy trading, M2M communication, TES, demand side management, and distribution side, as well as design the detection schemes and monitoring systems to identify meters that inject false power consumption data and to handle zero-day sort of attacks.
5) The scope of IoT- based smart grid projects is limited to closed environments (LAN, recursive internet working architecture). There is a need to extend the real-world smart grid infrastructures, such as the implementation and evaluation of a prototype in collaboration with smart grid operators or service providers, to analyze real-world data communication in smart grids.
6) Establishment of a lightweight authentication scheme to address specific cyber security challenges such as privacy of users and policy makers, reducing the protocol message size, lowering the computational cost

and shortening the time domains for a distributed secret-key management scheme. To enhance the privacy protection in smart grid communication channels blockchain technology shall be adopted.

## IX. CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

## REFERENCES

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[2] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3548–3557, May 2020.

[3] C. Ang. (2021). *The Most Cyber Attsignificant Acks From 2006-2020, by Country*. [Online]. Available: https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/

[4] M. Benmalek and Y. Challal, "MK-AMI: Efficient multi-group key management scheme for secure communications in AMI systems," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6.

[5] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094.

[6] R. E. Pérez-Guzmán, Y. Salgueiro-Sicilia, and M. Rivera, "Communication systems and security issues in smart microgrids," in *Proc. IEEE Southern Power Electron. Conf. (SPEC)*, Dec. 2017, pp. 1–6.

[7] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *Proc. Int. Conf. Artif. Intell. Data Process. (IDAP)*, Sep. 2018, pp. 1–5.

[8] H. Ritchie and M. Roser. (2018). *Two-Thirds of Global Population Will Live in Cities By 2050, Our World in Data*. [Online]. Available: https://ourworldindata.org/urbanization

[9] M. Benmalek, Y. Challal, and A. Derhab, "Authentication for smart grid AMI systems: Threat models, solutions, and challenges," in *Proc. IEEE 28th Int. Conf. Enabling Technologies: Infrastructure Collaborative Enterprises (WETICE)*, Jun. 2019, pp. 208–213.

[10] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine learning and deep learning approaches for cybersecuriy: A review," *IEEE Access*, vol. 10, pp. 19572–19585, 2022.

[11] A. Hasankhani, S. M. Hakimi, M. Bisheh-Niasar, M. Shafie-khah, and H. Asadolahi, "Blockchain technology in the future smart grids: A comprehensive review and frameworks," *Int. J. Electr. Power Energy Syst.*, vol. 129, Jul. 2021, Art. no. 106811.

[12] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electr. Power Syst. Res.*, vol. 215, Feb. 2023, Art. no. 108975.

[13] M. Abdalzaher, M. Fouda, A. Emran, Z. Fadlullah, and M. Ibrahem, "A survey on key management and authentication approaches in smart metering systems," *Energies*, vol. 16, no. 5, p. 2355, Mar. 2023.

[14] M. Sewak, S. K. Sahay, and H. Rathore, "Deep reinforcement learning in the advanced cybersecurity threat detection and protection," *Inf. Syst. Frontiers*, vol. 25, pp. 589–611, Aug. 2022.

[15] S. Banik, S. K. Saha, T. Banik, and S. M. M. Hossain, "Anomaly detection techniques in smart grid systems: A review," in *Proc. IEEE World AI IoT Congr. (AIIoT)*, Jun. 2023, pp. 331–337.

[16] J. Kua, M. B. Hossain, I. Natgunanathan, and Y. Xiang, "Privacy preservation in smart meters: Current status, challenges and future directions," *Sensors*, vol. 23, no. 7, p. 3697, Apr. 2023.

[17] K. Y. Yap, H. H. Chin, and J. J. Klemeš, "Blockchain technology for distributed generation: A review of current development, challenges and future prospect," *Renew. Sustain. Energy Rev.*, vol. 175, Apr. 2023, Art. no. 113170.

[18] S. S. Koduru, V. S. P. Machina, and S. Madichetty, "Cyber attacks in cyber-physical microgrid systems: A comprehensive review," *Energies*, vol. 16, no. 12, p. 4573, Jun. 2023.

[19] M. Lydia, G. E. P. Kumar, and A. I. Selvakumar, "Securing the cyber-physical system: A review," *Cyber-Phys. Syst.*, vol. 9, no. 3, pp. 193–223, Jul. 2023.

[20] S. Bhattacharjee and S. K. Das, "Detection and forensics against stealthy data falsification in smart metering infrastructure," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 1, pp. 356–371, Jan. 2021.

[21] X. Lou, "Learning-based time delay attack characterization for cyber-physical systems," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–6.

[22] A. Ameli, A. Ayad, E. F. El-Saadany, M. M. A. Salama, and A. Youssef, "A learning-based framework for detecting cyber-attacks against line current differential relays," *IEEE Trans. Power Del.*, vol. 36, no. 4, pp. 2274–2286, Aug. 2021.

[23] S. Yankson and M. Ghamkhari, "Transactive energy to thwart load altering attacks on power distribution systems," *Future Internet*, vol. 12, no. 1, p. 4, Dec. 2019.

[24] J. Khazaei, "Cyberattacks with limited network information leading to transmission line overflow in cyber–physical power systems," *Sustain. Energy, Grids Netw.*, vol. 27, Sep. 2021, Art. no. 100505.

[25] K. Wang, L. Yuan, T. Miyazaki, Y. Chen, and Y. Zhang, "Jamming and eavesdropping defense in green cyber–physical transportation systems using a Stackelberg game," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4232–4242, Sep. 2018.

[26] R. Gao and G.-H. Yang, "Sampled-data distributed state estimation with multiple transmission channels under denial-of-service attacks," *Appl. Math. Comput.*, vol. 429, Sep. 2022, Art. no. 127229.

[27] M. F. Moghadam, M. Nikooghadam, A. H. Mohajerzadeh, and B. Movali, "A lightweight key management protocol for secure communication in smart grids," *Electr. Power Syst. Res.*, vol. 178, Jan. 2020, Art. no. 106024.

[28] I. Staffell and S. Pfenninger, "The increasing impact of weather on electricity supply and demand," *Energy*, vol. 145, pp. 65–78, Feb. 2018.

[29] J. Staggs, D. Ferlemann, and S. Shenoi, "Wind farm security: Attack surface, targets, scenarios and mitigation," *Int. J. Crit. Infrastructure Protection*, vol. 17, pp. 3–14, Jun. 2017.

[30] J. Y. Siu and S. K. Panda, "A review of cyber-physical security in the generation system of the grid," in *Proc. IECON 46th Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2020, pp. 1520–1525.

[31] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo, W. Song, M. D. R. Greidanus, S. Sahoo, F. Blaabjerg, J. Zhang, L. Guo, B. Ahn, M. B. Shadmand, N. R. Gajanur, and M. A. Abbaszada, "A review of cyber–physical security for photovoltaic systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022.

[32] A. Jindal, A. K. Marnerides, A. Scott, and D. Hutchison, "Identifying security challenges in renewable energy systems: A wind turbine case study," in *Proc. 10th ACM Int. Conf. Future Energy Syst.*, Jun. 2019, pp. 370–372.

[33] F. Almutairy, L. Scekic, R. Elmoudi, and S. Wshah, "Accurate detection of false data injection attacks in renewable power systems using deep learning," *IEEE Access*, vol. 9, pp. 135774–135789, 2021.

[34] M. Ismail, M. F. Shaaban, M. Naidu, and E. Serpedin, "Deep learning detection of electricity theft cyber-attacks in renewable distributed generation," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3428–3437, Jul. 2020.

[35] N. Trantham and A. Garcia, "Reputation dynamics in networks: Application to cyber security of wind farms," *Syst. Eng.*, vol. 18, no. 4, pp. 339–348, Jul. 2015.

[36] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6816–6827, Nov. 2018.

[37] I. Gandhi, L. Ravi, V. Vijayakumar, and V. Subramaniyaswamy, "Improving security for wind energy systems in smart grid applications using digital protection technique," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102265.

[38] H. Jia, C. Shao, D. Liu, C. Singh, Y. Ding, and Y. Li, "Operating reliability evaluation of power systems with demand-side resources considering cyber malfunctions," *IEEE Access*, vol. 8, pp. 87354–87366, 2020.

[39] N. Fardad, S. Soleymani, and F. Faghihi, "Cyber defense analysis of smart grid including renewable energy resources based on coalitional game theory," *J. Intell. Fuzzy Syst.*, vol. 35, no. 2, pp. 2063–2077, Aug. 2018.

[40] S. Lee and J.-H. Huh, "An effective security measures for nuclear power plant using big data analysis approach," *J. Supercomput.*, vol. 75, no. 8, pp. 4267–4294, 2019.

[41] C. Lee, Y. Ho Chae, and P. H. Seong, "Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs," *Ann. Nucl. Energy*, vol. 158, Aug. 2021, Art. no. 108287.

[42] C. Lee, S. M. Han, Y. H. Chae, and P. H. Seong, "Development of a cyberattack response planning method for nuclear power plants by using the Markov decision process model," *Ann. Nucl. Energy*, vol. 166, Feb. 2022, Art. no. 108725.

[43] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors*, vol. 21, no. 18, p. 6225, Sep. 2021.

[44] H. Rahimpour, J. Tusek, A. Abuadbba, A. Seneviratne, T. Phung, A. Musleh, and B. Liu, "Cybersecurity challenges of power transformers," 2023, *arXiv:2302.13161*.

[45] R. Fan, J. Lian, K. Kalsi, and M. Elizondo, "Impact of cyber attacks on high voltage DC transmission damping control," *Energies*, vol. 11, no. 5, p. 1046, Apr. 2018.

[46] M. J. P. Jaghargh and H. R. Mashhadi, "Structural and behavioural evaluation of renewable energy power plants' impacts on transmission network congestion using an analytical approach," *IET Renew. Power Gener.*, vol. 14, no. 7, pp. 1164–1173, May 2020.

[47] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2017, pp. 1–6.

[48] M. Ghafouri, M. Au, M. Kassouf, M. Debbabi, C. Assi, and J. Yan, "Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5227–5238, Nov. 2020.

[49] D. Wilson, Y. Tang, J. Yan, and Z. Lu, "Deep learning-aided cyber-attack detection in power transmission systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[50] A. Ahmed, V. V. G. Krishnan, S. A. Foroutan, M. Touhiduzzaman, C. Rublein, A. Srivastava, Y. Wu, A. Hahn, and S. Suresh, "Cyber physical security analytics for anomalies in transmission protection systems," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 6313–6323, Nov. 2019.

[51] S. Chakrabarty and B. Sikdar, "Detection of hidden transformer tap change command attacks in transmission networks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5161–5173, Nov. 2020.

[52] S. Pal, B. Sikdar, and J. H. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 5057–5066, Sep. 2018.

[53] Q. Yang, L. Jiang, W. Hao, B. Zhou, P. Yang, and Z. Lv, "PMU placement in electric transmission networks for reliable state estimation against false data injection attacks," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1978–1986, Dec. 2017.

[54] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, M. Shasadeghi, N. Ghadimi, and F. Taghizadeh-Hesary, "Blockchain-based securing of data exchange in a power transmission system considering congestion management and social welfare," *Sustainability*, vol. 13, no. 1, p. 90, Dec. 2020.

[55] F. Mohammadi and R. Rashidzadeh, "Impact of stealthy false data injection attacks on power flow of power transmission lines—A mathematical verification," *Int. J. Electr. Power Energy Syst.*, vol. 142, Nov. 2022, Art. no. 108293.

[56] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Rep.*, vol. 7, pp. 7999–8012, Nov. 2021.

[57] X. G. Shan and J. Zhuang, "A game-theoretic approach to modeling attacks and defenses of smart grids at three levels," *Rel. Eng. Syst. Saf.*, vol. 195, Mar. 2020, Art. no. 106683.

[58] M. Montakhabi, A. Madhusudan, S. van der Graaf, A. Abidin, P. Ballon, and M. A. Mustafa, "Sharing economy in future peer-to-peer electricity trading markets: Security and privacy analysis," in *Proc. Workshop Decentralized IoT Syst. Secur. (DISS)*, San Diego, CA, USA, 2020, pp. 1–6.

[59] A. Marufu, A. V. Kayem, and S. D. Wolthusen, "The design and classification of cheating attacks on power marketing schemes in resource constrained smart micro-grids," in *Smart Micro-Grid Systems Security and Privacy*. Cham, Switzerland: Springer, 2018, pp. 103–144.

[60] R. Dasgupta, A. Sakzad, and C. Rudolph, "Cyber attacks in transactive energy market-based microgrid systems," *Energies*, vol. 14, no. 4, p. 1137, Feb. 2021.

[61] A. Arman, V. V. G. Krishnan, A. Srivastava, Y. Wu, and S. Sindhu, "Cyber physical security analytics for transactive energy systems using ensemble machine learning," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2018, pp. 1–6.

[62] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 931–941, Mar. 2020.

[63] P. Wang, K. Ma, J. Lian, and D. J. Hammerstrom, "On anomaly detection for transactive energy systems with competitive market," *Int. J. Electr. Power Energy Syst.*, vol. 128, Jun. 2021, Art. no. 106662.

[64] S. Fkaier, M. Khalgui, G. Frey, Z. Li, and J. Yu, "Secure distributed power trading protocol for networked microgrids based on blockchain and elliptic curve cryptography," *IET Smart Grid*, vol. 6, no. 2, pp. 175–189, Apr. 2023.

[65] S. Pal, S. Biswas, S. Sridhar, A. Ashok, J. Hansen, and V. Amatya, "Understanding impacts of data integrity attacks on transactive control systems," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2020, pp. 1–5.

[66] V. V. G. Krishnan, Y. Zhang, K. Kaur, A. Hahn, A. Srivastava, and S. Sindhu, "Cyber-security analysis of transactive energy systems," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo. (T&D)*, Apr. 2018, pp. 1–9.

[67] Q. Huang, T. E. McDermott, Y. Tang, A. Makhmalbaf, D. J. Hammerstrom, A. R. Fisher, L. D. Marinovici, and T. Hardy, "Simulation-based valuation of transactive energy systems," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 4138–4147, Sep. 2019.

[68] Y. Liu, S. Hu, and T.-Y. Ho, "Leveraging strategic detection techniques for smart home pricing cyberattacks," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 2, pp. 220–235, Mar. 2016.

[69] Y. Song, Z. Yu, X. Liu, J. Tian, and M. Chen, "Isolation forest based detection for false data attacks in power systems," in *Proc. IEEE Innov. Smart Grid Technol. Asia (ISGT Asia)*, May 2019, pp. 4170–4174.

[70] S. H. Majidi, S. Hadayeghparast, and H. Karimipour, "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid," *Int. J. Crit. Infrastruct. Protection*, vol. 37, Jul. 2022, Art. no. 100508.

[71] C.-C. Sun, D. J. Sebastian Cardenas, A. Hahn, and C.-C. Liu, "Intrusion detection for cybersecurity of smart meters," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612–622, Jan. 2021.

[72] P. A. Giglou and S. N. Ravadanegh, "Defending against false data injection attack on demand response program: A bi-level strategy," *Sustain. Energy, Grids Netw.*, vol. 27, Sep. 2021, Art. no. 100506.

[73] S. Ahmadian, X. Tang, H. A. Malki, and Z. Han, "Modelling cyber attacks on electricity market using mathematical programming with equilibrium constraints," *IEEE Access*, vol. 7, pp. 27376–27388, 2019.

[74] J. Tao and G. Michailidis, "A statistical framework for detecting electricity theft activities in smart grid distribution networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 205–216, Jan. 2020.

[75] K. Yang, H. Wang, H. Wang, and L. Sun, "An effective intrusion-resilient mechanism for programmable logic controllers against data tampering attacks," *Comput. Ind.*, vol. 138, Jun. 2022, Art. no. 103613.

[76] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, Jun. 2018.

[77] P. Gope, "PMAKE: Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid," *Comput. Commun.*, vol. 152, pp. 338–344, Feb. 2020.

[78] X. Lou, C. Tran, R. Tan, D. K. Y. Yau, Z. T. Kalbarczyk, A. K. Banerjee, and P. Ganesh, "Assessing and mitigating impact of time delay attack: Case studies for power grid controls," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 141–155, Jan. 2020.

[79] M. Attia, S. M. Senouci, H. Sedjelmaci, E.-H. Aglzim, and D. Chrenko, "An efficient intrusion detection system against cyber-physical attacks in the smart grid," *Comput. Electr. Eng.*, vol. 68, pp. 499–512, May 2018.

[80] M. R. C. Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," *IEEE Access*, vol. 8, pp. 19921–19933, 2020.

[81] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[82] S. Wu, Y. Jiang, H. Luo, and X. Li, "Deep learning-based defense and detection scheme against eavesdropping and typical cyber-physical attacks," in *Proc. CAA Symp. Fault Detection, Supervision, Saf. Tech. Processes (SAFEPROCESS)*, Dec. 2021, pp. 1–6.

[83] I. Aziz, H. Jin, I. Abdulqadder, Z. Hussien, Z. Abduljabbar, and F. Flaih, "A lightweight scheme to authenticate and secure the communication in smart grids," *Appl. Sci.*, vol. 8, no. 9, p. 1508, Sep. 2018.

[84] G. Tertytchny, N. Nicolaou, and M. K. Michael, "Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103121.

[85] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F. J. Aparicio-Navarro, A. Argyriou, and H. Janicke, "A novel intrusion detection system against spoofing attacks in connected electric vehicles," *Array*, vol. 5, Mar. 2020, Art. no. 100013.

[86] A. O. Aluko, R. P. Carpanen, D. G. Dorrell, and E. E. Ojo, "Real-time cyber attack detection scheme for standalone microgrids," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21481–21492, Nov. 2022.

[87] B. Huang, M. Majidi, and R. Baldick, "Case study of power system cyber attack using cascading outage analysis model," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[88] N. Kumar, V. M. Mishra, and A. Kumar, "Smart grid security by embedding S-Box advanced encryption standard," *Intell. Autom. Soft Comput.*, vol. 34, no. 1, pp. 623–638, 2022.

[89] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *J. Netw. Comput. Appl.*, vol. 209, Jan. 2023, Art. no. 103540.

[90] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: A trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network," *Secur. Commun. Netw.*, vol. 2021, pp. 1–9, Apr. 2021.

