Machine Intelligence Research
www.mi-research.net

21(2), April 2024, 294-317
DOI: 10.1007/s11633-023-1456-2

Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges

Yang Cao[1] Shiva Raj Pokhrel[2] Ye Zhu[1] Robin Doss[1] Gang Li[1]

[1] Centre for Cyber Resilience and Trust, Deakin University, Burwood 3125, Australia

[2] School of Information Technology, Deakin University, Geelong 3216, Australia

Abstract: Zero trust architecture (ZTA) is a paradigm shift in how we protect data, stay connected and access resources. ZTA is non-perimeter-based defence, which has been emerging as a promising revolution in the cyber security field. It can be used to continuously maintain security by safeguarding against attacks both from inside and outside of the network system. However, ZTA automation and orchestration, towards seamless deployment on real-world networks, has been limited to be reviewed in the existing literature. In this paper, we first identify the bottlenecks, discuss the background of ZTA and compare it with traditional perimeter-based security architectures. More importantly, we provide an in-depth analysis of state-of-the-art AI techniques that have the potential in the automation and orchestration of ZTA. Overall, in this review paper, we develop a foundational view on the challenges and potential enablers for the automation and orchestration of ZTA.

Keywords: Zero trust architecture, cyber security, artificial intelligence, access control, authentication.

Citation: Y. Cao, S. R. Pokhrel, Y. Zhu, R. Doss, G. Li. Automation and orchestration of zero trust architecture: Potential solutions and challenges. *Machine Intelligence Research*, vol.21, no.2, pp.294–317, 2024. http://doi.org/10.1007/s11633-023-1456-2

1 Introduction

To date, most network security architectures have used perimeter-based defence to isolate internal networks from external networks. Firewalls, virtual private networks (VPN), and demilitarized zone (DMZ) networks prevent external attacks by creating a network security perimeter[1]. This can effectively prevent external attacks, but it is difficult to prevent internal attacks because once an intruder breaches the security perimeter, further illegal actions will not be hindered[2]. In addition, with the rapid development of digital technologies such as 5G, the internet of things and cloud computing, the number of network users and devices[3] and their security concerns[4] are growing exponentially, as the perimeter of the network is becoming increasingly blurred[5, 6]. This makes it more difficult to protect organizational resources, especially as more data access points, information inputs and outputs are created[7]. Therefore, preventing internal attacks requires a security architecture that does not trust any network[8, 9].

Zero trust architecture (ZTA)[2] is a new concept of network security architecture based on the principle of least privilege, which aims to solve the above problems by restricting the behaviour of subjects inside the network. Based on the core idea of "never trust, always verify"[10], ZTA follows a resource-based security policy: no users, devices or applications (services) can access the data without authentication and authorization. However, while ZTA provides more robust cyber protection measures, it still faces significant implementation challenges[11]. The implementation of ZTA requires multiple security tools (e.g., firewalls) and policies to work together, and traditional stand-alone security detection approaches may not be applicable. In addition, the large amount of data collected and produced by these security tools can be used for risk analysis, prediction and evaluation within the framework. Thus, to maximize the security protection performance of ZTA, the components of existing frameworks need to be automated and orchestrated. In this context, artificial intelligence (AI) algorithms are considered as one of the most suitable technologies to automate and orchestrate ZTA[12].

AI technologies are considered as enablers for the security orchestration, automation and response (SOAR) solutions designed to automate and integrate different security tasks and processes in response to incidents[13]. SOAR is also one of the functions to be considered in the execution of ZTA[14], which provides a reference for AI to perform automation and orchestration across components.

Security teams consider ZTA as an enabler to uphold

Review
Manuscript received on February 1, 2023; accepted on May 16, 2023; published online on January 25, 2024
Recommended by Associate Editor Hao Sun
Colored figures are available in the online version at https://link.springer.com/journal/11633

security in their organization's networks. In particular, ZTA needs to develop capabilities that orchestrate and learn continuously to secure an environment based on hyper-granular access privileges. ZTA automation and orchestration can relieve security personnel from manually assigning and reassigning access credentials throughout the organization's network. Moreover, permission changes over ZTA should be orchestrated in minutes, eliminating the friction and annoyance of security procedures for employees and devices. In this paper, we focus on the potential of AI algorithms in the automation and orchestration for ZTA components.

1.1 Principles of zero trust

The concept of zero trust was first introduced in 2010 by John Kindwig, an analyst at consulting firm Forrester, who proposed the core idea of ZTA: "there are no longer trusted or untrusted networks, users and interface on security devices"[15, 16]. The ZTA automation and orchestration that our research paper focuses on was proposed by another Forrester researcher, Chase Cunningham. His zero trust extended (ZTX) research report published in 2018[17] extends ZTA capabilities from micro-isolation to visibility, analytics, automation and orchestration.

With the growing trend of Internet security issues, many research institutes and organizations are beginning to pay attention to ZTA and offer different insights. Google began building the zero-trust-based BeyondCorp system in 2011 and published a series of papers for a comprehensive introduction to BeyondCorp[18–23]. BeyondCorp always follows that access to services which depends on the contextual factors of authenticated, authorized, encrypted users and their devices rather than the network to which connected. In 2019, Gartner extended adaptive security architecture (ASA) and continuous adaptive risk and trust evaluation (CARTA) to zero trust network access (ZTNA), which is used to phase out the VPN-based service access[1]. In 2020, the national institute of standards and technologies (NIST) released the version 2 of SP-800-207: zero trust architecture[2], which provides detailed guidance on the design of zero-trust architectures based on a document format.

The main purpose of ZTA is to enhance security. Although enterprises or organizations propose different strategies to understand and implement ZTA depending on their application environments, they are all based on the following three principles:

1) Access control should be resource-centric and context-aware.

2) All users and devices must be authenticated and authorized based on dynamic policies before accessing the resources, following the least privilege policy.

3) Improve security by continuously monitoring the integrity and security of owned or associated assets.

1.2 Existing surveys

Although a large number of studies on ZTA have been published, there are a few literature reviews on ZTA. A brief summary of the existing surveys on ZTA is provided in Table 1. In particular, we classify the existing review works based on the following five categories:

Q1: Details of ZTA principles.

Q2: Comparison of security technologies based on perimeter and non-perimeter.

Q3: Categorization and revision of ZTA components.

Q4: Challenges of ZTA migration, automation and orchestration.

Q5: Future research directions of ZTA.

Evan Gilman's book "Zero Trust Networks"[31] begins with an introduction to the basic concepts of zero trust and describes step-by-step methods and techniques for implementing zero trust networks. It also examines the problems that zero trust may face from an attacker's view. Similarly, Jason Garbis, in the book "Zero Trust Security"[32], looks at enterprise security and IT infrastructure from a zero-trust perspective. He also explains how zero-trust security can have an impact on network and security system integration. The existing surveys focus on basic concepts of ZTA[12], migration strategies[24], economic analysis[25], intrusion detection[26] and authentic-

Table 1 Existing surveys on ZTA

Ref	Scope	Q1	Q2	Q3	Q4	Q5
Yan and Wang[12]	ZTA technological framework and application scenarios	√	–	√	×	√
Teerakanok et al. [24]	ZTA migration and deployment	√	×	√	–	√
Buck et al. [25]	ZTA research framework and research direction	√	×	–	×	√
Alevizos et al. [26]	ZTA model and blockchain-based intrusion detection	√	√	√	×	–
Syed et al. [27]	ZTA authentication and access control	√	×	√	–	√
He et al. [28]	ZTA core technologies	√	×	√	×	√
Pittman et al. [29]	Zero trust tenets on data object	√	×	–	×	×
Sarkar et al. [30]	Zero trust cloud networks	√	×	√	×	√
This work	AI-based automation and orchestration of ZTA	√	√	√	√	√

ation[27]. Yan and Wang[12] review the key technologies in the components of ZTA, and their application in real-world scenarios. The advantages of ZTA and the existing challenges are also presented. Teerakanok et al.[24] investigate the challenges, steps and matters to be considered in migrating from a legacy architecture to ZTA. Buck et al.[25] analyze the disadvantages and costs of ZTA from an economics and user perspective based on blockchain. Alevizos et al.[26] also use blockchain to enhance the zero-trust architecture of the endpoint and review state-of-the-art blockchain-based intrusion detection systems. Syed et al.[27] survey the latest technologies available for authentication and access control in ZTA different scenarios and discuss ZTA encryption, micro-segmentation and security automation methods.