[91] S. Sengan, V. Subramaniyaswamy, V. Indragandhi, P. Velayutham, and L. Ravi, "Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning," *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107211.

[92] G. D. L. T. Parra, P. Rad, K.-K.-R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *J. Netw. Comput. Appl.*, vol. 163, Aug. 2020, Art. no. 102662.

[93] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, and G. Cao, "Deep learning aided interval state prediction for improving cyber security in energy internet," *Energy*, vol. 174, pp. 1292–1304, May 2019.

[94] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Proc. Comput. Sci.*, vol. 185, no. 1, pp. 239–247, 2021.

[95] R. B. Benisha and S. R. Ratna, "Detection of data integrity attacks by constructing an effective intrusion detection system," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 11, pp. 5233–5244, Nov. 2020.

[96] T. M. Hoang, T. Q. Duong, H. D. Tuan, S. Lambotharan, and L. Hanzo, "Physical layer security: Detection of active eavesdropping attacks by support vector machines," *IEEE Access*, vol. 9, pp. 31595–31607, 2021.

[97] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragicevic, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[98] Y. Taniguchi, H. Tsutsumi, N. Iguchi, and K. Watanabe, "Design and evaluation of a proxy-based monitoring system for OpenFlow networks," *Sci. World J.*, vol. 2016, pp. 1–10, Jan. 2016.

[99] Y. Huang, L. Jin, Z. Zhong, Y. Lou, and S. Zhang, "Detection and defense of active attacks for generating secret key from wireless channels in static environment," *ISA Trans.*, vol. 99, pp. 231–239, Apr. 2020.

[100] A. Tolba and Z. Al-Makhadmeh, "A cybersecurity user authentication approach for securing smart grid communications," *Sustain. Energy Technol. Assessments*, vol. 46, Aug. 2021, Art. no. 101284.

[101] M. Sirajuddin, C. Rupa, S. Bhatia, R. N. Thakur, and A. Mashat, "Hybrid cryptographic scheme for secure communication in mobile ad hoc network-based E-healthcare system," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–8, Jun. 2022.

[102] X. Xiang and J. Cao, "An efficient authenticated key agreement scheme supporting privacy-preservation for smart grid communication," *Electric Power Syst. Res.*, vol. 203, Feb. 2022, Art. no. 107630.

[103] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

[104] A. A. Khan, S. Itoo, V. Kumar, M. Ahmad, and S. Jangirala, "Cryptanalysis and design flaws of anonymous ECC based self-certified key distribution scheme for smart grid," *Mater. Today, Proc.*, vol. 57, pp. 2185–2189, Jan. 2022.

[105] J. Srinivas, A. K. Das, X. Li, M. K. Khan, and M. Jo, "Designing anonymous signature-based authenticated key exchange scheme for Internet of Things-enabled smart grid systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 4425–4436, Jul. 2021.

[106] K. Mahmood, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, Nov. 2018.

[107] C. Guo, X. Jiang, K.-K. R. Choo, X. Tang, and J. Zhang, "Lightweight privacy preserving data aggregation with batch verification for smart grid," *Future Gener. Comput. Syst.*, vol. 112, pp. 512–523, Nov. 2020.

[108] A. Braeken, P. Kumar, and A. Martin, "Efficient and provably secure key agreement for modern smart metering communications," *Energies*, vol. 11, no. 10, p. 2662, 2018.

[109] T. Chen, X. Yin, and G. Wang, "Securing communications between smart grids and real users; providing a methodology based on user authentication," *Energy Rep.*, vol. 7, pp. 8042–8050, Nov. 2021.

[110] P. M. Lima, L. K. Carvalho, and M. V. Moreira, "Confidentiality of cyber-physical systems using event-based cryptography," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 1735–1740, 2020.

[111] N. B. Samyuel and B. A. Shimray, "Securing IoT device communication against network flow attacks with recursive internetworking architecture (RINA)," *ICT Exp.*, vol. 7, no. 1, pp. 110–114, Mar. 2021.

[112] A. N. Nazarov and A. N. A. Koupaei, "An architecture model for active cyber attacks on intelligence info-communication systems: Application based on advance system encryption (AES-512) using pre-encrypted search table and pseudo-random Functions(PRFs)," in *Proc. Int. Conf. Eng. Telecommun. (EnT)*, Nov. 2019, pp. 1–5.

[113] M. A. Elakrat and J. C. Jung, "Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network," *Nucl. Eng. Technol.*, vol. 50, no. 5, pp. 780–787, Jun. 2018.

[114] E. Ahene, Z. Qin, A. K. Adusei, and F. Li, "Efficient signcryption with proxy re-encryption and its application in smart grid," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9722–9737, Dec. 2019.

[115] Z. Wang, Y. Liu, Z. Ma, X. Liu, and J. Ma, "LiPSG: Lightweight privacy-preserving Q-learning-based energy management for the IoT-enabled smart grid," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3935–3947, May 2020.

[116] I. A. Kamil and S. O. Ogundoyin, "EPDAS: Efficient privacy-preserving data analysis scheme for smart grid network," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 33, no. 2, pp. 208–217, 2021.

[117] G. K. Verma, P. Gope, and N. Kumar, "PF-DA: Pairing free and secure data aggregation for energy internet-based smart meter-to-grid communication," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2294–2304, May 2022.

[118] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for Internet of Things-based energy Internet," *Future Gener. Comput. Syst.*, vol. 93, pp. 849–859, Apr. 2019.

[119] P. M. Lima, M. V. S. Alves, L. K. Carvalho, and M. V. Moreira, "Security against communication network attacks of cyber-physical systems," *J. Control, Autom. Electr. Syst.*, vol. 30, no. 1, pp. 125–135, Feb. 2019.

[120] S. Aghapour, M. Kaveh, M. R. Mosavi, and D. Martín, "An ultra-lightweight mutual authentication scheme for smart grid two-way communications," *IEEE Access*, vol. 9, pp. 74562–74573, 2021.

[121] B. K. Sethi, A. Singh, D. Singh, and R. Misra, "Optimal energy m anagement of s mart b uildings under cyber attack," *Int. J. Energy Res.*, vol. 45, no. 14, pp. 19895–19908, Nov. 2021.

[122] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages," *IEEE Access*, vol. 7, pp. 32343–32351, 2019.

[123] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.

[124] P. Gope and B. Sikdar, "A privacy-aware reconfigurable authenticated key exchange scheme for secure communication in smart grids," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5335–5348, Nov. 2021.

[125] M. Tahavori and F. Moazami, "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid," *Peer Peer Netw. Appl.*, vol. 13, no. 5, pp. 1616–1628, Sep. 2020.
[126] M. Kaveh and M. R. Mosavi, "A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4535–4544, Sep. 2020.
[127] H. M. Ibrahim, H. Abunahla, B. Mohammad, and H. AlKhzaimi, "Memristor-based PUF for lightweight cryptographic randomness," *Sci. Rep.*, vol. 12, no. 1, pp. 1–18, May 2022.
[128] H. Kishimoto, N. Yanai, and S. Okamura, "An anonymous authentication protocol for the smart grid," in *Smart Micro-Grid Systems Security and Privacy*. Cham, Switzerland: Springer, 2018, pp. 29–52.
[129] M. Tanveer, A. U. Khan, H. Shah, A. Alkhayyat, S. A. Chaudhry, and M. Ahmad, "ARAP-SG: Anonymous and reliable authentication protocol for smart grids," *IEEE Access*, vol. 9, pp. 143366–143377, 2021.
[130] T. Limbasiya and A. Arya, "Attacks on authentication and authorization models in smart grid," in *Smart Micro-Grid Systems Security and Privacy*. Cham, Switzerland: Springer, 2018, pp. 53–70.
[131] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K.-R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *J. Parallel Distrib. Comput.*, vol. 132, pp. 242–249, Oct. 2019.
[132] D. Sadhukhan, S. Ray, M. S. Obaidat, and M. Dasgupta, "A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography," *J. Syst. Archit.*, vol. 114, Mar. 2021, Art. no. 101938.
[133] M. Qi and J. Chen, "Two-pass privacy preserving authenticated key agreement scheme for smart grid," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3201–3207, Sep. 2021.
[134] P. Gope, "Anonymous mutual authentication with location privacy support for secure communication in M2M home network services," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 1, pp. 153–161, Jan. 2019.
[135] V. Sureshkumar, S. Anandhi, R. Amin, N. Selvarajan, and R. Madhumathi, "Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3565–3572, Sep. 2021.
[136] A. Irshad, S. A. Chaudhry, M. Alazab, A. Kanwal, M. S. Zia, and Y. B. Zikria, "A secure demand response management authentication scheme for smart grid," *Sustain. Energy Technol. Assessments*, vol. 48, Dec. 2021, Art. no. 101571.
[137] S. Yu, K. Park, J. Lee, Y. Park, Y. Park, S. Lee, and B. Chung, "Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment," *Appl. Sci.*, vol. 10, no. 5, p. 1758, Mar. 2020.
[138] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, "ECCAuth: A secure authentication protocol for demand response management in a smart grid system," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6572–6582, Dec. 2019.
[139] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107209.
[140] W. Wang, H. Huang, L. Zhang, Z. Han, C. Qiu, and C. Su, "BlockSLAP: Blockchain-based secure and lightweight authentication protocol for smart grid," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1332–1338.
[141] M. Stănculescu, S. Deleanu, P. C. Andrei, and H. Andrei, "A case study of an industrial power plant under cyberattack: Simulation and analysis," *Energies*, vol. 14, no. 9, p. 2568, Apr. 2021.
[142] H. S. Cho and T. H. Woo, "Cyber security in nuclear industry—Analytic study from the terror incident in nuclear power plants (NPPs)," *Ann. Nucl. Energy*, vol. 99, pp. 47–53, Jan. 2017.
[143] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1035–1044, Feb. 2020.
[144] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, "Consumer, commercial, and industrial IoT (in) security: Attack taxonomy and case studies," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 199–221, Jan. 2021.
[145] D. Tripathi, A. K. Tripathi, L. K. Singh, and A. Chaturvedi, "Towards analyzing the impact of intrusion prevention and response on cyber-physical system availability: A case study of NPP," *Ann. Nucl. Energy*, vol. 168, Apr. 2022, Art. no. 108863.
[146] S. Hossain-McKenzie, A. Chavez, N. Jacobs, C. B. Jones, A. Summers, and B. Wright, "Proactive intrusion detection and mitigation system: Case study on packet replay attacks in distributed energy resource systems," in *Proc. IEEE Power Energy Conf. Illinois (PECI)*, Apr. 2021, pp. 1–6.

**NAVEEN TATIPATRI** received the B.Tech. degree in electrical and electronics engineering and the M.Tech. degree in power systems from Jawaharlal Nehru Technological University (JNTU), Anantapur, Andhra Pradesh, India, in 2017 and 2020, respectively. He is currently pursuing the Ph.D. degree with the School of Electrical Engineering, VIT, Vellore. His research interests include transactive energy management systems and cyber security for communication channel attacks in power systems.

**S. L. ARUN** received the B.E. degree in electrical and electronics engineering from the Institute of Road and Transport Technology, Erode, India, in 2010, the M.Tech. degree in power systems from NIT Calicut, Kerala, India, in 2013, and the Ph.D. degree in electrical engineering from NIT Tiruchirappalli, India, in 2019. He is currently an Assistant Professor with the School of Electrical Engineering, VIT, Vellore, India. He has published many research papers in reputed international journals and international and national conferences. His research and teaching interests include smart grid technology, demand response, P2P energy transactions, cyber security for smart grid, power system analysis, operation and control, distributed generation, and micro-grid.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 31 August 2022, accepted 15 November 2022, date of publication 15 December 2022, date of current version 19 January 2023.

*Digital Object Identifier 10.1109/ACCESS.2022.3229766*

SURVEY

# Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review

**MOHAMED NOORDIN YUSUFF MARICAN[1], SHUKOR ABD RAZAK[2], (Senior Member, IEEE), ALI SELAMAT[1,3,4,5], (Member, IEEE), AND SITI HAJAR OTHMAN[1], (Member, IEEE)**

[1]Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[2]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Kuala Terengganu 21300, Malaysia
[3]Malaysia-Japan Institute of Technology, Universiti Teknologi Malaysia, Kuala Lumpur 54100, Malaysia
[4]MaGICX–Media and Game Innovation Centre of Excellence, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[5]Faculty of Informatics and Management, University of Hradec Kralove, Hradec Kralove 50003, Czech Republic

Corresponding author: Ali Selamat (aselamat@utm.my)

The author would like to acknowledge the financial support from the Ministry of Higher Education under the Fundamental Research Grant Scheme (FRGS) (FRGS/1/2022/ICT08/UTM/01/1).

**ABSTRACT** Cybersecurity has gained increasing importance among firms of different sizes and industries due to the significant rise of cyber-attacks over time. Technology startups are particularly vulnerable to cyber-attacks due to the lack of cyber security measures. This is because of limited human capital and financial resources to quantify cyber risks and allocate appropriate investments to cyber security. Technology startups are suppliers and vendors to large organisations such as MNCs, government and financial institutions. They could possibly have a network connection back to the large organisations and might even store confidential information of these large organisations such as financial records, personal data and other proprietary information. As such, with the lack of appropriate cyber security measures, technology startups may be an attack vector for malicious hackers to gain entry to the large organisations. Focusing on technology startups, this study conducted a systematic literature review on cyber security maturity assessment frameworks. This study addressed five research questions on the existing cyber security maturity assessment frameworks in various industries, the target for implementation, cyber security maturity level, shared control domains of these frameworks, and the quantification of the return of cyber security investments. Referring to the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) checklist, a detailed analysis was performed on 24 published research articles (out of 650) from reputable journals and conference proceedings from January 2011 to June 2022. The results revealed the lack of an end-to-end cyber security maturity assessment framework for technology startups. Despite the similarities in the cyber security maturity level for certain frameworks, the results revealed no singular framework that can evaluate the cyber security maturity level of technology startups. The results further revealed the lack of studies on the quantification of the return of cyber security investments in an end-to-end cyber security maturity assessment framework for technology startups. This put the startup in a vulnerable position since management is not able to obtain relevant data on the startup's cyber maturity posture and without such information, they are not able to appropriately justify their security investments to mitigate the evolving cyber risks.

**INDEX TERMS** Cyber security risk, cyber security maturity, cyber security framework, cyber risk quantification, return of security investment, technology startup.

## I. INTRODUCTION

Following the growing connectivity in this digital era, the occurrence of cyber-attacks has continued to increase tremendously. There are different cyber-attacks, such as ransomware attacks, distributed denial of service, phishing, and exploiting vulnerable web and mobile applications. Taking the case of the Southeast Asian region, Singapore encountered a significant increase in cyber-attacks on a weekly basis, with an annual increase of 145% in 2021 [1]. The number of

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

cyber-attacks has increased inevitably; it is only a matter of time before these attacks occur since anyone with the knowledge of hacking can execute malicious intentions. Being a victim of a cyber-attack is financially taxing which may cost businesses thousands of dollars in recent times [2]. Therefore, it is crucial for the cyber security functions in organisations to have the capability in addressing the potential cyber security threats on a timely basis.

Cyber risks critically affect businesses following widespread cyber-attack cases [3]. Organisations of different sizes, small and medium enterprises (SMEs) or multinational companies (MNCs) are susceptible to these attacks. The size of an SME is no different from a startup [4]. The substantial effects of cyber-attacks in terms of revenues and clients' trust have positioned cyber risks as the top agenda during board meetings. An SME in Singapore reports annual revenue of $100 million or has less than 200 employees [5]. The effects of cyber-attacks are more critical for startups. Startups have limited financial resources to invest in cybersecurity, which makes them more vulnerable to cyber-attacks [6]. Poor security measures put startups at higher risk against these attacks, which have made it particularly challenging for startup founders to gain clients' trust, especially with the rising cases of cyber-attacks [7].

Cyber security issues are no longer an information technology (IT) problem. It has now become a business risk which should be handled with due care at the highest level in the organisation. Most malicious perpetrators have shifted their focus to smaller organisations since they are easier targets than larger organisations [6]. The smaller organisations do not have adequate financial resources to strengthen their information security capabilities in order to protect the business [8]. Smaller organisations like technology startups need to allocate the appropriate investments to implement the required security measures to combat against these cyber threats. The significance of cyber security has propelled the need to establish a specific framework that can help businesses to recognise, prevent, respond, and recover from cyber-attacks [9]. Implementing a cyber security maturity assessment (CSMA) framework equips businesses to deal with cyber threats. Startups demonstrate low cyber security maturity levels due to their lack of cyber security measures, making them susceptible to cyber-attacks [10]. Thus, it is imperative to determine the cyber security maturity level in order to comprehend the current and target maturity level so that startups are able to implement the appropriate cyber security measures to deal with cyber-attacks based on the identified gaps uncovered during the cyber security maturity assessment.

Focusing on technology startups, the current study aims to review the existing CSMA frameworks that are commonly used by cyber security practitioners in the industry. This study specifically examined the comprehensiveness of these frameworks from an end-to-end perspective to assess cyber risks, determining cyber security maturity levels and quantifying the returns of cyber investments for technology startups. Moreover, this study compared the existing and commonly-used cyber security frameworks, underlined their common features and extrapolated the key control domains which can be streamlined to conduct a cyber security maturity assessment for technology startups in a more effective manner. The objective is to provide management with the information to make a more informed decision so that the right amount of investment can be allocated to implement cyber security solutions for the technology startup in order to mitigate the cyber security risks. With the appropriate security measures in place, this will give added protection for the startup to mitigate against cyber-attacks by malicious threat actors.

## II. BACKGROUND AND RELATED WORKS

Cybersecurity is one of the most effective methods to counter business risk [3] and is a key determinant in the decision-making process at the organisational level [11]. As of January 2022, there were more than 3,800 startups in Singapore [12]. The Ponemon Institute conducted a survey and revealed that the majority of SMEs experienced cyber-attacks (66%) and data breaches (63%) in the past 12 months [13]. These attacks affected the financial standing, operations, and reputation of organisations. The increasing connectivity and the upsurge of digital transformation initiatives have created a thriving environment for malicious perpetrators, increasing the rate of cyber-attacks. This has called for the need to establish CSMA frameworks and standards in the industry [11].

Various CSMA frameworks are available for cyber security practitioners in the industry to evaluate the cyber security maturity of organisations. Through these existing frameworks, organisations' current cyber security maturity level can be determined to establish a roadmap towards attaining the desired maturity level. Despite the importance of a cyber security framework against cyber-attacks for organisations [8], startups experience difficulties developing an appropriate framework for building up their cyber security maturity [11]. Without a clear framework, technology startups cannot invest properly in the suitable security measures. Poorly executed security measures result in poor cyber security, which reflects a low cyber security maturity level. Organisations can defend themselves from cyber-attacks that cause data breaches and financial losses by investing in the latest security measures [14].

### A. CYBER SECURITY FRAMEWORKS

There are existing cyber security frameworks used by industry practitioners to assess cyber risks and determine the cyber security maturity posture of their organisations. Some of the commonly-used cyber security frameworks include the National Institute of Standards and Technology (NIST), International Organisation for Standardization (ISO) 27001, Control Objectives for Information and Related Technologies (COBIT 5), Cyber Security Capability Maturity Model (C2M2), Capability Maturity Model Integration (CMMI). However, these frameworks lack the end-to-end structure on

assessing cyber risks, determining the cyber security maturity levels and quantifying the returns of security investments based on the mitigation measures. Technology startups do not have the budget to invest in cyber security [7]. As such, the ability to obtain an end-to-end viewpoint on the cyber maturity posture will allow management to make proper decisions on the investment that they make to implement cyber security measures. In order to do this, the ability to assess cyber risks, determining the cyber security maturity level and quantifying the returns of security investments are necessary to be included in the end-to-end framework.

The existing cyber security frameworks are also generally used in traditional setups. The control objectives in the frameworks are broad and aplenty which take a significant amount of time (e.g., 3 to 6 months) to complete. Technology startups are known to be lean and agile, and build products with speed through innovation [41]. Thus, they do not have the luxury of time to complete a cyber security assessment which takes 3 to 6 months. As such, the control objectives in the cyber security frameworks need to be more streamlined and focused for technology startup. With a leaner framework for technology startup, this will assist in shortening the time frame to complete the cyber security assessment.

### B. CYBER SECURITY MATURITY LEVELS

Cyber Security Maturity Levels help technology startups to determine their current and target maturity level [28]. It provides a good understanding for the startup to determine their existing cyber security posture and the gaps which need to be remediated in order to achieve their target maturity level. Knowing the cyber security maturity levels help cyber security practitioners to better manage the security of their organisations. According to [30], 12 cyber security maturity models have been identified between 3 to 5 maturity levels. From a maturity scale of 1 to 5, a startup with level 1 in the maturity scale has the lowest cyber security posture with very weak cyber defences which make the company susceptible to cyber-attacks. On the other hand, a startup with a 4 in the maturity scale have an above average cyber security posture with strong defences against malicious perpetrators.

The cyber security maturity level is determined by the number of effective cyber security and data protection controls implemented in the organisation. The number of effective cyber security and data protection controls is in turn determined by the amount of cyber security investments that have been allocated to mitigate cyber risks identified in the organisation. Knowing the cyber security maturity levels is important especially for technology startups as it helps management to appropriately cater cyber security investments so that they can right-size their cyber security measures depending on the current and target maturity level of the startup.

Cyber security frameworks have been extensively explored and discussed in the literature. However, end-to-end cyber security maturity assessment frameworks for SMEs, especially technology startups, have not been systematically reviewed, which is addressed in the current study. Focusing on technology startups, this study presented a comprehensive overview of the cyber security maturity assessment framework and a quantification approach to determine the return of cyber security investments. The end-to end framework will help technology startups to effectively review risks, appropriately identify the cyber security maturity level and provide management with sufficient data to make decisions in justifying investments related to cyber security. With such a framework, this will help technology startups to secure their enterprise against cyber-attacks and reduce the risk of becoming an attack vector to their clients which can be organisations such as MNCs, governments and financial institutions.

## III. SYSTEMATIC LITERATURE REVIEW

The systematic literature review (SLR) can determine future research in a particular field. SLR helps researchers to obtain a firm grasp of the field of study and recognize the current research trends and gaps [16]. SLR must be comprehensively methodologically performed with rigor to eliminate bias. It should be beyond a collection of research articles; these research articles should be analytically and objectively reviewed and summarised [17]. With that, SLR was performed in this study to identify, evaluate, and summarise the findings of prior studies within a particular field of study [15].

For this study's SLR, several research questions were clearly established:

1) What cyber security maturity assessment (CSMA) frameworks are available for use in various industries?
2) Are these existing CSMA frameworks targeted for implementation in technology startups?
3) Do these existing CSMA frameworks determine the cyber security maturity level?
4) What are the shared control domains among these existing CSMA frameworks?
5) Do the existing CSMA frameworks incorporate the quantification of the return of cyber security investments?

This study gathered research articles from the following digital databases: IEEE explore (ieeexplore.ieee.org); Scopus (www.scopus.com); Springer (www.springer.com); Web of Science (http://apps.webofknowledge.com). This study targeted research articles from January 2011 to June 2022 using the following keywords: ''Cyber Security Maturity Assessment Model''; ''Cyber Security Maturity Assessment Framework''; ''Cyber Security Maturity Assessment''; ''Cyber Security Maturity Assessment'' AND ''Technology Startup''; ''Cyber Security Maturity Assessment Framework'' AND ''Technology Startup''; Cyber Security Maturity Assessment Model'' AND ''Technology Startup''; ''Cyber Security Maturity Assessment'' AND ''SME''; ''Cyber Security Maturity Assessment Framework'' AND ''SME''; ''Cyber Security Maturity Assessment Model'' AND ''SME''; ''Cyber Security Maturity Assessment'' AND ''Startup''; ''Cyber Security Maturity

**TABLE 1.** Inclusion and exclusion criteria.

| S/N | Inclusion Criteria | Exclusion Criteria |
|---|---|---|
| 1 | Cyber security maturity assessment framework/model in technology startups | Research articles on cyber security maturity assessment framework/model with no reference to assessing cyber risks |
| 2 | Cyber security maturity assessment framework/model in startups | Research articles on cyber risk assessment framework/model with no reference to assessing cyber security maturity |
| 3 | Cyber maturity assessment framework or model for SMEs | Research articles with no reference to cyber security maturity assessment or cyber risk assessment |
| 4 | Only research articles written in English | Research articles written in languages other than English |
| 5 | Cyber security maturity assessment in various industry sectors and different organisational types | Unpublished articles, theses, references, or textbooks |
| 6 | Related research articles published between January 2011 to June 2022 | Related research articles published before January 2011 |

Assessment Framework'' AND ''Startup''; ''Cyber Security Maturity Assessment Model'' AND ''Startup''. As SMEs and startups share similar size [5], the search included ''SME'' to cover all related small businesses.

Table 1 summarises the inclusion and exclusion criteria of this study to ensure a targeted search with respect to the research questions. All selected research articles were saved in Mendeley (www.mendeley.com), which is a reference management software that manages scholarly publications.

The PRISMA methodology, which incorporates an evidence-based minimum set of items, was employed in this study for efficient reporting of systematic reviews and meta-analyses. Figure 1 presents this study's PRISMA flowchart [18].

Based on the keywords used in the systematic literature review, this study identified 1,772 (including duplicates) research articles published in IEEE explore, Scopus, Springer, and Web of Science using the described search strings in the identification stage. There were 51 articles extracted from IEEE Explore, 175 from Scopus, 74 from Web of Science and 1472 from Springer as shown in Figure 1.

The initial screening retained a total of 620 research articles after all duplicates were removed. The screening process further excluded a total of 550 research articles according to the inclusion and exclusion criteria that have been identified as per Table 1.

The abstracts of the remaining 70 research articles were then reviewed which excluded 27 research articles. Although the excluded research articles consisted of relevant keywords in the title, abstract, and content, these research articles

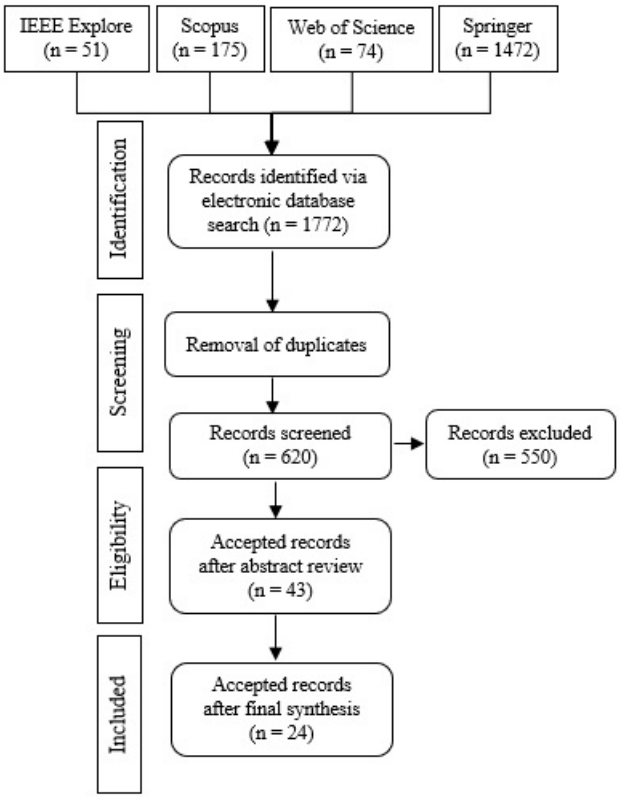



**FIGURE 1.** PRISMA flowchart.

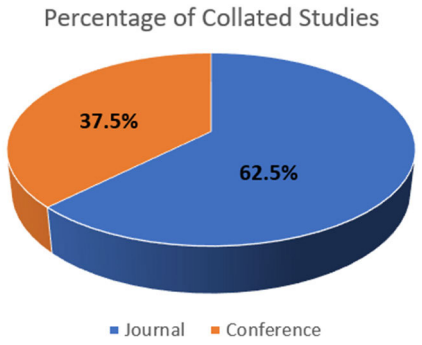



**FIGURE 2.** Percentage of collated studies.

focused on cyber risk with no context of cyber security maturity and vice versa. These research articles also did not address this study's research questions. After the final synthesis, 24 research articles have been accepted for an in-depth analysis.

### A. OVERVIEW OF SELECTED STUDIES

24 articles were selected for this research. Among them, 9 papers appeared in conference proceedings while 13 papers were published in journals. The numbers in percentages are represented in Figure 2.

Figure 3 shows the number of papers by year of publication based on the 24 papers that have been selected in this systematic literature review. The graph indicates that there

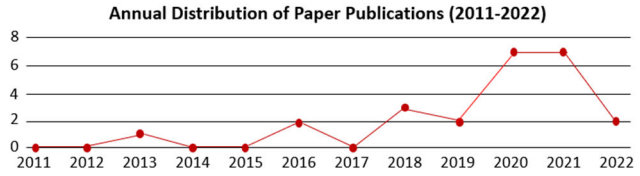



**FIGURE 3.** Number of papers by year of publication.

is an increase of publication from 2019 onwards. The low distribution of papers in 2022 was as of 31 Aug.

## IV. THREATS TO VALIDITY

The potential biasness and the data extraction in an imprecise manner could constrain our findings and pose a major threat to how this SLR is conducted. The four common threats to validity have been taken into account: constructing validity, internal validity, external validity and conclusion validity [40]. Initially, the search terms used may not be able to extract all relevant papers in the identified databases, but manual scrutiny was conducted in the reference section of each paper to further drill down and extract the papers that fall under the research area's realm. An independent evaluation of each of the 43 papers was conducted to ensure relevance to the research area and questions. The selection of the 24 journal papers was conducted as per the PRISMA guidelines [18] to reduce the risk of missing relevant papers and ensure the selected papers can address the research questions and consider the inclusion and exclusion criteria. Several combinations of the search terms were used to avoid the accidental exclusion of relevant papers. Following the PRISMA guidelines provide reasonable assurance, without bias and using the objective criteria, the selected and reviewed papers are among the most relevant studies related to the research area and relevant to the research questions that have been determined.

## V. FINDINGS

Data extraction is conducted based on the analysis of the keywords in the 24 selected papers and depicted in Figure 2 below using the VOSviewer software. The VOSviewer helped to identify the keywords which appeared most often in the articles and the links between the authors of the articles. The bigger bubbles showed the keywords which appeared most often.

This analysis is required to gather the results of the research in order to address the research questions (RQs) which have been determined for this systematic literature review. Data extraction was performed on the selected research articles (n=24), and the results are discussed with respect to this study's research questions (RQs).

*RQ1: What are the cyber security maturity assessment (CSMA) frameworks available for use in various industries?*

Table 2 presents the identified CSMA frameworks from all 24 research articles, which were identified as available for use in various industries across different countries. A few research articles highlighted the same CSMA framework. For instance, seven research articles [25], [28], [30], [32], [33], [35], [37] focused on the Cyber Security Capability Maturity Model (C2M2), whereas four research articles [27], [9], [33], [37] utilized the Control Objectives for Information and Related Technologies (COBIT) Framework. Several research articles also repeated and described the same framework in their literature review.

*RQ2: Are these CSMA frameworks targeted for implementation in technology startups?*

The analysis further revealed only one CSMA framework [28] was targeted for implementation in technology startups, which proved the lack of a CSMA framework for technology startups. In the research article entitled "Adoption of COBIT 5 Framework in Risk Management for Startup Company", a risk management model was described concerning the processes of the COBIT 5 Framework. Considering that SMEs and startups are similar in terms of size [5], seven other research articles that focused on CSMA frameworks for SMEs were also identified:

1) Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence [9]
2) The framework of Effective Risk Management in Small and Medium Enterprises (SMEs): A Literature Review [19]
3) A Dynamic Simulation Approach to Support the Evaluation of Cyber Risks and Security Investments in SMEs [22]
4) A Novel Cybersecurity Framework for Countermeasure of SMEs in Saudi Arabia [26]
5) Calculated Risk? A Cybersecurity Evaluation Tool for SMEs [29]
6) Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs [31]
7) Reference Framework "HOGO" for Cybersecurity in SMEs based on ISO27002 and 27032 [38]

Overall, this study identified 37 CSMA frameworks from 24 research articles. Adding to that, only seven frameworks were reported to be specifically targeted for SMEs, whereas only one framework for startups was identified. These results reaffirmed the need to emphasize the CSMA framework for technology startups.

*RQ3: Do the existing CSMA frameworks assess the cyber security maturity level?*

Table 3 presents CSMA frameworks that determine the cyber security maturity level. Assessing risk without determining the cyber security maturity level limits the ability of organisations to assess their current cyber security posture and to determine the intended or target cyber security posture. Having insights on the cyber security maturity level enables organisations to allocate the appropriate investments to enhance their cyber security maturity or posture [14].

Referring to Table 3, these frameworks were highlighted in 15 research articles. The remaining eight research articles

**TABLE 2.** Relevant papers describing CSMA framework.

| No. | CSMA Framework | Ref |
|---|---|---|
| 1 | Committee of Sponsoring Organisations of the Treadway Commission (COSO) | [19] |
| 2 | ISO 21827 | [20], [33], [35] |
| 3 | Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) | [21], [28], [32], [33], [35] |
| 4 | SMECRA (SME Cyber Risk Assessment) Methodology | [22] |
| 5 | Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) | [23] |
| 6 | CyberGov (Cybersecurity Governance) Framework | [24] |
| 7 | Cyber Security Capability Maturity Model (C2M2) | [25], [28], [30], [32], [33], [35], [37] |
| 8 | Information Security Management Maturity Model (ISM3) | [25], [30], [33], [37] |
| 9 | The Publisher's Programme Overview for Information Security Management Assistance (PRISMA) | [25] |
| 10 | ISO 27002 | [25], [38] |
| 11 | Holistic Cybersecurity SME's Coordination Model | [26] |
| 12 | COBIT Framework | [27], [9], [33], [37] |
| 13 | Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) | [28], [33], [35] |
| 14 | National Initiative for Cybersecurity Education Capability Maturity Model (NICE) | [28], [30], [32], [33], [35] |
| 15 | Federal Financial Institute of Examination Council Capability Maturity Model (FFIEC-CMM) | [28], [32] |
| 16 | African Union Maturity model for Cybersecurity (AUMMCS) | [28], [32] |
| 17 | National Institute of Standards and Technology (NIST) | [9], [29], [30], [33] |
| 18 | Health Information Trust Alliance (HITRUST CSF) | [9] |
| 19 | A Pedagogic Cybersecurity Framework (PSF) | [9] |
| 20 | Centre for Internet Security (CIS) | [9] |
| 21 | Cloud Security Alliance (CSA) | [9] |
| 22 | SME Cybersecurity Evaluation Tool (CET) | [29] |
| 23 | Information Security Evaluation Maturity (ISEM) Model | [29] |
| 24 | Systems Security Engineering Capability Maturity Model (SSE-CMM) | [30] |
| 25 | ISO 27001 | [30], [35], [36] |
| 26 | Information Security Maturity Model (ISM2) | [30] |
| 27 | Gartner's Information Security Awareness Maturity Model (GISMM) | [30] |
| 28 | Information Security Framework (ISF) | [30] |
| 29 | Resilience Management Model (RMM) | [30] |
| 30 | Community Cyber Security Maturity Model (CCSMM) | [30], [33] |
| 31 | Cyber Resilience Self-Assessment Tool | [31] |
| 32 | Citigroup's Information Security Evaluation Maturity model (ISEM) | [33] |
| 33 | IBM Information Security Framework | [33] |
| 34 | Saudi Cybersecurity Maturity Assessment Framework (SCMAF) | [34] |
| 35 | ISO 15408 | [35] |
| 36 | ISO 27032 | [38] |
| 37 | Cyber Security Governance Maturity Model (CSGMM) | [39] |

emphasised risk assessment that did not specifically include the assessment of cyber security maturity level. The detailed analysis of all 23 frameworks also revealed the application of different approaches in assessing cyber security maturity levels. However, this study identified similarities in certain frameworks. For instance, the following cyber security maturity models consist of five cyber security maturity levels but the maturity levels have been defined differently [30]:

1) Information Security Evaluation Maturity Model: 1–Complacency; 2–Acknowledgment; 3–Integration; 4–Common Practice; 5–Continuous Improvement
2) Information Security Management Maturity Model: 1–Undefined; 2–Defined; 3–Managed; 4–Controlled; 5–Optimised
3) Information Security Framework: 1–Initial; 2–Basic; 3–Capable; 4–Efficiency; 5–Optimising
4) Community Cyber Security Maturity Model: 1–Initial; 2–Advanced; 3–Self-Assessed; 4–Integrated; 5–Vanguard

On the other hand, the following cyber security maturity models consist of three to four cyber security maturity levels but define cyber security maturity level differently [30]:

1) Gartner's Information Security Awareness Maturity Model: 1–Blissful Ignorance; 2–Awareness; 3–Corrective; 4–Operational Excellence
2) Resilience Management Model: 1–Incomplete; 2–Performed; 3–Managed; 4–Defined
3) Nice Cyber Security Capability Maturity Model: 1–Limited; 2–Progressing; 3–Optimised

Overall, the results demonstrated the absence of a singular CSMA framework to determine organisations' cyber security maturity level, including technology startups.