Existing surveys provide a careful review and analysis of different ZTA theoretical frameworks and application scenarios. However, none of them elaborates on the potential benefits of the automation and orchestration of ZTA using AI techniques. In the wide range of ZTA application scenarios, where ZTA needs to process and analyze huge amounts of data from different sources, researchers have shown increasing interest in AI-driven automation and orchestration, which can provide assistance to ZTA in data classification, authentication and access control[12]. Therefore, our main focus in this survey is to fill the gap by developing a systematic review of AI-focused approaches important for ZTA automation technologies from a technical perspective in conjunction with existing surveys.

1.3 Scope and contribution

The scope and organization of this survey are shown in Fig. 1. We first discuss the motivation for using AI technologies in ZTA automation and orchestration and compare deperimetrized-based and perimetrized-based trust architectures. We then discuss the categorization and role of AI algorithms, and how they can be applied to ZTA automation and orchestration. Section 2 reviews traditional perimetrized architecture and provides a fine-grained delineation of ZTA logical components and data sources. Afterwards, we delve into AI-based solutions in ZTA automation and orchestration. We also discuss possible challenges and future research directions for the use of AI technologies in ZTA. Section 3 identifies problems in the implementation of ZTA component automation and describes the role of AI technologies in automating

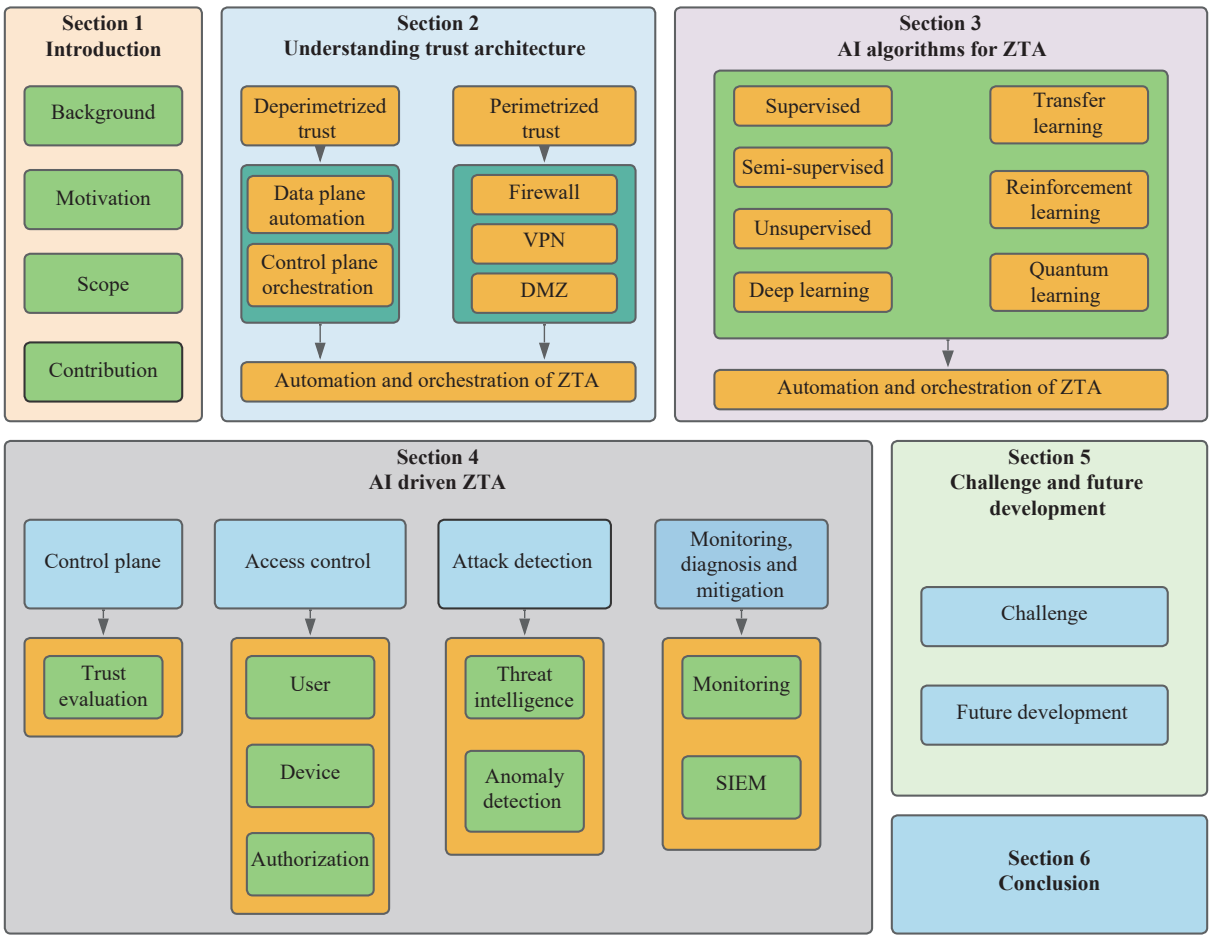


Fig. 1 Organization and structure

the implementation of different ZTA components. Our goal is to use AI technologies to facilitate ZTA automation and orchestration, which will help further improve its efficiency and performance. Section 4 provides an overview of existing AI-based solutions. Section 5 describes limitations and challenges, and points to future research development. Section 6 summarizes the survey paper.

1.4 Contributions

The main contributions of this paper are summarized as follows:

1) We comprehensively review and compare existing perimetrized-based and deperimetrized-based trust architectures.

2) We provide an in-depth analysis of existing AI technologies for ZTA automation and orchestration.

3) We discuss the challenges of implementing AI-based solutions in ZTA automation and future developments.

2 Understanding trust architecture

In this section, we provide a fine-grained categorization of the logical components, data sources of ZTA, and discuss the ZTA automation workflow. We also compare the difference between perimetrized and deperimetrized architecture in Table 2.

2.1 Perimetrized architecture

Information security gained widespread attention after World War II, researchers defended against external attacks by building physical perimeters around computer systems and stored information[1]. The core concept of perimeter-based protection is allowing trusted users to access the internal network and blocking untrusted users.

All users, services, infrastructure and assets exist only within the internal network. The architecture considers all internal users to be trusted with unrestricted access to internal resources; Any external users are untrusted and cannot access any services or devices inside the network. The perimeter-based security architecture effectively defends against incidents such as malware, phishing, denial of service and zero-day attacks[33].

Recently, large amounts of data resources are migrating to the cloud, and users are expanding from human users to IoT devices. The traditional sense of network perimeter is being disrupted, which leads to attacks from the outside becoming more penetrating and dynamic. The attack surface has been expanded, many attacks are launched from the inside, and perimeter-based defences are no longer effective against attacks from the inside.

Firewalls protect assets by isolating private networks from public networks by filtering traffic and blocking access to untrusted sources or IP addresses[34]. But the disadvantages of firewalls are also obvious, once an attacker breaches the network′s defensive perimeter, the firewall cannot stop him from acting illegally on the internal network.

VPN is often used for access to remote networks, where a secure connection is established between the local network and the remote network by encrypting the communication data. While this strategy is effective in securing communications, it poses a threat to corporate assets because it requires traversal of the corporate infrastructure. VPN is effective in securing communication connections, but it has obvious drawbacks as well. VPN uses static authentication and cannot continuously verify user identity and endpoint trust during user access. VPN is also unable to define and restrict user privilege, users can access and steal intranet resources with impunity once they connect to VPN.

The DMZ network provides security for the internal network with an additional layer of security. The DMZ is generally located between the two firewalls, external network traffic will enter the DMZ after passing through the first firewall and will be sent to the second firewall after a security review by the DMZ[35]. The DMZ′s policy of security defence by using multiple firewalls in the system is called defence-in-depth security policy. The advantage of DMZ is that dual firewalls make attacks more difficult, and attackers need to break through two layers of firewalls to bring down the network. In addition, even if one firewall fails, network traffic can be switched to a backup firewall to avoid a potential attack[36]. Although the DMZ defence policy deepens the depth of defence, it relies too

Table 2 Comparison between perimetrized and deperimetrized architectures

Features	Perimetrized architecture	Deperimetrized architecture
Principle	Trust and verify	Never trust, always verify
Privilege	Unlimited privilege (Internal)	Least privilege
Boundary	Always trust (Internal)	Micro segmentation
Authentication	Single and static	Continuous, multimodal and dynamic
Authorization	Static	Dynamic and fine-grained
Access control	Policy-based	Resource-centric and context-based
Security	Network traffic monitoring	Continuous monitoring, diagnosis, mitigation

much on the firewall. If an attacker uses some methods to bypass the firewall, for example, using malicious emails to gain direct access to the internal network, the DMZ will fail. Moreover, DMZ cannot identify attacks by trusted devices on other trusted devices.