*RQ4: What are the shared control domains between the existing CSMA frameworks?*

Fundamentally, control domains are necessary as key controls for risk assessment. Table 4 presents the extracted shared control domains among the CSMA frameworks reported in seven research articles [20], [25], [28], [31], [32], [34], [38].

Based on the obtained results, common control domains that can be streamlined and evaluated in the risk assessment stage were found evident. These common control domains

**TABLE 3.** Frameworks which include CSMA.

| No. | CSMA Framework | Ref |
|---|---|---|
| 1 | Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) | [21], [28], [32], [33], [35] |
| 2 | Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) | [23] |
| 3 | CyberGov (Cybersecurity Governance) Framework | [24] |
| 4 | Cyber Security Capability Maturity Model (C2M2) | [25], [28], [30], [32], [33], [35], [37] |
| 5 | Information Security Management Maturity Model (ISM3) | [25], [30], [33], [37] |
| 6 | The Publisher's Programme Overview for Information Security Management Assistance (PRISMA) | [25] |
| 7 | Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) | [28], [33], [35] |
| 8 | National Initiative for Cybersecurity Education Capability Maturity Model (NICE) | [28], [30], [31], [33], [35] |
| 9 | Federal Financial Institute of Examination Council Capability Maturity Model (FFIEC-CMM) | [28], [32] |
| 10 | African Union Maturity Model for Cybersecurity (AUMMCS) | [28], [32] |
| 11 | National Institute of Standards and Technology (NIST) | [9], [29], [30], [33] |
| 12 | SME Cybersecurity Evaluation Tool (CET) | [29] |
| 13 | Information Security Evaluation Maturity Model (ISEM) | [30] |
| 14 | Systems Security Engineering Capability Maturity Model (SSE-CMM) | [30] |
| 15 | Information Security Maturity Model (ISM2) | [30] |
| 16 | Gartner's Information Security Awareness Maturity Model (GISMM) | [30] |
| 17 | Information Security Framework (ISF) | [30] |
| 18 | Resilience Management Model (RMM) | [30] |
| 19 | Community Cyber Security Maturity Model (CCSMM) | [30], [33] |
| 20 | Cyber Resilience Self-Assessment Tool | [31] |
| 21 | Citigroup's Information Security Evaluation Maturity (ISEM) Model | [33] |
| 22 | Saudi Cybersecurity Maturity Assessment Framework (SCMAF) | [34] |
| 23 | Cyber Security Governance Maturity Model (CSGMM) | [39] |

can be classified as the highest priority, which ultimately exhibit substantial risk impact on organisations. The common key control domains can be generalised as follows:

- People: This domain incorporates the organisation's human capital under the management of the Human Resource function. It consists of workforce management and the capabilities and educational qualifications of employees in key positions.
- Process: This domain covers all organisational processes from document maintenance, change and configuration management, asset management, and cybersecurity to programme management. It helps identify and manage all related security development and management processes.
- Technology: This domain focuses on the application, development, implementation, and maintenance of devices and technologies. This implements a data loss prevention tool that prevents data leakage.
- Compliance: This domain involves monitoring the organisation's compliance with information security policies, regulatory standards, and industry certifications. For instance, the organisation must comply with the ISO27001 certification.

**TABLE 4.** Shared control domains.

| No. | Control Domains | Ref |
|---|---|---|
| 1 | Technology, Vulnerability, Risk, Impact, System, Entity, SubSystem, Capability, Threat and Process | [20] |
| 2 | Risk Management, Security Policy and Plan Management, Human Resource Management, Physical Security Management, IT Security Management, Communication Security Management, Security Technology Management, Security Event and Incident Management, Security Audit and Compliance Management | [25] |
| 3 | Asset, Change and Configuration Management, Cybersecurity Programme Management, Event and Incident Response, Continuity of Operation, Identify and Access Management, Information Sharing and Communications, Risk Management, Situational Awareness, Supply Chain and External Dependencies Management, Threat and Vulnerability Management and Workforce Management | [28], [32] |
| 4 | Risk, Assets, Access, Threat, Situation, Sharing, Response, Dependencies, Workforce and Cyber | [28], [32] |
| 5 | Asset Management, Threat and Vulnerability Management, Incident Analysis, Awareness and Training, Information Security, Detection Processes and Continuous Monitoring, Business Continuity Management, Information Sharing and Communication | [31] |
| 6 | Governance, Asset Management, Cybersecurity Risk Management, Physical Security, Third Party Security and Logical Security | [34] |
| 7 | People, Organisational Document, Process and Technology | [37] |

Instead of having comprehensive control domains, this study identified five key domains which can be examined during the risk assessment stage.

*RQ5: Is quantifying the return of cyber security investments embedded as part of the CSMA framework?*

This study identified one research article entitled "A Dynamic Simulation Approach to Support the Evaluation of Cyber Risks and Security Investments in SMEs" [22] that highlighted its framework's capability to evaluate SMEs' cyber security investments. The study examined the targeted investments based on the risks posed and incorporated various scenarios to evaluate the cyber security investments according to several standard parameters. In one of its simulations, an organisation experiences losses due to cyber-attack, suggesting its need to allocate more investments in cyber security. As a result, the organisation's losses reduced

and eventually stabilised with increased investments in cyber security.

The lack of a quantification model embedded in an end-to-end cyber security maturity assessment framework for technology startups is a critical concern, especially when startups are highly vulnerable against the increasing rise of cyber-attacks. Technology startups cannot quantify and allocate the appropriate investments in cyber security without risk quantification.

### A. GAP ANALYSIS

The existing cyber security frameworks are used by cyber security practitioners in various industries but there is a lack of a cyber security framework to assess the maturity level specifically for a technology startup from a cyber security standpoint. Out of the 37 frameworks reviewed, only seven were specifically targeted for SMEs, and only one framework was identified for technology startups. Though SMEs and startups are similar in terms of size [5], the fundamental difference is that technology startups are known for agility and thrives on innovation with information technology.

Based on the frameworks reviewed to determine the cyber security maturity levels, there are different approaches towards assessing the cyber security maturity levels. Though there are similarities in the maturity level, they are defined differently and are not suitable for a technology startup. The cyber security maturity levels for technology startups should be aligned with the stages of the startup lifecycle for clear understanding based on the investments the startup received in each stage. Figure 3 shows an appropriate cyber security maturity level based on each stage of the startup lifecycle.

Different cyber security frameworks have a variety of control domains. However, there is no framework which has control domains to assess the key controls specific for a technology startup. After analysing the control domains from the cyber security frameworks included in this study, five key domains have been extrapolated to be analysed as part of the Risk and Controls Assessment phase.

There is also a lack of a Cyber Quantification phase embedded in the cyber security framework. Since technology startups is a lean organisation, it is important to ensure that the security budget is used prudently. In order to do this, there should a cyber quantification model to calculate the return of security investments based on the mitigation costs for the control deficiencies. The return of security investments would allow management to make a proper decision when allocating the budget to invest in cyber security measures.

First and foremost, the analysis of the cyber security frameworks selected in this study have shown that there is a lack of a specific cyber security framework to examine the key control domains in a technology startup. There is no framework which assess the cyber security maturity level specifically for a technology startup. Finally, there isn't an end-to-end framework which is available to assess cyber risk, determine the cyber security maturity level and calculate the returns of cyber security investments. An end-to-end cyber security framework provides an overview to assess cyber security risk and justify mitigating measures in a more effective manner.

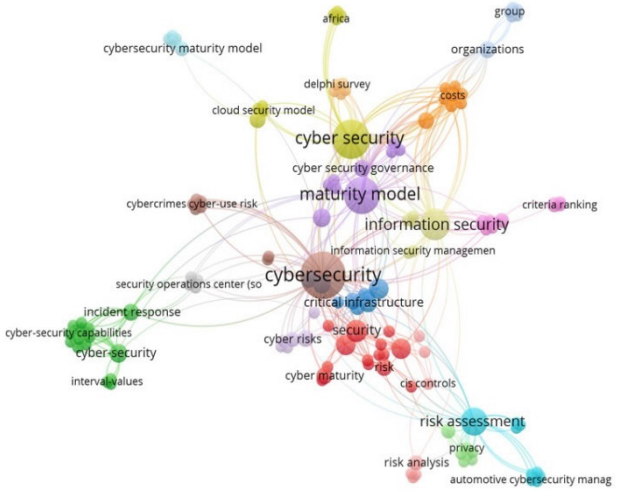



**FIGURE 4.** VOSviewer network visualization.

### B. PROPOSED CSMA FRAMEWORK

There are existing frameworks to assess the cyber security maturity of organisations. However, the frameworks are broad and generic, and thus not specific enough to be applied in technology startups. Since startups tend to be a lean organisation with limited resources, a new framework needs to be developed which is customised and focused in identifying, mitigating and quantifying risks in a technology startup. The new Cyber Security Maturity Assessment (CSMA) framework targets specifically at technology startups and provide a holistic and end-to-end framework. The CSMA framework consists of three phases; Risk and Control Assessment, Cyber Security Maturity Level and Cyber Quantification as shown in Figure 4 below.

After extrapolating the key control domains for technology startups from the existing cyber security frameworks, the People, Process, Product, Platform and Compliance or the 4P1C domains are introduced. The 4P1C domains would allow a more streamlined approach in conducting a cyber security maturity assessment and at a much quicker pace.

In Phase 1, a Risk and Control Assessment is conducted to assess the cyber risks. Each of the 4P1C domains are broken down into several sub-domains, and each of the sub-domains may contain one or more key control objectives which need to be assessed. In the Risk and Control Assessment phase, the risk assessment rating and risk treatment are derived. Phase 2 determines the cyber security maturity level of each of the key controls, sub-domains, the 4P1C domains and the overall cyber security maturity level of the technology startup. Finally, Phase 3 calculates the return of security investment for each of the mitigating measures using an enhanced version of the Return of Security Investment (ROSI) formula [42].

The proposed CSMA framework provide an avenue to effectively assess cyber risks using the 4P1C model,

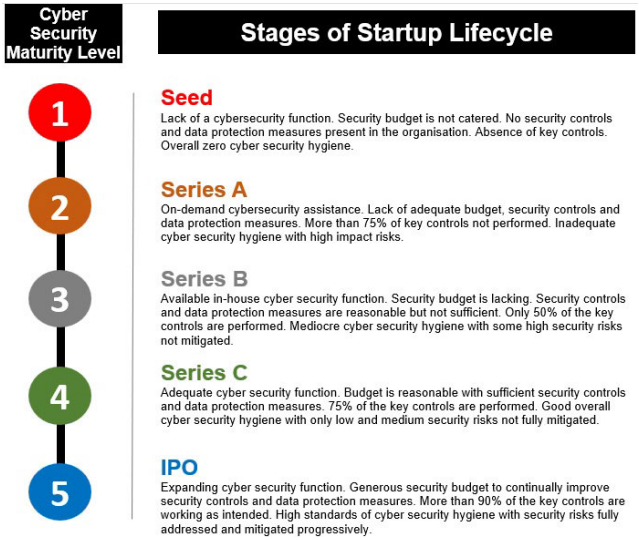



**FIGURE 5.** Cyber security maturity level for technology startups.

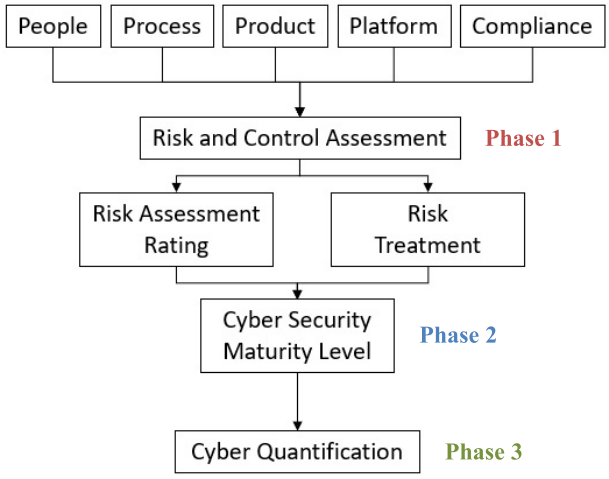



**FIGURE 6.** Cyber security maturity framework.

determine cyber security maturity level and quantify the returns of security investment in a technology startup. Instead of using a comprehensive framework with significant number of controls which are not applicable for a technology startup, the proposed framework can be used to assess cyber risks in a more objective, focused and streamlined manner. Determining the cyber security maturity level allow the required security controls to be implemented in order to address the identified gaps and finally quantifying the costs of mitigations and the returns of security investments provide management with sufficient data to justify the need to invest in appropriate cyber security solutions.

## VI. CONCLUSION AND FUTURE WORK

Technology startups are subjected to cyber-attacks on a frequent basis [2]. The impact of cyber-attacks on smaller organisations like startups is more severe than what larger organisations experience due to their limited financial resources. It may even result in the closure of a startup. Startups with limited financial resources to properly invest in cyber security are more likely to be targeted by malicious perpetrators [6]. Startups must gain their clients' trust and confidence by withstanding against cyber-attacks and building a secure and reliable product for their clients. A cyber security maturity assessment framework can substantially benefit technology startups in evaluating their cyber risks, recognizing their current and future cyber security posture, and quantifying the return of their cyber security investments based on the mitigation costs. Such a framework enables technology startups to allocate appropriate investments in cyber security to implement the required security measures based on the identified cyber risks.

This study performed a systematic literature review on cyber security maturity assessment frameworks for technology startups. Referring to the PRISMA checklist, all five research questions were addressed through the analysis of 24 selected research articles, which revealed several key points. Firstly, there is a lack of CSMA framework specifically for technology startups. This study extracted a total of 37 CSMA frameworks from the 24 research articles. However, only seven frameworks were specifically meant for SMEs, but only one framework was targeted for startups. These results proved the need to implement a streamlined CSMA framework for technology startups. Secondly, despite the shared similarities in the cyber security maturity levels among specific frameworks, the levels were defined differently, which proved the absence of a singular framework that can assess the cyber security maturity level of technology startups. Finally, in the review of 24 selected research articles, only one highlighted the aspect of investments in cyber security for SMEs. No other research articles highlighted the quantification of the return of cyber security investments for technology startups.

From this literature review, it can be highlighted that the existing cyber security frameworks used by industry practitioners are not suitable to be implemented in an agile and lean technology startup. The cyber security maturity model in the existing frameworks is not appropriately defined to suit the different stages in the startup lifecycle. The existing frameworks are also not embedded with a cyber quantification phase which is key to calculate the return of security investments for the startup. Without an end-to-end cyber security maturity assessment framework, management in technology startups is not able to obtain relevant data in order to justify the need to invest in cyber security measures.

As this study only targeted literature from IEEE explore, Scopus, Springer, and Web of Science, other relevant publications may have been excluded from this analysis. Therefore, it is recommended for future research to also explore other repositories. Researchers can also use the proposed model for technology startups in the different industry sectors such as fintech, logistics and e-commerce. Each country has different cyber security and data protection regulations; hence the proposed framework can also be tested on technology startups in the different countries to evaluate the effectiveness

of conducting the assessment. SMEs and MNCs in different industry sectors may also want to adopt this proposed framework instead of using a broad framework with significant number of controls which take a long time and plenty of resources to complete. This framework can thus be utilised as a lightweight approach for the SMEs and MNCs to conduct the assessment.

## REFERENCES


[1] Singapore Business Review, Singapore. (2022). *Singapore Cyber Attacks Soar 145% YoY in 2021*. [Online]. Available: https://sbr.com.sg/information-technology/news/singapore-cyber-attacks-soar-145-yoy-in-2021

[2] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Ephiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, pp. 1–20, Mar. 2021.

[3] B. Cerin, "Cyber security risk is a board-level issue," in *Proc. 43rd Int. Conv. Inf., Commun. Electron. Technol. (MIPRO)*, Sep. 2020, pp. 384–388.

[4] C. Zuszsanna, "Startup: Hype or tendency?" *J. Org. Culture, Commun. Conflict*, vol. 24, no. 3, pp. 1–9, 2020.

[5] *Ministry of Trade and Industry*. Accessed: Jul. 20, 2022. [Online]. Available: https://www.mti.gov.sg

[6] A. L. Mitrofan, E. V. Cruceru, and A. Barbu, "Determining the main causes that lead to cybersecurity risks in SMEs," *Bus. Excellence Manage.*, vol. 10, pp. 38–48, Dec. 2020.

[7] T. Mshvidobadze, "Security issues for digital technology entrepreneurships and startups," *Sci. Practical Cyber Secur. J.*, vol. 4, no. 4, pp. 66–73, 2020.

[8] L. Sanchez, A. S. Olmo, E. F. Medina, and M. Piattini, "Security culture in small and medium-sized enterprise," *Commun. Comput. Inf. Sci.*, vol. 110, pp. 315–324, Oct. 2010.

[9] A. A. Garba and A. M. Bade, "An investigation on recent cyber security frameworks as guidelines for organizations adoption," *Int. J. Innov. Sci. Res. Technol.*, vol. 6, pp. 103–110, Feb. 2021.

[10] A. Alahmari and B. Duncan, "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Jun. 2020, pp. 1–5.

[11] A. Rabii, S. Assoul, K. O. Touhami, and O. Roudies, "Information and cyber security maturity models: A systematic literature review," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 627–644, Jun. 2020.

[12] Action Community for Entrepreneurship, Singapore. (2022). *Creating a Future-Ready Startup Ecosystem*. [Online]. Available: https://ace.org.sg/wp-content/uploads/2022/01/ACE-Position-Paper-Jan-2022.pdf

[13] Ponemon Institute, Singapore. (2019). *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses*. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf

[14] T. Ncubukezi, L. Mwansa, and F. Rocaries, "A review of the current cyber hygiene in small and medium-sized businesses," in *Proc. 15th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2020, pp. 1–6.

[15] Angraini, R. A. Alias, and Okfalisa, "Information security policy compliance: Systematic literature review," *Proc. Comput. Sci.*, vol. 161, pp. 1216–1224, Jan. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919319465 and https://www.researchgate.net/scientific-contributions/Okfalisa-Okfalisa-2212519726

[16] I. Tikito and N. Souissi, "Meta-analysis of systematic literature review methods," *Int. J. Mod. Educ. Comput. Sci.*, vol. 2, pp. 17–25, Feb. 2019.

[17] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," *Sprouts, Work. Papers Inf. Syst.*, vol. 10, no. 26, pp. 1–51, May 2010.

[18] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Ann. Internal Med.*, vol. 89, no. 9, pp. 873–880, Sep. 2009.

[19] N. Ekwere, "Framework of effective risk management in small and medium enterprises (SMEs): A literature review," *Bina Ekonomi*, vol. 20, no. 1, pp. 23–46, Apr. 2016.

[20] R. Anass, A. Saliha, and R. Ounsa, "A concept & compliance study of security maturity models with ISO 21827," in *Proc. 22nd Int. Conf. Enterprise Inf. Syst.*, 2020, pp. 385–392.

[21] R. M. Adler, "A dynamic capability maturity model for improving cyber security," in *Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST)*, Nov. 2013, pp. 230–235.

[22] S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer, "A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs," *Decis. Support Syst.*, vol. 147, Aug. 2021, Art. no. 113580.

[23] A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, A. Cook, and H. Janicke, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Appl. Sci.*, vol. 10, no. 10, p. 3660, May 2020.

[24] M. Yassine, M. Belaissaoui, and S. Abdelkebir, "A maturity framework for cybersecurity governance in organizations," *EDP Audit, Control, Secur. Newslett.*, vol. 63, no. 6, pp. 1–22, May 2021.

[25] F. Ghaffari and A. Arabsorkhi, "A new adaptive cyber-security capability maturity model," in *Proc. 9th Int. Symp. Telecommun. (IST)*, Dec. 2018, pp. 298–304.

[26] L. Ajmi, Hadeel, N. Alqahtani, A. U. Rahman, and M. Mahmud, "A novel cybersecurity framework for countermeasure of SME's in Saudi Arabia," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–9.

[27] Y. Kusumaningrum, "Adoption of COBIT 5 framework in risk management for startup company," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 3, pp. 1446–1452, Apr. 2021.

[28] A. A. Garba, M. M. Siraj, and S. H. Othman, "An explanatory review on cybersecurity capability maturity models," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 5, no. 4, pp. 762–769, 2020.

[29] M. Benz and D. Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," *Bus. Horizons*, vol. 63, no. 4, pp. 531–540, Jul./Aug. 2020.

[30] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?" in *Proc. IEEE 35th Int. Perform. Comput. Commun.*, Dec. 2016, pp. 1–7.

[31] J. F. Carias, S. Arrizabalaga, L. Labaka, and J. Hernantes, "Cyber resilience self-assessment tool (CR-SAT) for SMEs," *IEEE Access*, vol. 9, pp. 80741–80762, 2021.

[32] A. Garba, A. M. Bade, M. Yahuza, and Y. Nuhu, "Cybersecurity capability maturity models review and application domain," *Int. J. Eng. Technol.*, vol. 9, no. 3, pp. 779–784, Sep. 2020.

[33] R. Kour, R. Karim, and A. Thaduri, "Cybersecurity for railways—A maturity model," *J. Rail Rapid Transit*, vol. 234, no. 10, pp. 1–20, Oct. 2019.

[34] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Comput. Sci.*, vol. 7, no. 2, pp. 1–26, Sep. 2021.

[35] H. Imran, M. Salama, C. Turner, and S. Fattah, "Cybersecurity risk management frameworks in the oil and gas sector: A systematic literature review," in *Advances in Information and Communication*, vol. 2. New York, NY, USA: Springer, Mar. 2022, pp. 871–894.

[36] D. Proenca and J. Borbina, "Information security management systems—A maturity model based on ISO/IEC 27001," in *Proc. Int. Conf. Bus. Inf. Syst.*, vol. 320, Jun. 2018, pp. 102–114.

[37] M. Zammani, R. Razali, and D. Singh, "Organisational information security management maturity model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 9, pp. 668–678, 2021.

[38] C. F. Cruzado, L. S. Rodriguez-Baca, L. G. Huanca-Lopez, and E. I. Acuna-Salinas, "Reference framework 'HOGO' for cybersecurity in SMEs based on ISO 27002 and 27032," in *Proc. 12th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2022, pp. 35–40.

[39] S. R. Hamidi, A. A. Aziz, S. M. Shuhidan, A. A. Aziz, and M. Mokhsin, "SMEs maturity model assessment of IR4.0 digital transformation," in *Proc. Int. Conf. Kansei Eng. Emotion Res.*, in Advances in Intelligent Systems and Computing, vol. 739, Mar. 2018, pp. 721–732.

[40] X. Zhou, Y. Jin, H. Zhang, S. Li, and X. Huang, "A map of threats to validity of systematic literature reviews in software engineering," in *Proc. 23rd Asia–Pacific Softw. Eng. Conf. (APSEC)*, 2016, pp. 153–160.

[41] E. S. Rasmussen and S. Tanev, "The emergence of the lean global startup as a new type of firm," *Technol. Innov. Manage. Rev.*, vol. 5, no. 11, pp. 12–19, Nov. 2015.

[42] T. Yaqoob, A. Arshad, H. Abbas, M. F. Amjad, and N. Shafqat, "Framework for calculating return on security investment (ROSI) for security-oriented organizations," *Future Gener. Comput. Syst.*, vol. 95, pp. 754–763, Jun. 2019.

**MOHAMED NOORDIN YUSUFF MARICAN** received the master's degree (Hons.) in internet security management from the Curtin University of Technology, Australia. He is currently pursuing the Ph.D. degree in computer science with Universiti Teknologi Malaysia. He is also an Adjunct Lecturer in cyber security with universities in Singapore, Australia, and U.K. In August 2022, he was a cyber security professional for more than 20 years working in various sectors of the industry, such as government, banking, oil and gas, consulting, social enterprise, and technology startups. He is also a member of the Information Systems Audit and Control Association (ISACA), International Information System Security Certification Consortium (ISC2), and Association of Certified Fraud Examiners (ACFE). He also holds industry certifications, such as Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Fraud Examiner (CFE), and PRINCE2 Foundation and Practitioner.

**SHUKOR ABD RAZAK** (Senior Member, IEEE) is currently a Professor at Universiti Teknologi Malaysia (UTM) and currently seconded as the Deputy Vice Chancellor of Universiti Sultan Zainal Abidin (UNISZA), Terengganu, Malaysia. He also actively conducts several types of research in digital forensic investigation, wireless sensor networks, and cloud computing. He is the author or coauthor for many journals and conference proceedings at national and international levels. His research interests include the security issues for mobile *ad-hoc* networks, mobile IPv6, vehicular *ad-hoc* networks, and network security.

**ALI SELAMAT** (Member, IEEE) has been the Dean of the Malaysia Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia (UTM), Malaysia, since 2018. An academic institution established under the cooperation of the Japanese International Cooperation Agency (JICA) and the Ministry of Education Malaysia (MOE) to provide the Japanese Style of Education in Malaysia. He is currently a Full Professor with UTM, where he is also a Professor with the Software Engineering Department, Faculty of Computing. He has published more than 60 IF research papers. His H-index is 20 and his number of citations in WoS is more than 800. His research interests include software engineering, software process improvement, software agents, web engineering, information retrievals, pattern recognition, genetic algorithms, neural networks, soft computing, computational collective intelligence, strategic management, key performance indicator, and knowledge management. He is on the Editorial Board of the *Journal Knowledge-Based Systems* (Elsevier). He has been serving as the Chair for the IEEE Computer Society Malaysia, since 2018.

**SITI HAJAR OTHMAN** (Member, IEEE) received the Ph.D. degree from the University of Wollongong, Australia. She is currently a Senior Lecturer with the Department of Computer Science, Universiti Teknologi Malaysia (UTM). Her current research interests include cybersecurity, security management, computer forensic, conceptual modeling, disaster management, disaster recovery, and business continuity planning.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 20, 2022, accepted June 3, 2022, date of publication June 13, 2022, date of current version June 16, 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3182383*

# ICSTASY: An Integrated Cybersecurity Training System for Military Personnel

**DONGHWAN LEE[1,2], (Graduate Student Member, IEEE), DONGHWA KIM[1], CHANGWON LEE[1], MYUNG KIL AHN[1], AND WONJUN LEE[2], (Fellow, IEEE)**

[1]Cyber/Network Technology Center, Agency for Defense Development, Seoul 05771, Republic of Korea
[2]School of Cybersecurity, Korea University, Seoul 02841, Republic of Korea

Corresponding author: Wonjun Lee (wlee@korea.ac.kr)

This work was supported in part by the Agency of Defense Development, Republic of Korea; and in part by the National Research Foundation (NRF) of Korea Grant by the Korean Government through the Ministry of Science and ICT (MSIT) under Grant 2019R1A2C2088812.

**ABSTRACT** Cyberwarfare can occur at any moment, anywhere on the planet, and it happens more often than we realize. The new form of warfare is wreaking havoc on not only the military but also on every aspect of our daily lives. Since cybersecurity has only recently established itself as a critical element of the military, the military community relies heavily on the private sector to ensure cyber mission assurance. Given the military's secrecy, such reliance may increase the danger of mission degradation or failure. To address this issue, the military has attempted to build a dedicated cybersecurity training system for the purpose of internalizing cybersecurity training. However, existing cybersecurity training systems frequently lack comprehensive support for effective and efficient cybersecurity training. In this study, we propose ICSTASY, a scenario-based, interactive, and immersive cybersecurity training platform that supports a variety of training features holistically. The primary requirements and design principles required to overcome the challenges inherent in developing a cyber training system were offered based on a review of prior work. Through the demonstration of our prototype, we have proven the feasibility of efficient and truly realistic cyber training, not only for the military environment but also for the private sector.

**INDEX TERMS** Cybersecurity training, cybersecurity training system, cyber trainer, prototype demonstration.

## I. INTRODUCTION

Cybersecurity is indispensable to the attainment of success in military operations nowadays. According to the results of a recent survey of military professionals, over the next five years, cyber attacks will be the greatest concern for the national security enterprise [1]. One of the biggest challenges lying ahead of us is a dearth of the forces capable of repelling enemy attacks. There are highly trained, intellectual criminals behind cyber attacks whereas defense's human resource pool is limited and heavily relies on automated devices for the majority of their defensive activities. Due to these constraints, the defensive operations in cyberwarfare can barely protect critical assets, and other actions such as backtracking and identifying threat actors are practically impossible. Many organizations including the military have attempted to address this issue by introducing a cybersecurity training program that is specifically tailored to train and educate their defense forces.

Cybersecurity training is a critical prerequisite to the military being fully cyberized. The military has attempted to build its own specialized cybersecurity training system, or the cyber range. SIMTEX (Simulator Training Exercise Network) [2] is one of the earliest examples of military-developed cybersecurity training systems. SIMTEX was designed initially for the US Air Force's training purposes and later selected as the operational platform for US military-hosted cybersecurity exercises such as Black Daemon and Cyber Flag. SIMTEX offered virtualized hosts to simulate the information assets targeted by cyber attacks and a VPN tunnel to isolate attack flow across remote sites for the exercises.

CAAJED (Cyber And Air Joint Effects Demonstration) [3] is another USAF effort that combines a commercial wargame simulator called MAP (Modern Air Power) and a cyber simulation model called SECOT (Simulated Enterprise for

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

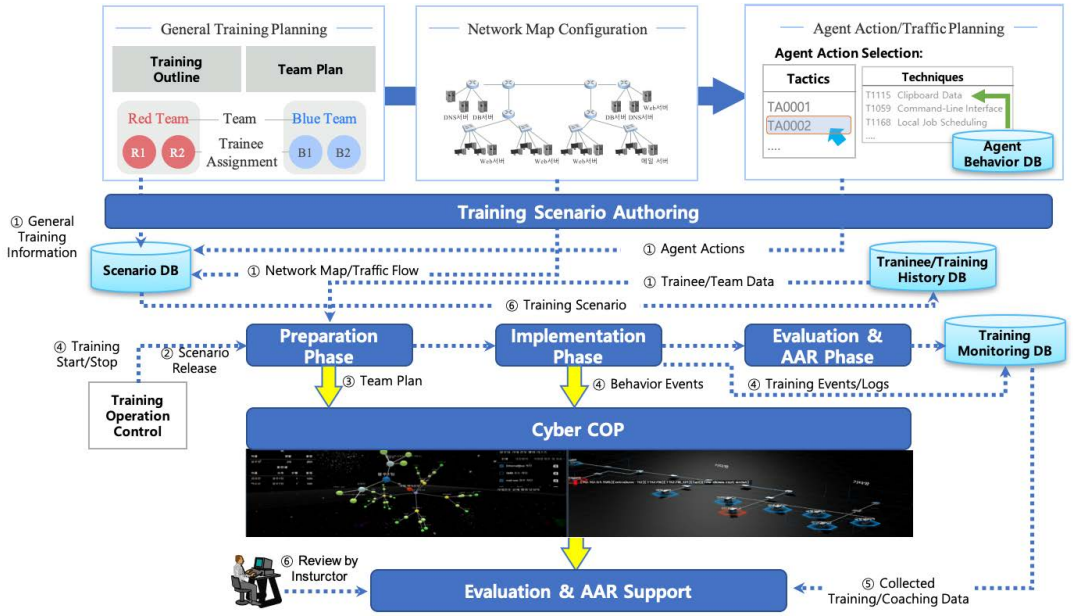



**FIGURE 1.** Operational concept and procedure of ICSTASY.

Cyber Operations Training). CAAJED was utilized in Cyber Defense Exercise 2007 (CDX 2007), a cyber exercise based on capture-the-flag tactics. During the exercise, red team members conduct simulated cyber attacks, and once the attacks are successful, SECOT calculates the cyber attack's impact on mission performance in the kinetic world.

SAST (Security Assessment Simulation Toolkit) [4] was developed by Pacific Northwest National Laboratory to provide high-level, specialized training to USAF CNO personnel. SAST provides an isolated network that simulates a large network under cyber attack. Additionally, SAST comprises MUTT, a Multi-User Training Tool that generates millions of simulated users to simulate realistic background traffic, and CAT, a Coordinated Attack Tool that incorporates cyber attacks into simulations.

StealthNet [5] is a US Army-funded LVC (Live-Virtual-Constructive) platform for cyber-related testing, evaluation, and training on the Army's tactical networks. StealthNet contains emulation models of cyber attacks such as jamming, DDoS, and worm propagation to determine the impact of cyber threats on tactical networks. StealthNet, in particular, provides simulation models for wireless tactical networks, enabling LVC co-simulation for cybersecurity training in tactical networks.

However, military-developed cybersecurity training programs are constrained in two ways: To begin, they were created for large-scale, short-term exercises such as capture-the-flag drills or cyber wargames. While these events may be beneficial for strengthening capabilities for existing cybersecurity responsibilities, they are detrimental in developing the highly qualified individuals required in the long run. Second, they frequently lack the capabilities necessary for training or are overly focused on tactical applications. These restrictive, overly-specific cybersecurity training systems have hampered the development of a realistic and effective cybersecurity training process.

Meanwhile, in the private sector, many research efforts have been conducted in recent days to build more comprehensive training systems that would address more fundamental, long-term cybersecurity training demands. These modern cybersecurity training systems include graphical user interfaces for configuring the training environment, autonomous red/blue team agents, and automated scoring. However, private-developed cybersecurity trainers have limitations in that such features are not fully integrated, limiting the ability to provide comprehensive, practical cybersecurity training. To overcome these shortcomings, we present a novel cybersecurity training platform, ICSTASY, in this work. ICSTASY provides holistic support for a variety of training capabilities.

To ascertain prerequisites and capability gaps and to develop a blueprint concept for a fully integrated cybersecurity training system, we begin by formulating the desired training system's operational concept. ICSTASY's operational concept and procedure are depicted in Fig. 1. To begin, the initial (preparation) phase defines all of the preliminary information for cybersecurity training, such as a team plan, network map configuration, and agent actions. The following step (implementation) manages a training session, via which trainees interact with the system and associated tasks such as user/agent behavior monitoring and progress/situation visualization. The last (evaluation & AAR) phase of the system facilitates the instructor's assessment and After-Action-Review (AAR) activities by consolidating training logs into trainees' scores and providing reports and replays

of completed sessions. The considerations identified with the operational concept are condensed to the ICSTASY design requirements, which we will use to demonstrate that our prototype is developed in accordance with our initial goals and conceptions throughout the development process. The contribution of our study is as follows:

- The operating concept and procedure were suggested to develop a fully integrated cybersecurity training platform for the military environment that requires more discreet but realistic and comprehensive cybersecurity training.
- We defined requirements and specifications and presented a system architecture that enables the implementation of the operating concept and procedure.
- Finally, we built a prototype of the desired platform, ICSTASY, and demonstrated its capabilities of accommodating the numerous features necessary to deliver effective and realistic cyber training dedicated to (but not limited to) the military.

The rest of this paper is arranged as follows: Section II introduces related studies. Section III provides the design concepts and requirements for ICSTASY, and Section IV elaborates on the overall architecture and system design of ICSTASY by expending on the previously stated design principles and requirements. Section V illustrates the development process through several, detailed screenshots of ICSTASY and compares our cybersecurity training system to others. The concluding section recaps and summarizes this paper.

## II. RELATED WORK

As with the military, there is little completed research on integrated cybersecurity training systems in the private sector, including academia; nonetheless, there is some notable work on each technological part of cybersecurity training systems. This section will highlight some of the essential work proposed in the private sector.