In comparison, the perimeter-based protection approach effectively protects against external attacks, but it ignores the internal attacks. Perimeter-based defence architecture is no longer suitable for today′s cyber attacks, privileged access paths become riskier and make perimeter-based defence difficult to defend against illegal attacks from legitimate internal users. ZTA′s principle of least privilege and micro-segmentation effectively limits the privileges of internal users and avoids the risk of unrestricted lateral movement of users within the network.

2.2 Deperimetrized architecture

The national institute of standards and technologies (NIST) divides the zero-trust model into a control plane, a data plane and a data source[2]. Among them, the control plane is primarily responsible for decision making, the data plane is responsible for executing the decisions made by the control plane, and the data source is predominantly responsible for providing data and policy rules to the control plane. We provide a more refined division of logical components and data sources on this basis and illustrate the process of their automated application.

Fig. 2 shows the automation process of ZTA. The accessing subject receives session-based authentication generated by the PA before accessing the resource. Then identity information is sent to the PE to decide whether to grant permission. After PE decides to grant permission, PA configures the policy enforcement point (PEP) to allow the session to start, otherwise, it closes the session. The access subject still accepts continuous tracking and verification of access behaviour and identity by the security system during access to resources. Once illegal behaviour is detected, the security system will inform PE to stop authorizing the session and the PE will close the session.

2.2.1 Intelligent control plane

In the traditional ZTA control plane, the policy decision point (PDP) is divided into policy engine (PE) and policy administrator (PA) for making and executing decisions[2]. Trust evaluation is the core algorithm of PE, which evaluates the trustworthiness of the subject based on data from different sources. The PE decides whether to grant the subject access to resources based on the trust evaluations via the supplied credentials. PE is essentially access control to user identity and devices. Therefore, in order to achieve the accuracy and timeliness of access control, authentication and authorization, it is necessary to automate the trust evaluation process and dynamically adjust the decision through trust value updates in real-time based on the continuously collected information.

2.2.2 Authentication and ID management

In ZTA, the PA is primarily responsible for establishing the communication path between the accessing subject and the resource, and then generating session-specific authentication credentials. Due to the wide range of ZTA application scenarios, authentication no longer refers to verifying user identity alone, but also includes authen-

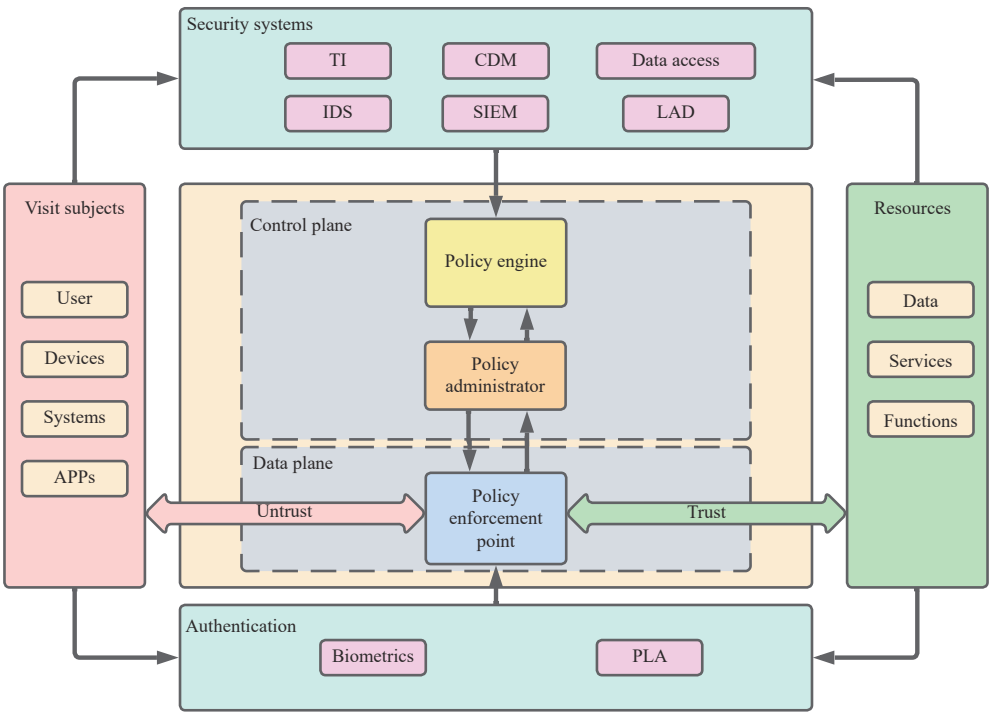


Fig. 2 ZTA components workflow

tication of IoT devices and cloud services. Accurate authentication can directly reduce the risk of being attacked by falsified identity, so we divide authentication into user authentication and device authentication. Biometrics and physical layer authentication (PLA) are considered effective authentication solutions, with biometrics identifying users based on their unique biometric features and physical layer identification identifying them by verifying device channel state information (CSI) or radio frequency fingerprint (RFF).

ID management is responsible for creating, storing and managing user identity information, such as access rights, biometrics, etc. The enterprise public key infrastructure (PKI) is responsible for generating authentication and communication encryption certificates issued by the system for devices, services and users. Therefore, even though biometric authentication and PLA can dynamically verify the identity of the access subject, the generated authentication information still needs PKI for communication transmission.

2.2.3 Attack detection

Automated attack detection can help ZTA defend against internal and external attacks. Nevertheless, attack detection is not a single technique or algorithm, but a combination and coordination of multiple techniques. We divide them into three categories based on different attack phases: Automated threat intelligence collects information about potential attacks before they occur; Automated intrusion detection detects ongoing attacks promptly; And automated log-based anomaly detection continuously monitors the internal operation of the network to identify and locate anomalous locations even if an attack breaks through the first two layers of detection. The coordination of multiple automation technologies can secure the ZTA to a large extent.

2.2.4 Connection monitoring

The data plane is used for the actual communication between applications and its main role is to monitor the connection between the subject and the resource. All actions taken by the subject while accessing the resource are recorded by the logs, so it is possible to stop possible illegal actions by legitimate users by checking for abnormal log records. The continuous diagnostics and mitigation (CDM) system and the security information and event management (SIEM) system are also used to collect information and provide response strategies.

CDM mainly collects information about assets and updates configurations, and its capabilities include asset management, identity and access management, network security management and data protection management. SIEM systems analyze relevant security information within a system and provide response strategies, and are composed of multiple monitoring and analysis components such as log managements (LMS), security information management (SIM) and security event management (SEM). LMS is used as a traditional log collection and storage tool; SIM collects data from multiple security-related tools or systems; SEM is based on a proactive monitoring and analysis system that includes data visualization, event correlation and alerts.

3 AI algorithms for ZTA

In light of the increasing demand for AI technologies in zero-trust[37, 38], we focus on, but are not limited to AI technologies that can be applied to the automation and orchestration of ZTA. Fig. 3 shows the categories of ZTA components which can use AI algorithms. We divide ZTA components into four parts: control plane, authentication, attack detection and resources monitoring.

3.1 Control plane

The control plane is the brain of the ZTA, and it evaluates and analyzes the data from other components for decision-making. The control plane is divided into two main parts: trust evaluation and access control.

3.1.1 Trust evaluation

As mentioned in Section 2, the trust algorithm evaluates the trustworthiness of the subject based on different data sources to decide whether to grant access[2]. It can support the automation of the modules inside the policy engine, which handles decision-making and flexible control over the tenets of ZTA by constantly assessing the

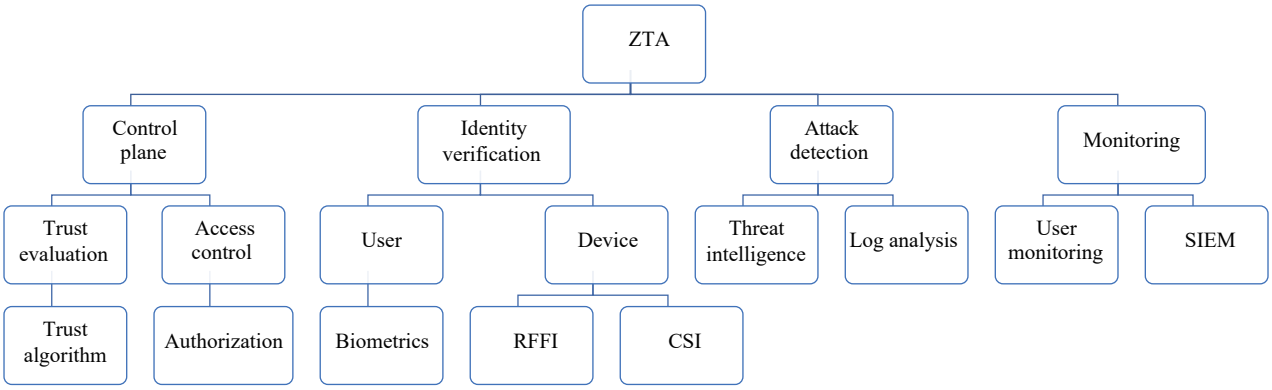


Fig. 3 AI classes and applications in ZTA

trustworthiness of several network devices and enterprise systems. However, automating the modules of ZTA′s PE is highly challenging and non-trivial, because the access grant to network resources is often governed by the underlying trust evaluation algorithm[2]. To this end, advanced machine learning techniques can be applied to handle effective trust evaluation; Wang et al.[39] have analyzed several conditions where machine learning-based trust evaluation methods enable improving the trustworthiness of the underlying devices in a distributed system.