CyRIS [6] is a cyber range instantiation system developed by JAIST in which KVM-based virtual hosts are set up and created automatically following a script-based scenario file. Additionally, the scenario script specifies the types of emulated attacks to be executed and the target nodes. Their latest cybersecurity training system, CyTrOne [7], includes these technologies.

Nautilus [8] devised its own script language called SDL (Scenario Description Language) for automating the deployment and configuration of a virtualization-based cybersecurity training environment. As with CyRIS, SDL specifies virtual hosts and network configurations for a training environment, but instead of emulated attacks, it defines vulnerabilities embedded in hosts. A CVE (Common Vulnerability Enumerator) code [9] identifies each vulnerability and, based on a predetermined script, automatically plants it upon the instantiation of the vulnerable host.

ASL (Attack Specification Language) [10] provides an integrated representation of cyber threat scenarios for cybersecurity trainers. Considering the dynamic nature of the cyber threat scenarios, ASL is built with the innate feature to deduce the most advantageous attack technique given the conditions using machine learning based inference. Taking a step forward, GHOSTS [11] introduced the concept of a Non Player Character (NPC) into cyber training systems, which aims to emulate the hostile behaviors of an enemy and the benign activities of regular users.

CybOrg [12] is a cyber gym platform dedicated to the training of autonomous agents. The platform is built on a commercial cloud platform, AWS, and intends to provide a repeating training environment for autonomous agents to practice cyber attack and defense techniques using reinforcement learning. Each repeat uses a YAML-based script to duplicate and diversify the episodes given to the agents. Agents trained in this manner get deployed as red and blue team agents that face off against trainees.

However, the linked work discussed above concentrated on specific technological aspects rather than proposing a comprehensive platform. The Swedish research agency FOI launched CRATE (Cyber Range and Training Environment), a pioneering cybersecurity training platform [13], [14]. In contrast to the other previous effort, CRATE's objective was to create an integrated cybersecurity training platform by combining the fragmented technology elements. For example, CRATE's NodeAgent and Core API services facilitate the configuration and deployment of virtualized hosts and networks. Its CRATE Exercise Control (CEC) platform enables situational monitoring and evaluation of cybersecurity training [15]. Additionally, SVED (Scanning, Vulnerabilities, Exploits, and Detection) identifies vulnerabilities in a training environment and assists automated red-team agents with attack planning. [16]. Although a significant portion of the features rely on commercial off-the-shelf software such as OpenVAS [17], snort [18], or TCPdump and thus provide only partial, limited capabilities, CRATE retains meaning as the initial attempt to integrate the technology elements of a cybersecurity training system.

KYPO [19] is another notable study that takes into account the exhaustive design principles of a cybersecurity training system. KYPO acknowledges the importance of real-time monitoring and evaluation (so-called post-mortem analysis) by suggesting a highly fine-grained log production and collection architecture.

## III. DESIGN CONCEPTS AND REQUIREMENTS

A detailed assessment of existing cyber trainers showed that most of their systems could not handle the inclusion of additional elements needed for full-fledged cybersecurity training. Our novel training system addresses these limitations by being developed according to the standard V model, i.e., based on identified capability gaps. We first developed a set of principles and requirements to consider when designing

a novel cybersecurity training system. The system design, implementation, and evaluation follow in due order.

### A. EDITABLE AND REUSABLE SCENARIO WITH TEMPLATES

A scenario is a critical component of any cybersecurity training system. A training session is essentially a reproduction of a training scenario, and a robust cyber training system is one with rich scenarios. However, many cyber trainers supply scenarios as a bundled package which usually does not allow instructors to change the scenarios. This precludes the trainer from diversifying training scenarios and providing variance within a single training session. As a result, a novel cyber training system must enable an editable and reusable scenario. To ensure that this design principle is adhered to, we propose the following requirements.

1) A scenario should contain all of the elements necessary to conduct a training session, such as host and network configuration, agent behavior schedule, expected user events, and other relevant information.
2) A scenario should be exportable and re-importable as an editable script or markup language.
3) A scenario should have a layered structure with numerous layers, enabling the training system and scenario editor to access and locate required data.

### B. AUTONOMOUS OPPONENT FOR TRAINEE INTERACTION

In a typical cyber training system, interactive experiences are confined to engagement with a human opponent or to unidirectional activities outlined in a script file [20]. This prevents trainees from encountering a variety of situations that can arise in cyberspace. More intelligent *agents* capable of interacting with learners in a training environment is necessary to offer as many situations as possible. Additionally, trainees can benefit from a variety of cybersecurity experiences if an autonomous blue team and an autonomous red team are available, which is the only form of team permitted in the majority of conventional cyber trainers. In summary, we propose the following requirements for this design principle.

1) Autonomous agents capable of varying their behavior in response to changing variables in the training environment should be provided.
2) A user should be able to plan and edit the essential actions of agents throughout the scenario authoring process.
3) Agents from either the red or blue teams should be able to be chosen for an autonomous opponent team.

### C. FULL VISIBILITY INTO TRAINING SESSIONS

Because comprehensive situation awareness in cyberspace has been one of the most significant issues in the cybersecurity area, a question-and-answer-based test for trainees was an indirect method used to provide visibility into the training environment. We can promote productive interactions between a trainee and their instructor if we can automatically recognize and notify the instructor about the trainees' behavior. This enables an instructor to adjust their teaching methods while keeping a close eye on the trainee's progress. The following requirements would provide complete visibility into training sessions.

1) The training system should recognize and collect all potential events associated with trainee activity into raw logs, which are the system's most granular logs.
2) The expected training event for a training session should be definable during the scenario creation phase using the logical operations of the raw log events.
3) The training system should notify the instructor immediately upon detecting expected training events, using a visually effective method such as a dashboard and/or a Common Operational Picture (COP) for the cyber training environment.

### D. AUTOMATED EVALUATION AND AFTER-ACTION-REVIEW

As indicated previously, a question-and-answer-based test has typically been the primary approach for enabling visibility into the training environment. For instance, if a trainee responds with a string only obtained through successive privilege escalation, it implies the trainee successfully executed the privilege escalation. The evaluation process is identical in the majority of conventional cyber trainers. However, if we can automatically detect and analyze trainees' behaviors, we will be able to evaluate trainee behavior as well. The following requirements are needed to substantiate our cyber training system's automatic evaluation and AAR features.

1) The trainee behavior events that occur during a training session should be recorded in a database to be utilized post-session by the evaluation and AAR features.
2) The training system should provide an interface via which an instructor can assign scores to observed behaviors ahead of time so that the score is automatically attributed when the trainee exhibits that expected behavior.
3) When the system detects important behaviors, the main screens, such as the dashboard/COP screen and the trainee's screens, should be captured as screencasts for the AAR phase debriefing.

## IV. OVERALL ARCHITECTURE AND SYSTEM DESIGN

This section presents the proposed training system's overall architecture and system design based on the principles and requirements described in the preceding section. We begin by proposing the system's overall architecture, followed by a description of the system's design in three primary components.

### A. OVERALL ARCHITECTURE

To begin, we determine the operational procedures for our training system to create a design for the overall architecture.

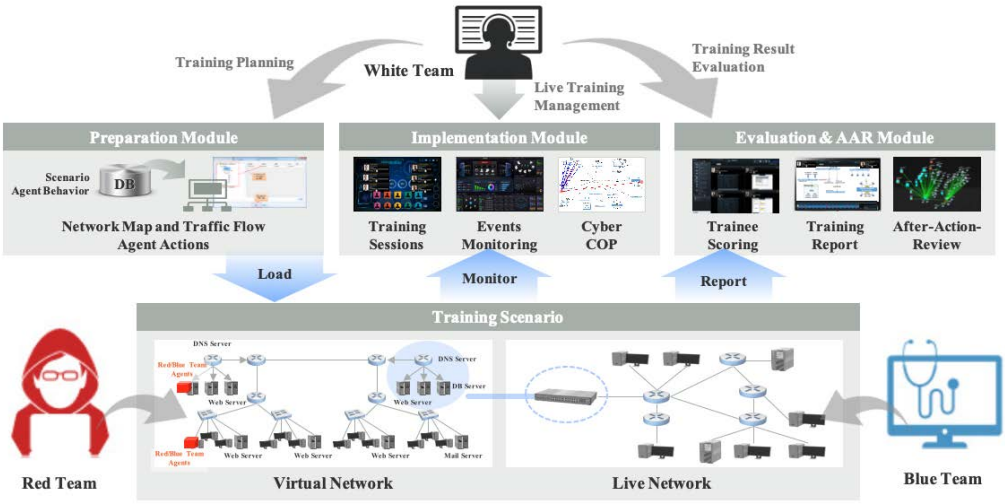



**FIGURE 2.** System architecture and modules of the ICSTASY prototype.

When considering the cybersecurity training system's use cases, the key user is the instructor. They create the scenario required for a training session, conduct the session, and lead and evaluate trainees. These tasks may be accomplished collaboratively by members of several teams, such as white, yellow, and green. Unless otherwise specified, we refer to a user who can participate in any of these teams as an instructor. As briefly mentioned above, the ICSTASY operational procedure has three phases, mainly from the instructor's perspective:

1) The preparation phase: contains activities such as scenario creation, network map/virtual machine configuration, agent behavior design, and training session management.
2) The implementation phase: includes initiating, managing, and terminating a training session. Automated agents, live monitoring, and coaching activities are performed throughout the session.
3) The evaluation and AAR phase: the final stage of training, during which an instructor can assess trainees' progress and advise them based on the information acquired throughout the assessment.

Given the operational procedure stated above, ICSTASY has three modules that correspond to the three phases: the preparation, implementation, and evaluation & AAR modules. As shown in Fig. 2, each module performs the functionality necessary for each operational phase.

### B. MODULE-WISE FEATURES AND SYSTEM DESIGN

This section details the features and specifications of each module focused on meeting the aforementioned significant requirements.[1]

[1]The requirements are referred to by their section and item numbers, for example, III-A-1 refers to the first requirement in Section III.A.

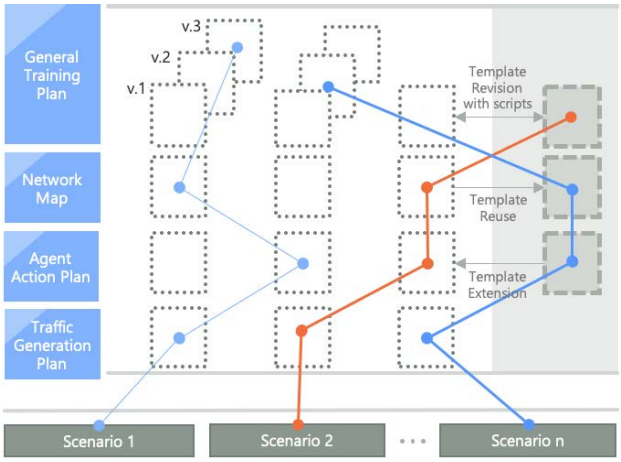



**FIGURE 3.** Layered structure of the ICSTASY training scenario.

#### 1) PREPARATION MODULE: SCENARIO AUTHORING/MANAGEMENT

First of all, we divided the scenario authoring process into multiple steps to accommodate the multi-layered structure of a training scenario (Requirements III-A-1 and III-A-3): 1) Defining general training concepts and organizing teams 2) Configuring network map/virtual hosts; 3) Scheduling the actions of agents and listing expected events. Each step intends to aid instructor teams in their preliminary work. For instance, in the second step, ICSTASY provides a drag-and-drop UI that enables the instructor to easily and efficiently build virtualized infrastructure, which is distinct green team work. In this manner, based on the objectives of training, the instructor can readily deploy security appliances: from virtualizable IDS/IPS/firewalls like pfSense, snort, Suricata, and Bro to any hardware-type appliances supporting IP networks such as firewalls, IDS/IPSes, and the anti-DDoS and anti-spam devices. The third permits instructors to more easily

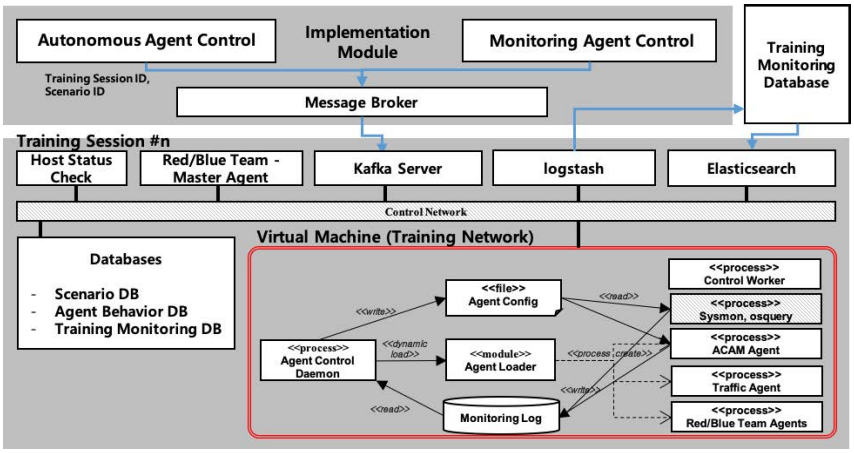



**FIGURE 4.** Structure and data flow of the ICSTASY log collection.

monitor and evaluate trainees' actions and performance, which may be related to the work of a yellow or white team.

To meet the scenario's requirements (Requirements III-A-2, III-C-2, and III-D-2), we designed a scenario as an editable XML file containing gathered data from each step in each layer. A proficient instructor may quickly locate and edit specific sections of a scenario file, resulting in a more sophisticated scenario than one prepared via the GUI. Fig. 3 illustrates a scenario file reflecting the layered structure of the ICSTASY training scenario. Scenarios are saved as templates in each layer, enabling scenario reuse and editing on a template-by-template basis.

We added a session management step before the implementation phase, in addition to the scenario authoring activity. An instructor must complete this step by creating a session where a selected scenario will be loaded. This enables us to build several sessions from a single scenario and easily manage temporal data such as trainee logs.

### 2) PREPARATION MODULE: AGENT ACTION PLANNING

The agent action planning feature is one of the most prominent features of the preparation module. The agents' actions are produced and structured automatically by specifying a few parameters, such as the starting and ending points of attack (Requirement III-B-2). Each activity of a red team agent is associated with a Technique Instance (TI), which is defined as an instantiated technique in MITRE's ATT&CK framework [21]. Each TI has pre-and-post conditions that allow us to simulate the attack path before training and pre-determine the agent's availability. Our prior work [22] and [23] have the particular automation strategies upon which our red team and blue team agents were built, respectively. Thus, an instructor can assign agents alternative roles and courses of action according to the training objective, giving a high level of diversity and flexibility for an advanced cyber training experience (Requirements III-B-1 and III-B-3). It eliminates the need for a costly white/green team and allows for the potential of a one-person white team, whereas many existing cyber trainers rely on pre-determined, immutable agent activities. Appendix contains the complete list of TIs included in ICSTASY.

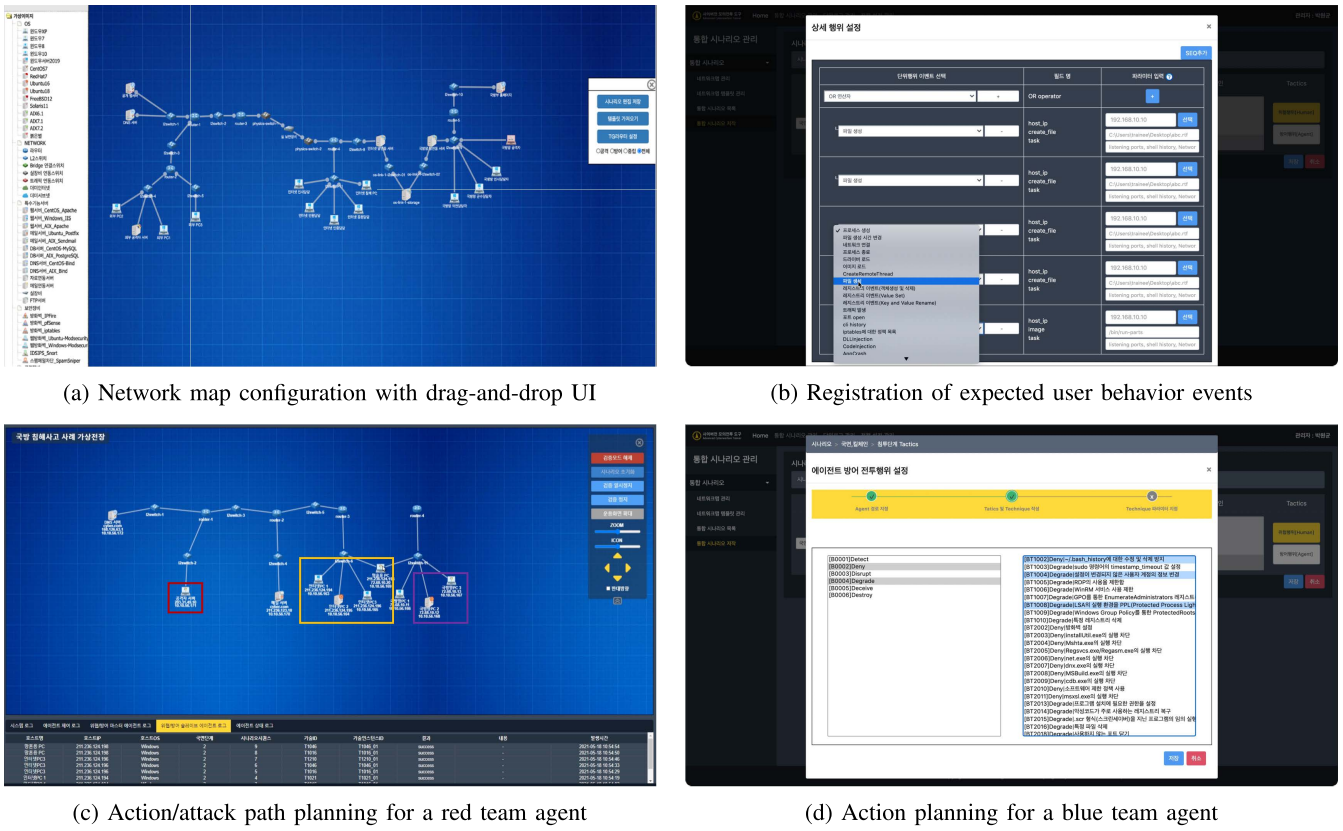
In addition to the autonomous agents, we enabled ICSTASY to imitate background and network traffic using pre-stored pcap files [24]. The preparation phase allows for the configuration of source-and-destination pairs for traffic creation. The source and destination can be hosts in a simulation or a real-world environment and in [25], indicating that our training system is LVC interoperation ready.