The clustering algorithm performs binary clustering on the information features collected by different ZTA components, labelled as trustworthy or untrustworthy in the trust evaluation. This method can be applied to ZTA′s access control decision-making to decide whether to grant or deny access. Similarly, deep reinforcement learning can enhance the performance of the access control model by strengthening the trust evaluation policy by rewarding and punishing each evaluation action in an active trial-and-error manner[40, 41]. Moreover, transfer learning can be used to reduce the training time for the models because of its inherent knowledge-sharing approach.

3.1.2 Access control

In ZTA, access control is a vital security protection method, trust evaluation can be considered as an import access control policy. Traditional access control refers to restricting what a user and a program are capable of acting on his behalf can perform directly[42]. With the advent of the era of 5G and IoT, more and more intelligent devices have joined the network, and access control is no longer limited to restricting users′ and programs′ access to data. Access control in ZTA is redefined as only authenticated and authorized subjects can access resources, other subjects will be denied access. Subjects can be understood as users, applications (or services), or combinations of devices; resources can be interpreted as any objects connected to the network, such as printers, or computing resources[2]. In addition, dynamic grants or revocation is also the primary function of the ZTA PE.

Before we discuss AI-based automated access control that can be applied to ZTA, it is also essential to focus on the different application scenarios of access control. Ravidas et al.[43] investigated the development trend of access control in IoT and analyzed the existing IoT authorization framework. Similarly, Ouaddah et al.[44] reviewed the goals, models and mechanisms of different access control schemes in IoT and analyzed their security and privacy requirements. In order to solve the lack of flexibility and scalability of access control based on symmetric encryption and public-key encryption, Zhang et al.[45] reviewed access control attribute-based encryption (ABE) in cloud computing, and proposed the classification and evaluation criteria of ABE.

There are three main types of access control techniques: role-based access control (RBAC), attribute-based access control (ABAC), and fine-grained access control (FGAC)[46]. The access control policy in ZTA is a combination of these three techniques, which automatically assign roles or permissions to users based on their static and dynamic attributes for fine-grained access control. Static attributes can be understood as user identity, while dynamic attributes include user access request time and location. Different roles within an organization have different permissions. Due to powerful classification capability, supervised learning can be used to automatically assign role permissions based on user attributes, or even directly assign user permissions. Those AI approaches can significantly reduce the time and improve the accuracy of privilege assignments compared to manual privilege assignments.

3.2 Identity verification

Authentication is the primary factor in the control panel′s decision to grant or deny access. Existing authentication technologies can be divided into biometric identification and physical layer authentication, which are used to authenticate human users and devices, respectively.

3.2.1 Biometric authentication

Many biometric features of the human body are unique, such as the iris and fingerprints[47]. However, these traditional surface biometrics of the human body are no longer reliable because they can be easily lost and copied, such as fingerprints left on a glass. With the development of wearable devices, features of internal human organs can also be effectively captured. However, how to classify and identify the collected biometric features is the main challenge that biometrics currently encounters. The application of artificial intelligence can extract and classify the features obtained from wearable devices to verify the user′s identity.

A detailed investigation of the application scheme of machine learning classification methods in continuous multimodal biometric authentication is presented by Ryu et al.[48] In automated user identification, the user biometric features stored in the ID management system are first quantified, and then the features are classified by machine learning supervised algorithms such as K-nearest neighbors (KNN) and decision tree (DT) for model training to perform authentication. Deep learning algorithms such as convolutional neural network (CNN) can automatically extract and learn the user′s biometric vector features directly from the information collected by biometric monitoring devices to confirm the user′s identity. Deep transfer learning has also been used to address the problem of poor authentication performance due to insufficient user biometric data.

3.2.2 Physical layer authentication

Continuous authentication aims to continuously verify the identity of the endpoint during a communication session. AI-based PLA is considered as a potential solution, where AI algorithms can effectively extract device

features from the communication channel and continuously verify the identity of users and devices[49]. Xie et al.[50] conducted a detailed survey on existing PLA technologies, and they classified IoT device features into detecting device-based and channel-based features.

Compared to device-based features, channel-based features are more difficult to copy or imitate, which provides improved security for device authentication. However, channel-based features are extracted from device communications, and manually distinguishing the communication features of different devices is impractical. Therefore, in ZTA automated device identification, deep learning can be used to automatically learn device channel features to distinguish device identity, thereby improving device authentication performance.

3.3 Attack detection automation

Automated attack detection was the main means for ZTA to prevent attacks from internal and external. Attack detection techniques can be divided into threat intelligence collection and log-based anomaly detection.

3.3.1 Threat intelligence collection

Automated threat intelligence collection requires AI algorithms to sense, reason and detect advanced cyber attacks[51]. Currently, most cyber threat intelligence comes from open-source communities such as different hacker forums, blogs and tweets[52–54]. Therefore, using AI technologies to extract useful information automatically is currently an immediate and effective way of extracting threat intelligence. Cascavilla et al.[55] reviewed existing cyber criminal activities and supplemented their classification for risk assessment. Cyber threat intelligence sharing is considered as an effective means to address the increasing number of cyberattacks, and Wagner et al.[56] investigated existing automated cyber threat intelligence sharing techniques.

In ZTA, we believe that AI technologies are the primary solution for automating cyber threat intelligence collection. The clustering algorithms of unsupervised learning can group different patterns of threat intelligence according to their similarity[57, 58]. The log-based anomaly detection method uses AI technologies to realize automatic log monitoring and anomaly identification. Because the log data is often in billions, unsupervised learning such as dimensionality reduction algorithms can effectively reduce the computational cost and improve the efficiency of anomaly identification[59]. Furthermore, deep reinforcement learning is also used to collect threat intelligence, reinforcement learning subjects actively learn to extract more accurate threat intelligence through trial and error, which improves the identification performance of threat intelligence[60, 61].

3.3.2 Log anomaly detection

Automated anomaly detection of log files can detect abnormal or illegal behaviours of ZTA internal resources in time. Soldani and Brogi[62] reviewed anomaly detection methods and anomalies cause analysis methods in cloud services. Landauer et al.[63] investigated clustering methods for analyzing large volumes of log data. Likewise, Chalapathy and Chawla[64] provided an overview of deep learning-based anomaly detection methods and evaluated the effectiveness of these methods.

According to our survey, semi-supervised learning is mainly used to detect logs with abnormal conditions in ZTA. Although log anomaly detection can effectively detect known attack behaviours, the detection performance will drop sharply in the case of unknown attacks. Semi-supervised learning uses large amounts of unlabelled data, as well as simultaneous use of labelled data, to perform pattern recognition work. It avoids the waste of data and resources, and solves the problems of weak generalization ability of supervised learning models and inaccuracy of unsupervised learning models.

3.4 Automated resources monitoring

Automated resource monitoring is an organization resource-centric security approach that continuously monitors the behaviour of accessing subjects on resources. The main purpose of automated resource monitoring is to avoid illegal actions from legitimate users or devices.

3.4.1 SIEM orchestration

Although the attack detection methods mentioned above can help ZTA effectively detect internal and external threats, they are unable to effectively classify and manage these security events. Attack detection methods also cannot automatically alert the security administrator or take countermeasures automatically. Automated SIEM orchestration is an effective solution to this problem. It can automatically collect and analyze information from the attack detection system, and automatically trigger security alerts to provide repair or mitigation solutions. Supervised learning classification algorithms are used to automatically classify various security events, solving the problem of inefficient manual classification[65].

3.4.2 Automated user behaviour monitoring

Although users and devices in the ZTA architecture have been continuously authenticated and authorized, it doesn't mean that they are always credible, incidents such as fraudulent use of identity may occur[2, 66]. Continuous monitoring of internal users and equipment is an effective solution. Modelling user behaviour extracted from logs using artificial intelligence techniques is the main solution to automate abnormal user identification. Since there are few papers reviewing AI-based user abnormal behaviour monitoring, we provide potential AI-based approaches to user behaviour detection in Section 4.4.1.

Cluster algorithms detect legitimate users' illegal behaviours by clustering normal user behaviours into a cluster, while users away from the clustering are labelled as abnormal users. Similarly, the deep learning algorithm

learns the daily access habits of users, and classifies them into normal and abnormal according to their behaviours. In addition, deep learning can also predict the possible behaviours of users based on their context and historical behaviours, and detect or prevent threats from them in time.

4 AI-driven ZTA

ZTA automation and orchestration can be considered as the process of reducing frequent mediation by security personnel via automating the detection and prevention of cyber threats. In this section, we review the AI approaches for ZTA components to ZTA automation and orchestration. Tables 3 and 4 surveyed the recent AI-based approaches to trust evaluation, authentication, attack detection and system monitoring, respectively.

4.1 Experience-driven trust evaluation

Traditional trust evaluation is performed by quantifying trust-related attributes such as historical interaction information by using Bayesian inference[136], weighted average models[137], and other methods. Although these methods can assess trust to a certain extent, with the advent of the era of big data, traditional trust evaluation methods have become difficult to carry exponential trust-related attribute data, which greatly affects the accuracy of trust evaluation[39]. Moreover, traditional methods must rely on known trust-related attributes for trust evaluation and cannot be applied in the absence of a priori knowledge.

The rapid processing of big data by AI makes AI-based trust evaluation methods suitable for existing complex network application scenarios. Online social networks (OSN) is one direct way to obtain user features, supervised learning classifies users into trustworthy and untrustworthy by treating trust evaluation as a classification problem[67–69], or quantifies trust values directly using continuous values[70–72] based on OSN users′ features.

However, supervised learning must have labelled data to train the model, in most ZTA practical application scenarios, users and device features lack clear labels, and unsupervised learning such as K-means[73–76] can solve this problem by clustering trust objects without label into a different level of trust groups. To further improve unsupervised learning performance, semi-supervised learning, which combines supervised and unsupervised learning, can be used to optimize the clustering boundaries. Multi-class supervised learning algorithms such as support vector machine (SVM) and random forest[77–79] are used to find the optimal decision boundary between trusted and untrusted clusters. Moreover, reinforcement learning[80–84] can be used to find the optimal trust evaluation policy and improve trust evaluation models by continuously interacting with the surrounding environment by trial and error[138].

Since AI-based trust evaluation methods have high time complexity which requires significant computational and time resources for model training, improving the performance while reducing the computation time of trust values is important for automating trust evaluation. To achieve this, distributed learning[85, 86, 139–141] and transfer learning[40] can be used to improve trust evaluation model performance and reduce model training time costs, respectively. Similarly, the quantum learning-based trust evaluation model[142, 143] can further optimize the trust model and reduce the computational complexity of the model with the high parallelism of quantum computing[144, 145].

4.2 Contextual continuous access control

Access control restricts the subject′s access to objects through authentication and authorization. Since it is important to determine whether the subject requesting access is legitimate, authentication and authorization are fundamental considerations when trying to implement zero trust[27]. In this section, we provide an overview of AI-based techniques for access control.

4.2.1 Automated user authentication

Existing user authentication technique has shortcomings, knowledge-based (password, token, etc.) authentication methods are only established when the subject requests access and the user is not verified and tracked after passing the authentication[146]. Biometric authentication methods also require specific specialized equipment to monitor which elevated the difficulty of continuous authentication. Therefore, continuous, multimodal and contextual biometric authentication techniques are important for ZTA to verify user identity.

Because traditional physiological features such as fingerprints and irises are easy to obtain or copy, continuous authentication[87–90, 147] requires uninterrupted confirmation of user identity based on different features which should meet the conditions of universality, uniqueness and uninterruptedness[148], such as electrocardiogram (ECG). Contextual authentication[91–95] is similar to continuous authentication, but contextual authentication focuses on changes in the user′s physiological and behavioural features over time, including pre-authentication behaviour. To further improve the security and accuracy of identity verification, multimodal biometric authentication [96–99, 149, 150] combined different biometric authentication methods to avoid the uncertainty of a single authentication method, which is similar to multi-factor authentication (MFA)[151].

4.2.2 Automated device authentication

ZTX[17] considers IoT devices in a zero-trust network as a threat to network security, therefore allowing enterprises to segment, protect and restrict devices connected to the network and treat them as zero-trust devices (ZTD).

Table 3 AI approaches for ZTA trust evaluation and authentication

Ref.	Objective	Model	Type	Evaluation data	Contribution	Application scenarios	Claim advantages
[67]	Classification	SVM	Sup.	Weibo	TE	OSN	High trust predicting accuracy
[68]	Classification	Multi.	Sup.	Twitter	TE	OSN	Lightweight feature selection
[69]	Classification	Bayesian	Sup.	Twitter, Facebook	TE	OSN	No need to build trust relationships in OSN
[70]	Prediction	LR	Sup.	Track1	TE	OSN	More accurate and stable result
[71]	Classification	DT & ANN	Sup.	N/A	TE	VANET	Direct and recommended TE strategy
[72]	Prediction	LSTM	Sup.	Ori.	TE	IoT	Consider the time-dependent features
[73]	Cluster	K-mean	Unsup.	N/A	TE	IoT	Low error rate
[74]	Cluster	K-mean & FCM	Unsup.	Epinions, Douban, Flixster	TE	OSN	Co-clustering method
[75]	Cluster	K-mean	Unsup.	N/A	TE	WSN	Identify legitimate and malicious nodes
[76]	Cluster	K-mean	Unsup.	N/A	TE	WSN	Defend against malicious attacks
[77]	Classification	K-mean & SVM	Unsup.+Sup.	CRAWDAD	TE	IoT	Identify trust boundaries
[78]	Classification	K-mean & SVM	Unsup.+Sup.	N/A	TE	UASN	Improve the security and lifetime of network
[79]	Classification	K-mean & RF	Unsup.+Sup.	CRAWDAD	TE	IoT	Isolates the trustworthy and untrustworthy nodes
[80]	Score	LR	RL	N/A	TE	OSN	Maintain user privacy and confidentiality
[81]	Classification	RL	RL	Veins, OMNet++, SUMO	TE	VANET	Learning from feedback on historical assessments
[82]	Score	RL	RL	N/A	TE	UASN	Improve efficient trust update
[83]	Privacy protection	Q-Learning	RL	Taxi trajectory	TE	IoT	Prevent co-cheating
[84]	Score	DoubleDQN	RL	Filmtrust	TE	OSN	Find reliable trust paths without contact
[85]	Classification	SVM, KNN	Distri.	CRAWDAD	TE	VANET	Identify and eradicate malicious vehicles
[86]	Classification	Learning automata	Distri.	Advogato	TE	OSN	Identify reliable trust paths
[40]	Score	DDPG, DQN	RL, TL	Mnist	TE	IoT	Trust evaluation at different granularity
[87]	UAuthn.	CNN	Sup.	MWM-HIT, PTB, CYBHi	AC	ECG	Efficient signal feature extraction
[88]	UAuthn.	SVM	Sup.	Ori.	AC	ECG	Identify regions of interest from raw signals
[89]	UAuthn.	DT	Sup.	PhysioBank	AC	Human activity	Short authentication time

Table 3 (continued) AI approaches for ZTA trust evaluation and authentication

Ref.	Objective	Model	Type	Evaluation data	Contribution	Application scenarios	Claim advantages
[90]	UAuthn.	SVM, LSTM	Sup.	Ori.	AC	Finger gesture	Cross-domain authentication
[91]	UAuthn.	AE	Sup.	Crowdsignals	AC	Smart phone	Reduce computational burden
[92]	UAuthn.	RF	Sup.	Ori.	AC	Keystroke dynamics	Contextual awareness
[93]	UAuthn.	LSTM	Sup.	UMDAA	AC	Face	Contextual awareness
[94]	UAuthn.	LSTM	Sup.	Ori.	AC	Smart phone	Consider different user behaviours
[95]	UAuthn.	SVM	Sup.	NetHealth	AC	Wearables	Robustness against attacks
[96]	UAuthn.	RNN	Sup.	Ori.	AC	EEG, Gait	Stable performance
[97]	UAuthn.	CNN, QG-MSVM	Sup.	PTB, CYBHi, LivDet2015, FVC2004	AC	EEG, FP	Biometric fusion and data augmentation
[98]	UAuthn.	CNN	Sup.	Ori.	AC	Finger nail Plates/Knuckles	Fusion of biometric attributes
[99]	UAuthn.	CNN	Sup.	Synthetic	AC	Face, voice	Online learning
[100]	DAuthn.	RPCA, RF	Sup.	Ori.	AC	RFFI	Improve wireless device security protection
[101]	DAuthn.	CNN	Sup.	Ori.	AC	RFFI	Use spectrogram to improve classification
[102]	DAuthn.	CNN	Sup.	Ori.	AC	RFFI	Low power consumption and cost
[103]	DAuthn.	CNN, RNN	Sup.	Ori.	AC	CSI	Hybrid methods achieve higher accuracy
[104]	DAuthn.	SVM	Sup.	CIRs	AC	CSI	Effective feature selection
[105]	DAuthn.	GAN	Sup.	Ori.	AC	CSI	GAN was more accurate at lower SNR levels
[106]	DAuthn.	KNN	Sup.	Ori.	AC	CSI	Identify Wi-SUN devices