### 3) IMPLEMENTATION MODULE

The implementation module includes a variety of features for managing live training sessions. The implementation module's primary feature is session management, which enables an instructor to control the flow of a training session via an initiation/pause/termination interface. A notable feature of ICSTASY is the ability to pause a session, which is rarely available in other cyber trainers. This capability suspends all system activities, including the log collection for the session and all associated virtual machines. We integrated VMware vShpere API [26] and IBM PowerVC API [27] into ICSTASY connecting the session management feature to the backend that manages all the virtual machines.

Another critical feature included in the implementation module is the ability to visualize training sessions. The visualization function provides a visual representation of the session statuses and enables event-driven monitoring of learner behavior. The implementation module utilizes Logstash [28] to capture all data associated with a training session, accumulating it in the monitoring database (Requirements III-C-1 and III-D-1). Elasticsearch is used to retrieve and analyze the stored logs [29].

The key concept behind the visualization feature is a *behavior event*, which is pre-defined metadata during the preparation process. It provides expected user/agent behaviors during a training session to meet the objectives. In this manner, we may focus our search on a subset of the massive



(a) Network map configuration with drag-and-drop UI

(b) Registration of expected user behavior events

(c) Action/attack path planning for a red team agent

(d) Action planning for a blue team agent

**FIGURE 5.** Demonstrative screenshots of the preparation phase.

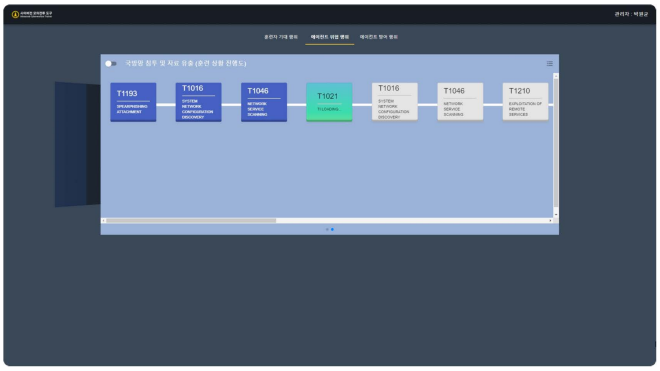
amount of logs. On the other side, we ensured that we collected as many fine-grained logs as possible from hosts and networks, referred to as an emphatomic event. In addition to the usual IDS-based detection method, live forensic/EDR (End-Host Response)-based techniques were incorporated. For instance, Microsoft's Sysinternals Suite [30] and Facebook's OSquery [31], as well as a self-developed mini-filter driver named ACAM (Advanced Cyber Activity Monitoring), collected a large amount of host-related data. These are deployed in each host, enabling highly sensitive detection of kernel level changes such as privilege escalation, driver loading/unloading, process crashes, and DLL/code injections. The atomic logs are stratified, so at least one comprises an *interim event*, and one or more interim events constitute a behavior event at the highest level. For visualization purposes, Fig. 4 illustrates the hierarchical structure of the log collection. The resulting behavioral events appear in the form of a cyber COP (Common Operational Picture) (Requirement III-C-3). ICSTASY can efficiently and precisely detect trainee/agent behaviors using this approach, whereas the majority of existing trainers rely on the instructor's skill.

Visualization also requires the log collection of autonomous agents. Once the training session initiates, the implementation module triggers automated agents to begin trace the pre-programmed path planned in the preparation phase. Unlike human behaviors, agents report agent behaviors and hence do not require the module to gather granular logs and detect them. After determining the success or failure of an action, an agent generates a behavior log.

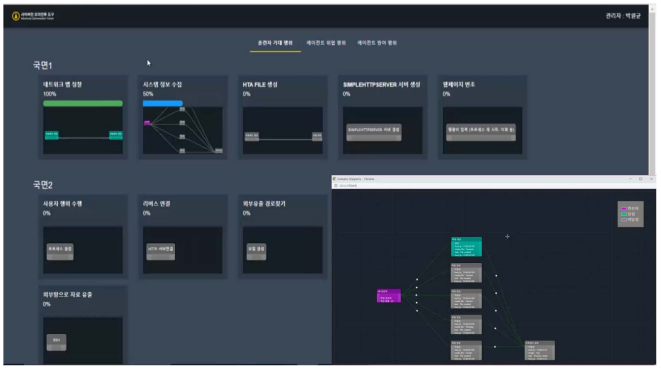
The module's final feature is live coaching, which provides an engaging experience for trainees and increases training efficiency. To avoid possible intrusion into the training world while conducting coaching activities, we isolated the training network from the 10 GbE network. All data not used for training, including atomic logs for visualization, flows up through this network. The coach can monitor each trainee's shared screen guide any trainees using the live coaching feature.

#### 4) EVALUATION AND AAR MODULE

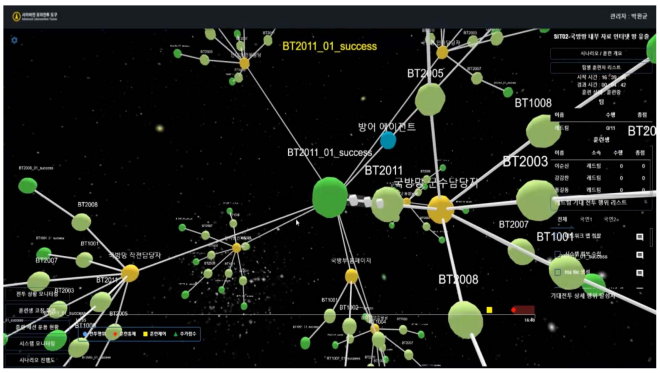
The module for evaluation and AAR relies heavily on the implementation module. From a design standpoint, the evaluation and AAR module can be defined as an implementation module that uses archived data rather than real-time data. After a training session, the instructor can playback recorded COP and trainee screens and examine saved behavior events and other records (Requirements III-D-2 and III-D-3). To facilitate evaluation and AAR, we first built a central time server and timestamped all visualization and coaching data collected during a training session. This simplifies data synchronization and enables instructors to



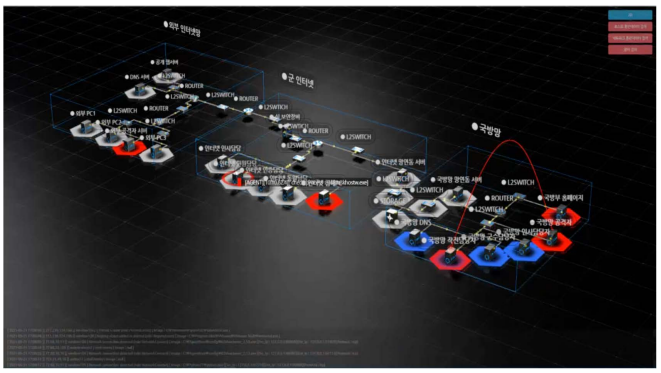
(a) Progress diagram of the red team agent action execution



(b) Dashboard with the status of expected user behavior events




(c) Cyber COP in the force-directed graph expression



(d) Cyber COP in the network map expression

**FIGURE 6.** **Demonstrative screenshots of the implementation phase.**

navigate trainees' training records by moving around a single timeline. Second, we assured that the module visualized COP using the latest web standards, including CSS3, and that the visualization data was stored after time stamping. As a result, a more informative and lightweight COP-centric replay feature emerged, especially when compared to video recording techniques that consume considerable system resources. Thus, an instructor can review the training situation collectively and conveniently for the chosen time period without losing any knowledge.

## V. DEVELOPMENT RESULTS

We developed a prototype of ICSTASY based on the module design described previously to illustrate the feasibility and usability of an advanced, immersive cyber training experience. We cannot give detailed training situations due to the possibility of disclosing confidential information; nonetheless, we have attempted to provide as many different screenshots as possible to understand our training system.

### A. PREPARATION PHASE

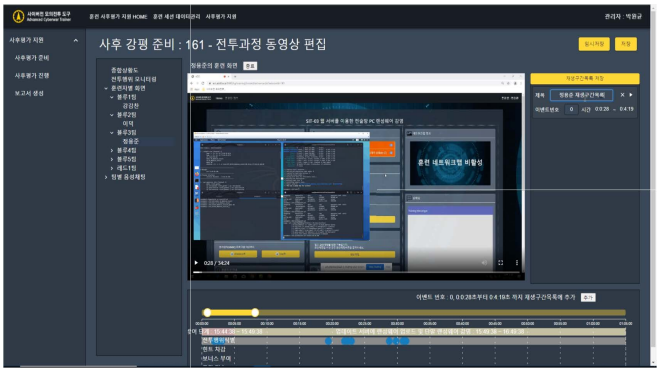
Given that the preparation phase is the most labor-intensive, we placed focus on the instructor interface during the development process. As specified in the module design, drag-and-drop-based UI for configuring the network map/virtual hosts was implemented. Refer to Fig. 5a for a screenshot of the network map configuration tool. An instructor can drag and drop the desired host template from the tool's left side panel to the tool's main panel. The host is then instantiated, allowing the instructor to update the host's different metadata, including the network configuration and user account/credential information. The metadata is initially recorded in the scenario database and is then simultaneously sent to VMware vCenter and IBM PowerVM via the vSphere API and the PowerVC API.

Fig. 5b shows the expected trainee behavior events listed in the preparation phase. As of the prototyping stage, 79 different types of atomic logs are available for an instructor to select an interim log. Given that only the AND operation is permitted for combining atomic logs, combinations can generate $(79-1)(79-2)/2 = 3003$ interim logs. As a two-step logical operation using AND or OR is permitted while composing a behavior log, $(3002 \times 3001 - 1) \times (3002 \times 3001 - 2) \approxeq 8.11 \times 1013$, i.e., a nearly infinite number of behavior logs, can be constructed in our training system. However, providing all of the behavior logs expected for a training session might be challenging for an instructor. Therefore, we enabled the prototype to reuse behavior logs utilized in prior sessions to address this issue.

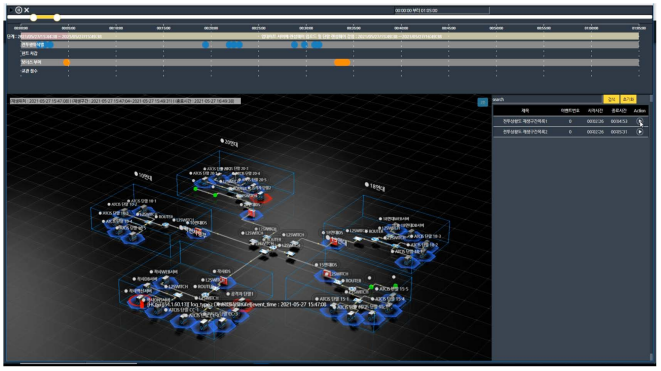
Fig. 5c and Fig. 5d illustrate the action planning processes of the red and blue team agents, respectively. As for a red team agent, the network map built in the previous process


(a) Dashboard with the trainee scoring status


(b) Generation of training report




(c) Editing of a trainee screencast for After-Action-Review



(d) Playback of a cyber COP screencast for After-Action-Review

**FIGURE 7. Demonstrative screenshots of the evaluation and AAR phase.**

allows an instructor to automatically configure the attack path and assign offensive TIs utilized in the attack by selecting the attack's start and end points. As indicated previously, the walk-through feature is used to rehearse with the autonomous red team agents. At the bottom of Fig. 5c, we can see the logs generated by the red team agents as they walk through a penetration scenario in which an external host (red square) infiltrates victim hosts (violet square) via intermediary nodes (amber square). In the case of a blue team agent, we supplied a detailed configuration UI that allowed an instructor to fine-tune the blue team's behaviors using a variety of defensive TIs in addition to the fundamental defense measures that may be done automatically with a few inputs. On the right side of the panel in Fig. 5d, we can confirm the many defensive TIs provided under the 6D categories of defense course-of-actions: detection, deny, disrupt, degrade, deceive, and destroy [32].

### B. IMPLEMENTATION PHASE

The implementation phase focused on the visualization of COP, which enables instructors to assess the training situation and trainee progress quickly. Because the achievement of expected behavior events is the primary indicator of the flow of the training process and the trainee progress, we developed and organized the forms of COPs expected to be the most effective at representing the state of behavior events.

The graphic in Fig. 6a depicts the progress of agent behavior events, specifically the status of TI executions. TIs are activated per the execution route determined by the pre-and post-conditions specified. With the diagram, an instructor can verify that each TI was successfully run and quickly determine which TI caused the flow to fail to complete as expected. The progress diagram for the blue team agent action execution is constructed similarly to the red team agent's but is displayed in parallel, as the blue team agent's activities are not serialized as the red team agent's actions are.

The dashboard seen in Fig. 6b monitors the status of expected behavior occurrences. Once a trainee's actions identify interim events, the progress bar for the corresponding behavior event reflects the percentage of completed interim events. By clicking on any behavior event, an instructor can view the detailed state of event detection and the logical breakdown of that behavior event.

Fig. 6c and 6d illustrate the two primary Cyber COP displays produced for ICSTASY. The first is a cyber COP with a force-directed graph, which serves as the primary COP for assisting an instructor's situational awareness via a conceptual data model. Specifically, when an agent or trainee node has a new behavior event as a child node, it is added to the center node. The child nodes are added up whenever the agent or trainee experiences a new behavior event. If the conditions between events are dependent, the event nodes have a

**TABLE 1. Comparison between cybersecurity training system/platforms.[2]**

| Phase | Features | Cybersecurity Training System/Platforms | | | | | |
|---|---|---|---|---|---|---|---|
| | | CyRIS [6] | Nautilus [8] | CybOrg [12] | CRATE [15] | KYPO [19] | ICSTASY |
| Preparation | Script/markup language-based training environment configuration (III-A-1, III-A-2) | Yes | Yes | Yes | Yes | No | Yes |
| | GUI-based training environment configuration (III-A-1, III-A-3) | No | Yes | No | No | No | Yes |
| | Automated agent action planning (III-B-1, III-B-2) | P/S | No | Yes | Yes | No | Yes |
| Implementation | Automated training environment provisioning (III-1-1, III-1-3) | Yes | Yes | Yes | Yes | Yes | Yes |
| | IDS-based basic event monitoring (III-C-1) | No | No | No | Yes | Yes | Yes |
| | Dedicated agent-based fine-grained event monitoring (III-C-1, III-C-2) | No | No | No | No | N/A | Yes |
| | Visualization via cyber COP (III-C-3) | No | No | No | P/S | P/S | Yes |
| | Autonomous red/blue team agents (III-B-3) | P/S | No | Yes | Yes | No | Yes |
| | Background traffic generation/traffic injection (III-B-1) | No | No | No | P/S | No | Yes |
| Evaluation & AAR | Automated trainee scoring (III-D-1, III-D-2) | No | No | No | Yes | Yes | Yes |
| | Screen recording & replay (III-D-3) | No | No | No | No | No | Yes |
| | Training report generation (III-D-1, III-D-2) | No | No | No | Yes | N/A | Yes |

subordinate connection. On the right side of the cyber COP, trainees' achieved behavior events are also listed. By selecting an event from the list, a video with the trainee's screencast at the time of the event will play. ICSTASY accomplishes this by maintaining video recordings of trainees' screencasts with a 30-second window size.

The second is a cyber COP with a conventional network map diagram, which serves as a secondary COP to aid intuitive network plane knowledge. The red and blue hexagonal loops surrounding the nodes in Fig. 6d denote the region of the red and blue teams, respectively. The white team designates the color-coded information prior to the train session and can swap to another color when an instructor confirms a trainee's occupation report. The red parabolic line in the figure represents the network flow associated with a cyber attack, connecting the attack's origin and destination. These visual elements provide instructors and observers of cyber training with an instantaneous perception of a training situation and create a highly immersive, competition-like (i.e., gamified) environment for trainees when combined with the varied coaching experience supported by various media.

### C. EVALUATION AND AAR PHASE

In terms of user experience, the assessment and AAR phase is divided into two distinct components: evaluation and AAR. Fig. 7a and 7b illustrate the trainee scoring and training report generation features, respectively, which are mostly used for the instructor's evaluation work. The trainee scoring dashboard summarizes and displays the current training session's point-scoring and learning progress. For instance, an instructor can use the dashboard to determine how trainees earned scores and which trainee contributed the most to their team's point total. The training history saved in the training monitoring database, along with relevant data contained in other databases, is assembled into a single training report, including the scoring data. Additionally, the training report includes additional statistics about the training that are not displayed in the UI, such as the status of file/network/process access and privilege escalation, as well as the CPU/RAM consumption on each host.

Regarding the AAR part shown in Fig. 7c and 7d, we attempted to maximize the use of screencasts of trainees' screens and cyber COPs captured during a training session. However, because retaining complete screencasts of all the screens displayed during a session could result in an enormous strain on the ICSTASY system's storage, the editing process for the screencasts to be used in AAR was added immediately upon the session's conclusion. As illustrated in Fig. 7c, only the partial, selected segments of the trainees' screencasts required for AAR remain after a training session. Although the screencasts of cyber COPs are editable in the same way as those of trainees, they are substantially more lightweight to process since only the visualization data for each COP is recorded and replayed.

### D. COMPARISONS WITH OTHER TRAINING SYSTEMS

Table 1 outlines and contrasts the primary features of each work. We can certify that ICSTASY offers the most comprehensive features over any other training solution. While certain training systems, such as CRATE, may contain a number

[2]P/S and N/A denote *Partially Supported* and *Not Available* (unknown), respectively.