N/A: Not claim; Ori.: Original datasets.
ECG: Electrocardiogram; VANET: Vehicular Ad Hoc network.
UAuthn: User authentication; DAuthn: Device authentication.
OSN: Online social networks; WSN: Wireless sensor network; UASN: Underwater acoustic sensor network.
FP: Fingerprint; RFFI: Radio frequency fingerprint identification; CSI: Channel state information.

Table 4 AI approaches for ZTA attack detection and monitoring

Ref.	Objective	Model	Type	Evaluation data	Contribution	Application scenarios	Claim advantages
[107]	Classification	SVM, LDA	Sup.+Unsup.	Ori.	TI	Hacker forum	Integrated with traditional security controls
[108]	Classification	MLP	Sup.	Ori.	TI	Forum	Extract critical posts
[109]	Classification	CNN	Sup.	Ori.	TI	Forum	End-to-end cyber-threat intelligence management platform
[110]	Classification	BERT	Sup.	Twitter	TI	Forum	Discovery of trending attacks patterns and vulnerabilities
[111]	Classification	DT & ANN	Sup.	N/A	TI	VANET	Direct and recommended TE strategy
[112]	Classification	CNN	Sup.	Ori.	TI	Forum	Improve the efficiency and accuracy of TI identification
[113]	Classification	LSTM	Sup.	Ori.	TI	Hacker forum	Proactive and timely TI
[114]	Classification	LSTM	RL	Ori.	TI	Forum	Constructing a dictionary template of TI entities
[115]	Classification	LSTM	Sup.	HDFS, OpenStack	LAD	System log	Build workflows from underlying system logs
[116]	Classification	LSTM	Semi	HDFS, OpenStack	LAD	System log	End-to-end log anomaly detection
[117]	Classification	CNN	Sup.	HDFS	LAD	Big data	Automatic learning of event relationships in system log
[118]	Classification	CNN, AE	Sup.	HDFS	LAD	Big data	Generate anomaly score
[119]	Cluster	LSTM	Unsup.	LANL	LAD	System log	Reduce overall storage costs
[120]	Cluster	LSTM	Unsup.	HDFS	LAD	System log	No need data preprocessing
[121]	Classification	DBSACAN, RNN	Semi	HDFS	LAD	System log	Immunity to unstable log data
[122]	Classification	CNN, LSTM	Semi	HDFS	LAD	System log	Reduce training time
[123]	Classification	LSTM	TL	HDFS	LAD	System log	Reduce the effect of noise in anomalous log sequences
[124]	Cluster	AP	Unsup.	Ori.	Monitoring	Web log	Good time complexity and detection rate
[125]	Cluster	K-means	Unsup.	Ori.	Monitoring	Web traffic	N/A
[126]	Cluster	K-means	Unsup.	Ori.	Monitoring	Web log	High detection rate and low false alarm rate
[127]	Classification	LSTM	Sup.	CMU-CERT v6.2	Monitoring	Activity logs	Detect insider threats
[128]	Classification	LSTM, SVM	Sup.	CMU-CERT v6.2	Monitoring	Activity logs	Efficient feature extraction
[129]	Classification	LSTM	Sup.	CERT v4.2	Monitoring	Session activities	Automatic anomaly detection
[130]	Cluster	K-means	Unsup.	KDD Cup 1999	Monitoring	SIEM	Big data processing
[131]	Classification	CNN, LSTM	Sup.	NSLKDD, CICIDS2017	Monitoring	SIEM	Learning-based models for network intrusion-detection
[132]	Classification	NN, SVM	Sup.	NSL-KDD	Monitoring	SIEM	Studied the impact of parameters in NN on classification accuracy
[133]	Classification	Multi.	Sup.	Ori.	Monitoring	SIEM	Automatic event categorization tool
[134]	Classification	Multi.	Sup.	Ori.	Monitoring	SIEM	Covered a wide range of events
[135]	Classification	Multi.	Sup.	Ori.	Monitoring	SIEM	Enhanced detection and management of business risks

N/A: Not claim; Ori.: Original datasets.
TI: Threat intelligence; LAD: Log anomaly detection.
AP: Affinity propagation; Multi.: Multiple AI models.

Shah et al.[152] specially designed a lightweight device-to-device authentication protocol for ZTA called lightweight continuous device-to-device authentication (LCDA), which uses mathematical functions to dynamically generate a session key to verify the identity of the device. Because traditional methods of device authentication that rely on IP addresses are susceptible to tampering or forgery[101], physical layer authentication (PLA) is used to verify the device identity in wireless communication, and existing PLA techniques mainly identify the device identity through radio frequency fingerprint (RFF) and channel state information (CSI).

RFF is similar to human biometric fingerprints, the difference is that RFF is extracted from a wireless device communication signal. The main stages of an RF fingerprint-based wireless device identification system are signal capture, feature extraction and classification. After capturing the signal, unique features need to be extracted from different parts of the signal[153]. Therefore, radio frequency fingerprint identification (RFFI)[100–102, 154] is more secure and reliable than using IP for wireless device authentication.

CSI describes the channel state of wireless communication, and CSI variation is unique from device to device which can prevent spoofing attacks in PLA. AI techniques can perform dimensionality reduction, denoising and feature extraction on CSI data[155]. Therefore, the identity of wireless devices can be verified by using AI to classify CSI in ZTA[103–106].

4.2.3 Automated authorization

Cloud is also a major application scenario for ZTA because many applications store their data in the cloud. Therefore, a dynamic access control model is needed to handle access requests from a large number of dynamic users. Riad et al.[156] proposed a hierarchical access control scheme with dynamic revocation threshold vectors based on multi-dimensional access control to dynamically authorize or revoke users with multiple rights in the cloud. This scheme revokes user rights based on the legal vector in the authorization process, and the revoked users can no longer encrypt the ciphertext, which effectively reduces the computational cost. And only non-revoked users have the right to generate a decryption token to decrypt the ciphertext. The authors also report that the proposed scheme is faster than other schemes in encryption and decryption time.

However, continuous user interaction with the cloud can lead to data breaches. Esposito[157] addressed these issues by orchestrating different access control models. In addition, Esposito also proposed a pseudonym-based privacy protection method to protect users′ personal information. To enhance the privacy of users and the security of encryption schemes, Li et al.[158] proposed a multi-authority ciphertext-based access control method with accountability. This method hides the access policy in the ciphertext from the encrypted file, and only the user policy that matches the access policy in the ciphertext can decrypt the ciphertext. In addition, the authors proposed a tracking protocol to track the identities of file visitors.

4.3 Orchestrating attack detection

Threat intelligence (TI) and system activity logs are important data sources of ZTA, as they provide near real-time feedback to the policy engine for decision-making through the collection or recording of internal and external data.

4.3.1 Automated threat intelligence identification

Threat intelligence is information about threats and guides organizations to improve security to counter threats by mining publicly available resources for vulnerabilities, cyber-attacks and other information. Due to the numerous sources of threat intelligence, an automated system is needed to enable the collection of threat intelligence and to discriminate the authenticity of the collected intelligence. Sentuna et al.[159] discussed the emerging technologies of cyber threat intelligence, they combined the naive Bayes posterior probability function and risk assessment function to propose a threat prediction model.

Hacker forums are an important source of data for cyber threat intelligence, in order to collect cyber threat intelligence from hacker forums, Deliu et al.[107–111] used a supervised learning model as the classifier to classify the data based on security topics. Threat intelligence identification methods based on deep learning[112] and transfer learning[113, 114] have also been used for improving threat intelligence identification performance and reducing model training time.

4.3.2 Automated log-based anomaly detection

System logs provide near real-time feedback on the operation of components within the system and automated anomaly detection of system log files can identify abnormal access activities to resources in a timely manner[115]. System logs often record system operation in a time-series fashion, and supervised learning-based log analysis methods[117, 118] have advantages in automating the extraction of time-series anomaly features. Deeplog[115] focused on building a workflow from the underlying logs and analyzing the detected anomalies. Wang and Ji[116] argued that the performance of Deeplog is unsatisfactory, and they deeply optimized Deeplog and combined the first-order outlier detection algorithm of parameters to propose a semi-supervised anomaly detection model.

However, supervised machine learning strategies that rely on labels are not suitable for real-time anomaly detection systems because data labeling is time and cost expensive. To solve this problem, unsupervised log analysis methods[119, 120] are used to effectively detect anomalies in a log without features. The output anomaly score represents the degree to which a log event is anomalous in terms of its content and temporal context. Semi-supervised learning-based log analysis methods[116, 121, 122] fur-

ther improve the performance of unsupervised learning. Transfer learning-based log analysis methods[123, 160] can effectively reduce training time and improve training efficiency.

4.4 Continuous monitoring, diagnosis and mitigation

Automated anomaly detection can effectively collect information about attacks from both internal and external sources of a system, but it is difficult to effectively diagnose and mitigate the attack. Therefore, the collected information needs to be further tracked and analyzed to make diagnostic decisions and policy updates.

4.4.1 Automated user and device monitoring

Continuous authentication and authorization can only identify the legitimacy of a user or device, but cannot effectively identify the illegal behaviour of a legitimate user. Continuous monitoring of internal users and devices access behaviour to resources is an effective solution to identity masquerading.

The clustering algorithm[124–126, 161, 162] can effectively divide users into groups based on their behaviour. However, user behaviour may change in different scenarios, and this may generate much unknown data. Therefore, Tang et al.[163] proposed a clustering method based on user behaviour trajectory for software system user behaviour analysis. Tang et al.[163] converted the user's access data and operation data to the software into a trajectory matrix and normalize, then calculate the similarity of user behaviours and cluster the user visits and operating habits based on similarity.

Deep learning, such as long short-term memory (LSTM), algorithms[127–129] are used to automatically select user and device behaviour features due to its ability to efficiently capture time series features. Singh et al.[127] proposed an anomaly detection method for network internal user behaviour based on a hybrid machine learning algorithm. Singh et al.[127] focused on analyzing user behaviour sequence to monitor users and detect potential internal threats. However, Singh et al.[127] also believed that existing internal detection methods had problems such as a high false alarm rate and insufficient feature selection. Therefore, Singh et al.[128] continued to propose an internal threat detection method based on user behaviour for key infrastructure to improve feature extraction performance. Compared with the [127], Singh et al.[128] used bi-directional long short-term memory (Bi-LSTM) for efficient feature extraction and used SVM as a classifier to classify user behaviours into normal and malicious. Singh et al.[128] achieved an accuracy of 87.5%, which is higher than LSTM+CNN (75.3%). Similarly, Sharma et al.[129] proposed an abnormal user behaviour detection model, which can use LSTM to model user behaviour in conversation activities.

4.4.2 SIEM orchestration

Although anomaly detection methods mentioned above can help ZTA effectively detect internal and external threats, they are unable to effectively classify and manage these security events. Anomaly detection also cannot automatically alert the security administrator or take countermeasures automatically. Automated SIEM orchestration is an effective solution to this problem. SIEM can automatically collect and analyze information from the anomaly detection system and automatically trigger security alerts to provide diagnosis or mitigation solutions.

However, the existing SIEM system may have defects because the existing data packet analysis scheme cannot adapt to massive data[164]. Therefore, Li and Yan[130] applied machine learning technologies to the SIEM system and proved the feasibility of machine learning to analyze data in the SIEM system. Li and Yan[130] used Logstash to collect system logs from different sources, used K-means to cluster the connection information, and then used the spark or flink framework for real-time calculations. Lee et al.[131] proposed an AI-SIEM system based on a combination of neural network algorithms FCNN, CNN and LSTM. Lee et al.[131] focused on using deep learning techniques to learn normal and threat patterns from the collected information. The main purpose is to improve the accuracy of real alarm classification and reduce the number of irrelevant alarms.

El Hajji et al.[132] focused on data combination techniques from different sources to enhance SIEM systems and used intrusion detector models based on neural networks. The first layer of the model used neural networks to classify system events into malignant and benign; The second layer used SVM to improve classification performance. The experimental results showed that the proposed model has improved classification performance and convergence speed. On the other hand, Hossain et al.[133] believed that manually classifying the events collected by SIEM is a difficult task, so they developed a set of automatic classification tools based on machine learning to solve this problem. In addition, Hossain et al.[133] also experimented with various machine learning algorithms on multiple datasets to find the best text classification model, such as DT and SVM. The test results show that SVM has achieved the best performance on dataset TippingPoint and NetScreen, which are 95.08% and 94.05% respectively.

Automated SIEM systems are also widely used in practical scenarios. Hindy et al.[134] proposed a SIEM system to detect abnormal events in a water supply system controlled by SCADA. Hindy et al.[134] used machine learning to divide the attack data into fourteen different scenarios and reported the scenarios to the security operator. The proposed SIEM model can help operators accelerate the process of mitigating network attacks, but they also point out that the system cannot provide operators

with information on new attack scenarios. Feng et al.[135] believed that the false alarm rate issued by existing SIEM is too high, which is far beyond the processing range of the security operation center (SOC). To solve this problem, Feng et al.[135] proposed a user-centric framework that uses machine learning algorithms to reduce the false alarm rate of security threats.

5 Challenges and future development

5.1 Challenges

Harmonization policy

Although each data source of ZTA has its own operational policies and standards, there is still a lack of a unified policy that governs the automation of ZTA components, including encryption policies, code specifications, etc. The most immediate consequence of the lack of uniform policy is the problem of data heterogeneity. In ZTA, monitoring network traffic and user behaviour within the system is extremely dependent on the log data provided by each security tool, and PAs have to use multiple trust evaluation algorithms to adapt to different data formats, which not only makes the trust evaluation hard, but also leads to performance degradation of the automated trust evaluation model.

Legacy system

With the development of the Internet of things, cloud and other technologies, many devices can be realized by the central control system unified orchestration. But legacy infrastructure, applications, services, etc. still cannot pass zero-trust awareness because there is no concept of least privilege or lateral movement, nor is there any dynamic context-based authentication model that can be used, so the legacy system is vulnerable to a range of security threats[165]. The existing solution is to add an authentication module to the central control system and then define its privileges. Although this solution alleviates the system legacy problem to some extent, it requires the accessing subject to traverse the infrastructure directly, which violates the network micro-segmentation principle of zero trust.

Data inconsistency

The data for trust evaluation comes from different data sources, but the current ZTA has no uniform standard for the data of trust algorithms, so it may lead to data inconsistency, which further affects the performance of trust evaluation. Since the input for trust evaluation is provided by different data sources such as CDM, there is no uniformity in the format, role and size of the data collected from these data sources, which makes it impossible for the trust algorithm to use the same method for evaluating the information sources. If different algorithms are used for evaluation, the efficiency of the model operation will be reduced. If the same algorithm is used for evaluation, the evaluation results will be affected directly.

5.2 Future development

5.2.1 Human expertise

AI-based ZTA systems offer the advantage of automatic authorization management, which can significantly reduce the burden of manual authentication processes. However, relying solely on AI-based decision-making may lead to incorrect or biased decisions, and then further result in false positives or false negatives. Therefore, incorporating human expertise in the loop can help reduce or eliminate the impact of errors caused by AI systems. By incorporating human feedback and review, the ZTA system can improve its accuracy and adapt to changing circumstances more efficiently. For example, if an AI-based ZTA system denies access to a legitimate user, a human expert can be referred to re-evaluate the decision and provide feedback to improve the system′s accuracy. Then, the AI-based system can learn from its mistakes and continuously improve its performance. Therefore, it is necessary to introduce human-in-the-loop machine learning[166] for ZTA in order to make more accurate and efficient decisions.

5.2.2 Data quality

Another critical factor to consider in AI-based ZTA systems is the availability and quality of training data. These systems rely on large datasets to train their models, and if the training data is compromised, the system′s performance can be severely affected. Data poisoning, a type of adversarial attack, can manipulate the training data to mislead the system′s decision-making, resulting in poor decisions based on misleading outputs[167]. To mitigate the impact of data poisoning, ZTA systems should implement robust data cleansing and validation techniques to ensure the quality and integrity of training data. Additionally, it could use multi-modal datasets from different sources and apply techniques such as data randomization to reduce the impact of potential data poisoning issues.