**TABLE 2.** List of Technique Instances for Red Team Agents.

| No. | Tactic | Technique | TI ID | Target Platforms | Description |
|---|---|---|---|---|---|
| 1 | TA0001 (Initial Access) | Valid Accounts | T1078 | Linux, Windows | Using ordinary user accounts |
| 2 | | Spearphishing Link | T1192 | Linux, Windows | Spearphishing using URL links |
| 3 | | Spearphishing Attachment | T1193 | Linux, Windows | Spearphishing using file attachments |
| 4 | TA0002 (Execution) | Service Execution | T1035 | Windows | Windows service execution |
| 5 | | Scheduled Task | T1053 | Windows | Execution of a program via scheduled task |
| 6 | | Command-Line Interface | T1059 | Linux, Windows | Execution of an executable file with CLI |
| 7 | | PowerShell | T1086 | Windows | Execution with Windows PowerShell |
| 8 | | Clipboard Data | T1115 | Linux, Windows | Collecting data stored in clipboard |
| 9 | | Space after Filename | T1151 | Linux | Adding a space after a filename |
| 10 | | Source | T1153 | Linux | Execution of a function or a file using the source command |
| 11 | | Local Job Scheduling | T1168 | Linux | Registering a task on the cron daemon |
| 12 | | User Execution | T1204 | Linux, Windows | Execution of an executable file with the ordinary user privilege |
| 13 | TA0003 (Persistence) | Winlogon Helper DLL | T1004 | Windows | Registering DLL on Windows Registry (e.g., HKLM\Software [Wow6432Node]Microsoft\Windows NT\CurrentVersion\Winlogon\ and HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\) |
| 14 | | Port Monitors | T1013 | Windows | Manipulating a Windows Registry key to modify the DLL path called by spoolsv.exe |
| 15 | | Modify Existing Service | T1031 | Windows | Modifying sc.exe or a Windows Registry key to change binPath of a running service |
| 16 | | New Service | T1050 | Windows | Registering a new service with sc.exe |
| 17 | | Service Registry Permissions Weakness | T1058 | Windows | Modifying binPath or imagePath of services registered on Windows Registry (HKLM\SYSTEM\ CurrentControlSet\Services) |
| 18 | | Registry Run Keys / Startup Folder | T1060 | Windows | Adding/Modifying Windows Registry key related to starting programs |
| 19 | | AppInit DLLs | T1103 | Windows | Modifying a Windows Registry key (HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows NT\CurrentVersion\Windows) used by AppInit |
| 20 | | Netsh Helper DLL | T1128 | Windows | Modifying a Windows Registry key (HKLM\SOFTWARE\Microsoft\Nets) used by NetSH |
| 21 | | Authentication Package | T1131 | Windows | Modifying a Windows Registry key (HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows NT\CurrentVersion\Windows) used by Local Security Authority (LSA) |
| 22 | | Create Account | T1136 | Linux, Windows | Creation of an account |

**TABLE 2.** List of Technique Instances for Red Team Agents.

| | | | | | |
|---|---|---|---|---|---|
| 23 | | .bash_profile and .bashrc | T1156 | Linux | Adding a script code in .bash_profile or .bashrc |
| 24 | | AppCert DLLs | T1182 | Windows | Modifying a Windows Registry key (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager) used by AppCert DLL |
| 25 | | Port Knocking | T1205 | Linux | Conduct of network port scanning |
| 26 | | Time Providers | T1209 | Windows | Modifying a Windows Registry key (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\) used by the W32Time service |
| 27 | TA0004 (Privilege Escalation) | Sudo | T1169 | Linux | Execution of a program with the administrator privilege |
| 28 | | Sudo Caching | T1206 | Linux | Using the privilege of root-privileged executable before its returning to the normal user privilege |
| 29 | TA0005 (Defense Evasion) | Masquerading | T1036 | Linux, Windows | Disguise the names of malicious programs/processes as normal ones |
| 30 | | File Deletion | T1107 | Linux, Windows | Deletion of files using a normal delete operation |
| 31 | | Modify Registry | T1112 | Windows | Creation/modification/deletion/hiding of a Windows Registry entry/key |
| 32 | | Clear Command History | T1146 | Linux | Deletion of CLI command history |
| 33 | | File Permissions Modification | T1222 | Linux, Windows | Modifying the file permissions |
| 34 | TA0006 (Credential Access) | Credential Dumping | T1003 | Linux, Windows | Dumping of the account credentials |
| 35 | | Credentials in Files | T1081 | Linux, Windows | Using the contents in stored files for account access management (e.g., xml files used for FileZilla to manage sessions) |
| 36 | | Bash History | T1139 | Linux | Accessing the .bash_history file |
| 37 | | Exploitation of Remote Services | T1210 | Linux, Windows | Penetrate into a host using vulnerability of the SMB protocol (e.g., Eternal Blue) |
| 38 | TA0007 (Discovery) | System Service Discovery | T1007 | Windows | Collecting the system service information |
| 39 | | Application Window Discovery | T1010 | Windows | Accessing the application list |
| 40 | | System Network Configuration Discovery | T1016 | Linux, Windows | Accessing the system network configurations |
| 41 | | System Owner/User Discovery | T1033 | Linux, Windows | Accessing the system administrators/users informations |
| 42 | | Network Service Scanning | T1046 | Linux, Windows | Scanning the network services |
| 43 | | System Network Connections Discovery | T1049 | Linux, Windows | Accessing informations on the active network connections |
| 44 | | Process Discovery | T1057 | Linux, Windows | Accessing the running processes list |

**TABLE 2.** List of Technique Instances for Red Team Agents.

| | | | | | |
|---|---|---|---|---|---|
| 45 | | System Information Discovery | T1082 | Linux, Windows | Accessing the system informations |
| 46 | | File and Directory Discovery | T1083 | Linux, Windows | Exploring files and directories |
| 47 | | Account Discovery | T1087 | Linux, Windows | Accessing the user accounts list |
| 48 | | System Time Discovery | T1124 | Windows | Accessing the system time information |
| 49 | | Network Share Discovery | T1135 | Windows | Scanning shared networks |
| 50 | | Remote Service | T1021 | Windows | Making a connection using a remote service |
| 51 | | Taint Shared Content | T1080 | Windows | Uploading a malware on a shared file server |
| 52 | TA0009 (Collection) | Data Staged | T1074 | Linux, Windows | Storing data in a temporary space |
| 53 | | Automated Collection | T1119 | Linux, Windows | Collecting files in an automatic manner |
| 54 | | Data from Information Repositories | T1213 | Linux, Windows | Acquiring data via information repositories such as databases and file servers |
| 55 | TA0010 (Command & Control) | Data Compressed | T1002 | Linux, Windows | Conducting the compression of data |
| 56 | | Data Encrypted | T1022 | Linux, Windows | Conducting the encryption of data |
| 57 | | Exfiltration Over Command and Control Channel | T1041 | Linux, Windows | Exfiltration of data to a C2 server with the commonly used communication protocols |
| 58 | | Exfiltration Over Alternative Protocol | T1048 | Linux, Windows | Exfiltration of data to a C2 server with a special communication protocol |
| 59 | TA0011 (Exfiltration) | Standard Cryptographic Protocol | T1032 | Linux, Windows | Conducting C&C communication for data exfiltration with the standard encryption techniques |
| 60 | | Commonly Used Port | T1043 | Linux, Windows | Conducting C&C communication for data exfiltration with the commonly used ports |
| 61 | | Uncommonly Used Port | T1065 | Linux, Windows | Conducting C&C communication for data exfiltration with non-commonly used ports |
| 62 | | Standard Application Layer Protocol | T1071 | Linux, Windows | Conducting C&C communication for data exfiltration with the standard application layer protocols |
| 63 | | Data Encoding | T1132 | Linux, Windows | Conduct of data encoding for data exfiltration |
| 64 | TA0040 (Impact) | Data Destruction | T1485 | Linux, Windows | Deleting all the data in a storage |
| 65 | | Data Encrypted for Impact | T1486 | Linux, Windows | Conducting data encryption for sabotage (e.g., ransomware) |
| 66 | | Service Stop | T1489 | Windows | Termination of a running service |
| 67 | | Stored Data Manipulation | T1492 | Linux, Windows | Modifying stored data such as documents, email files and databases |

of features comparable to ICSTASY, given the publicly available data, the technological maturity of each feature appears to be less than that of ICSTASY.

## VI. CONCLUSION

This paper introduces ICSTASY, a novel cybersecurity training system for military personnel. It outlines the essential

requirements and design architectures that must be met for trainees to have an immersive training experience and to facilitate instructors in their capacity to coach and manage cybersecurity training effectively. The development outcome of ICSTASY as a prototype proved that design concepts and requirements were concretely represented and incorporated into the system, demonstrating the feasibility of integrated, comprehensive cybersecurity training. Our next effort will include integrating LVC interoperability with ICSTASY.

## APPENDIX
## LIST OF TECHNIQUE INSTANCES FOR RED TEAM AGENTS

See Table 2.

## REFERENCES


[1] (Oct. 2021). A. Mehta. *Cyber Concerns, Classification Disagreements Lead Space Survey Results*. Breaking Defense. [Online]. Available: https://breakingdefense.com/2021/10/cyber-concerns-classification-disagreements-lead-space-survey-results/

[2] M. G. Wabiszewski, T. R. Andel, B. E. Mullins, and R. W. Thomas, "Enhancing realistic hands-on network training in a virtual environment," in *Proc. Spring Simul. Multiconf. (SpringSim)*, San Diego, CA, USA, Mar. 2009, pp. 1–8.

[3] R. S. Mudge and S. Lingley, "Cyber and air joint effects demonstration (CAAJED)," Inf. Directorate, Air Force Res. Lab, Rome, NY, USA, Tech. Rep. AFRL-RI-RS-TM-2008-12, Mar. 2008.

[4] W. D. Meitzler, S. J. Ouderkirk, and C. O. Hughes, "Security assessment simulation toolkit (SAST) final report," Pacific Northwest Nat. Lab. (PNNL), Richland, WA, USA, Tech. Rep. PNNL-18964, Nov. 2009.

[5] G. Torres, K. Smith, J. Buscemi, S. Doshi, H. Duong, D. Xu, and H. K. Pickett, "Distributed stealthnet (D-SN): Creating a live, virtual, constructive (LVC) environment for simulating cyber-attacks for test and evaluation (T&E)," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2015, pp. 1284–1291.

[6] C. Pham, D. Tang, K.-I. Chinen, and R. Beuran, "CyRIS: A cyber range instantiation system for facilitating security training," in *Proc. 7th Symp. Inf. Commun. Technol.*, Ho Chi Minh, Vietnam, Dec. 2016, pp. 251–258.

[7] R. Beuran, D. Tang, C. Pham, K.-I. Chinen, Y. Tan, and Y. Shinoda, "Integrated framework for hands-on cybersecurity training: CyTrONE," *Comput. Secur.*, vol. 78, pp. 43–59, Sep. 2018.

[8] G. Bernardinetti, S. Iafrate, and G. Bianchi, "Nautilus: A tool for automated deployment and sharing of cyber range scenarios," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, Vienna, Austria, Aug. 2021, pp. 1–7.

[9] S. Christey and R. A. Martin, "Vulnerability type distributions in CVE," MITRE, McLean, VA, USA, Tech. Rep., May 2007. [Online]. Available: https://cwe.mitre.org/documents/vuln-trends/vuln-trends.pdf

[10] S. Arshad, M. Alam, S. Al-Kuwari, and M. H. A. Khan, "Attack specification language: Domain specific language for dynamic training in cyber range," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Apr. 2021, pp. 873–879,

[11] D. D. Updyke, G. B. Dobson, T. G. Podnar, L. J. Osterritter, B. L. Earl, and A. D. Cerini, "Ghosts in the machine: A framework for cyber-warfare exercise npc simulation," Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2018-TR-005, Dec. 2018.

[12] M. Standen, M. Lucas, D. Bowman, T. J. Richer, J. Kim, and D. Marriott, "CybORG: A gym for the development of autonomous cyber agents," in *Proc. 1st Int. Workshop Adapt. Cyber Defense*, Aug. 2021, pp. 1–7. [Online]. Available: https://arxiv.org/html/2108.08476v1

[13] T. Sommestad, "Experimentation on operational cyber security in CRATE," in *Proc. NATO STO-MP-IST Spec. Meeting*, Copenhagen, Denmark, 2015, pp. 7:1–7:12. [Online]. Available: http://www.sommestad.com/teodor/

[14] T. Gustafsson and J. Almroth, "Cyber range automation overview with a case study of CRATE," in *Proc. 25th Nordic Conf. Secure IT Syst. (NordSec)*, Nov. 2020.

[15] J. Almroth and T. Gustafsson, "CRATE exercise control—A cyber defense exercise management and support tool," in *Proc. 5th IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 37–45.

[16] H. Holm and T. Sommestad, "SVED: Scanning, vulnerabilities, exploits and detection," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, Nov. 2016, pp. 976–981.

[17] Greenbone Networks GmbH. *OpenVAS–Open Vulnerability Assessment Scanner*. Accessed: Nov. 13, 2021. [Online]. Available: https://www.openvas.org

[18] M. Roesch, "Snort–lightweight intrusion detection for networks," in *Proc. 13th USENIX Large Installation Syst. Admin. Conf. (LISA)*, Seattle, WA, USA, Nov. 1999, pp. 1–11.

[19] P. Čeleda, J. Čegan, J Vykopal, and D Tovarňák, "KYPO—A platform for cyber defence exercises," in *Proc. Modelling Simulation Support Oper. Tasks Including War Gaming, Logistics, Cyber Defence (NATO STO-MP-MSG)*, Munich, Germany, Oct. 2015. [Online]. Available: https://www.sto.nato.int/publications/STOMeetingProceedings/STO-MP-MSG-133/MP-MSG-133-COVER.pdf

[20] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, "Cyber ranges and TestBeds for education, training, and research," *Appl. Sci.*, vol. 11, no. 4, p. 1809, Feb. 2021.

[21] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "MITRE ATT&CK: Design and philosophy," MITRE, McLean, VA, USA, Tech. Rep. MP180360R1, Jul. 2018.

[22] S. Y. Enoch, Z. Huang, C. Y. Moon, D. Lee, M. K. Ahn, and D. S. Kim, "HARMer: Cyber-attacks automation and evaluation," *IEEE Access*, vol. 8, pp. 129397–129414, 2020.

[23] S. Y. Enoch, C. Y. Moon, D. Lee, M. K. Ahn, and D. S. Kim, "A practical framework for cyber defense generation, enforcement and evaluation," *Comput. Netw.*, vol. 208, May 2022, Art. no. 108878.

[24] C. Lee, "Method for providing background traffic using IP random assigning in cyber range," *Electron. Lett.*, vol. 57, no. 6, pp. 261–263, Feb. 2021.

[25] D. Lee, D. Kim, M. K. Ahn, W. Jang, and W. Lee, "Cy-through: Toward a cybersecurity simulation for supporting live, virtual, and constructive interoperability," *IEEE Access*, vol. 9, pp. 10041–10053, 2021.

[26] VMware. *vSphere Automation API Reference*. Accessed: Nov. 13, 2021. [Online]. Available: https://developer.vmware.com/apis/vsphere-automation/latest

[27] *IBM Power Virtualization Center APIs*. Accessed: Nov. 13, 2021. [Online]. Available: https://www.ibm.com/docs/en/powervc/1.4.3?topic=power-virtualization-center-apis

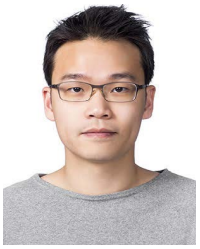
[28] J. Turnbull, *The Logstash Book*. Research Triangle, NC, USA: Lulu Press, 2013.

[29] C. Gormley and Z. Tong, *Elasticsearch: The Definitive Guide: A Distributed Real-Time Search and Analytics engine*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[30] *Sysinternals Suite*. Accessed: Nov. 13, 2021. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

[31] *Osquery*. Accessed: Nov. 13, 2021. [Online]. Available: https://github.com/osquery/osquery

[32] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues Inf. Warfare Secur. Res.*, vol. 1, no. 1, pp. 80–106, Apr. 2011.

**DONGHWAN LEE** (Graduate Student Member, IEEE) received the B.E. degree in industrial engineering and the M.S. degree in computer science and engineering from Korea University, Seoul, Republic of Korea, in 2006 and 2008, respectively, where he is currently pursuing the Ph.D. degree in cybersecurity. He is a Senior Researcher at the Cyber/Network Technology Center, Agency for Defense Development, Seoul. His research interests include wireless communication, parallel and distributed computing, wireless security, and virtualization technologies for cybersecurity.

**DONGHWA KIM** received the B.S. and M.S. degrees from the School of Electrical Engineering, Korea University, Seoul, Republic of Korea, in 2004 and 2007, respectively. He is currently a Senior Researcher at the Cyber/Network Technology Center, Agency for Defense Development, Seoul. His research interests include cybersecurity training systems and red team automation.

**CHANGWON LEE** received the B.S., M.S., and Ph.D. degrees in electronics and computer engineering from Hanyang University, in 1999, 2001, and 2019, respectively. He is currently a Principal Researcher at the Cyber/Network Technology Center, Agency for Defense Development, Seoul, Republic of Korea. His current research interests include cyber security and hardware security.

**MYUNG KIL AHN** received the B.S. degree in information and communication engineering from Chungnam National University, Daejeon, Republic of Korea, in 1997, the M.S. degree in computer engineering from Sogang University, Seoul, Republic of Korea, in 2003, and the Ph.D. degree in electrical and electronics engineering from Chung-Ang University, Seoul, in 2021. She is currently a Principal Researcher at the Cyber/Network Technology Center, Agency for Defense Development, Seoul. Her research interests include computer security and cyberwarfare modeling and simulation.

**WONJUN LEE** (Fellow, IEEE) received the B.S. and M.S. degrees in computer engineering from Seoul National University, Seoul, Republic of Korea, in 1989 and 1991, respectively, the M.S. degree in computer science from the University of Maryland, College Park, MD, USA, in 1996, and the Ph.D. degree in computer science and engineering from the University of Minnesota, Minneapolis, MN, USA, in 1999. In 2002, he joined the Faculty of Korea University, Seoul, where he is currently a Professor with the School of Cybersecurity. He has authored or coauthored over 220 papers in refereed international journals and conferences. His research interests include communication and network protocols, optimization techniques in wireless communication and networking, security and privacy in mobile computing, and RF-powered computing and networking. He has served as the TPC and/or an Organizing Committee Member for IEEE INFOCOM, from 2008 to 2023, the PC Vice Chair for IEEE ICDCS 2019 and the ACM MobiHoc, from 2008 to 2009, and over 130 international conferences.