5.2.3 SASE

Secure access service edge (SASE) is a service based on an entity′s identity, real-time context, enterprise security/compliance policies, and continuous assessment of risk/trust throughout the session[168]. SASE converges network access and security capabilities and unifies in the cloud for management and delivery. Zero trust is a way of thinking that focuses on authentication and data access authorization on an as-needed basis, whereas SASE refers to a cloud delivery platform implemented at the edge that provides broad protection for data anywhere. SASE cannot be seen as a fast track to zero trust, but rather, SASE should be combined with ZTA to better protect cloud-based services as well as local services using zero trust principles.

5.2.4 Fast communication

The growing reliance on digital technology has increased the complexity and scale of cyber threats, making it challenging for organizations to protect their systems and data. However, implementing ZTA in untrusted infrastructures requires handling a massive amount of data generated between facilities, which needs to be transmitted to the appropriate components for security analysis and access policy updates.

Traditional wired communication technologies, such as Ethernet and fiber-optic cables, offer high data rates and reliability. However, they require physical connections between devices, which can be costly and challenging to maintain, especially in remote and challenging environments. Moreover, wired networks are vulnerable to physical attacks, such as cable cuts or sabotage, which can lead to network downtime and data breaches. Wireless communication technologies, such as WiFi and cellular networks, provide mobility and flexibility in untrusted infrastructures. However, they suffer from limited bandwidth, low data rates and high latency, making them inadequate for handling the massive amount of data generated in ZTA.

In contrast, next-generation networks such as 6G offer several advantages over traditional wired and wireless communication technologies. 6G networks provide massive connectivity, ultra-low latency and faster data rates, making them suitable for handling the massive amount of data generated in ZTA[169, 170]. It is worth mentioning that 6G networks have ability to support massive machine-type communications (mMTC) from IoT devices[171], sensors and other connected devices, which is a critical requirement in ZTA. On the other hand, ZTA can also dynamically detect anomaly activities of users/devices/applications in 6G networks and restrict internal and external access to IoT resources[170].

6 Conclusions

With its least privilege and the end-to-end principle, ZTA solves the security problems prevalent in perimeter-based security architectures such as lateral movement, insider attacks, etc. The implementation and development of ZTA is further promoted by the use of AI technologies. This survey provides an insightful analysis of the recent literature on ZTA, revealing gaps in addressing AI in ZTA component automation and orchestration. In addition, this survey has identified trust evaluation, authentication, attack detection, and monitoring as the fundamental classifications that constitute the operation of ZTA component automation. To address the challenges associated with these classifications, an overview of AI-based solutions is provided.

With the development of cloud computing, 5G/6G and other technologies, ZTA will be used in an increasingly wide range of fields. As we have observed in the literature, only a few zero-trust models employ AI-based automation techniques in their design. Therefore, this survey provides an overview of opportunities for future investigations to be explored by researchers. Mechanisms that leverage AI technologies to drive the automated operation of ZTA will lead developers to achieve ZTA automation and orchestration.

Acknowledgements

Open Access funding enabled and organized by CAUL and its Member Institutions.

Declarations of conflict of interest

The authors declared that they have no conflicts of interest to this work.

References

[1] M. Campbell. Beyond zero trust: Trust is a vulnerability. *Computer*, vol. 53, no. 10, pp. 110–113, 2020. DOI: 10.1109/MC.2020.3011081.

[2] S. Rose, O. Borchert, S. Mitchell, S. Connelly. Zero trust architecture. Gaithersburg, USA: *NIST Special Publication 800–207*, 2020. DOI: 10.6028/NIST.SP.800-207.

[3] A. A. Barakabitze, A. Ahmad, R. Mijumbi, A. Hines. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, vol. 167, Article number 106984, 2020. DOI: 10.1016/j.comnet.2019.106984.

[4] P. J. Sun. Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, vol. 160, Article number 102642, 2020. DOI: 10.1016/j.jnca.2020.102642.

[5] D. A. E. Haddon. 9 — Zero trust networks, the concepts, the strategies, and the reality. *Strategy, Leadership, and AI in the Cyber Ecosystem*, H. Jahankhani, L. M. O'Dell, G. Bowen, D. Hagan, A. Jamal, Eds., Amsterdam, The

Netherlands: Academic Press, pp. 195–216, 2021. DOI: 10.1016/B978-0-12-821442-8.00001-X.

[6] D. Nicholson. Blurring the boundaries between networking and it security. *Network Security*, vol. 2018, no. 1, pp. 11–13, 2018. DOI: 10.1016/S1353-4858(18)30007-2.

[7] A. Kerman, O. Borchert, S. Rose, A. Tan. Implementing a zero trust architecture. *National Institute of Standards and Technology (NIST) special publication 1800-35E*, 2020.

[8] Z. Zaheer, H. Chang, S. Mukherjee, J. Van Der Merwe. eZTrust: Network-independent zero-trust perimeterization for microservices. In *Proceedings of the ACM Symposium on SDN Research*, San Jose, USA, pp. 49–61, 2019. DOI: 10.1145/3314148.3314349.

[9] Z. A. Collier, J. Sarkis. The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*, vol. 59, no. 11, pp. 3430–3445, 2021. DOI: 10.1080/00207543.2021.1884311.

[10] A. Wylde. Zero trust: Never trust, always verify. In *Proceedings of International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, Dublin, Ireland, 2021. DOI: 10.1109/CyberSA52016.2021.9478244.

[11] C. Katsis, F. Cicala, D. Thomsen, N. Ringo, E. Bertino. Can I reach you? Do I need to? New semantics in security policy specification and testing. In *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*, pp. 165–174, 2021. DOI: 10.1145/3450569.3463558.

[12] X. S. Yan, H. J. Wang. Survey on zero-trust network security. In *Proceedings of the 6th International Conference on Artificial Intelligence and Security*, Hohhot, China, pp. 50–60, 2020. DOI: 10.1007/978-981-15-8083-3_5.

[13] J. Kinyua, L. Awuah. AI/ML in security orchestration, automation and response: Future research directions. *Intelligent Automation & Soft Computing*, vol. 285, no. 2, pp. 527–545, 2020. DOI: 10.32604/iasc.2021.016240.

[14] E. Bertino, K. Brancik. Services for zero trust architectures-a research roadmap. In *Proceedings of IEEE International Conference on Web Services*, Chicago, USA, pp. 14–20, 2021. DOI: 10.1109/ICWS53863.2021.00016.

[15] J. Kindervag. Build security into your network's DNA: The zero trust network architecture, Technical Report 27, Forrester Research Inc., USA, 2010.

[16] J. Kindervag, S. Balaouras. No more chewy centers: Introducing the zero trust model of information security. *Forrester Research*, vol. 3, 2010.

[17] C. Cunningham. The Zero Trust Extended (ZTX) Ecosystem, Combridge, UK: Forrester Research, Inc., 2018.

[18] R. Ward, B. Beyer. BeyondCorp: A new approach to enterprise security. *Usenix Login*, vol. 39, no. 6, pp. 6–11, 2014.

[19] B. Osborn, J. McWilliams, B. Beyer, M. Saltonstall. BeyondCorp: Design to deployment at Google. *Login*, vol. 41, no. 1, pp. 28–34, 2016.

[20] L. Cittadini, B. Spear, B. Beyer, M. Saltonstall. BeyondCorp: The access proxy. *Security*, vol. 41, no. 4, pp. 28–33, 2016.

[21] J. Peck, B. Beyer, C. Beske, M. Saltonstall. Migrating to BeyondCorp: Maintaining productivity while improving security. *Summer*, vol. 42, no. 2, pp. 49–55, 2017.

[22] V. M. Escobedo, F. Zyzniewski, B. A. E. Beyer, M. Saltonstall. BeyondCorp: The user experience. *Login*, vol. 42, no. 3, pp. 38–43, 2017.

[23] M. Janosko, H. King, B. A. E. Beyer, M. Saltonstall. Beyondcorp 6: Building a healthy fleet. *Login*, vol. 43, no. 3, pp. 26–64, 2018.

[24] S. Teerakanok, T. Uehara, A. Inomata. Migrating to zero trust architecture: Reviews and challenges. *Security and Communication Networks*, vol. 2021, Article number 9947347, 2021. DOI: 10.1155/2021/9947347.

[25] C. Buck, C. Olenberger, A. Schweizer, F. Völter, T. Eymann. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, vol. 110, Article number 102436, 2021. DOI: 10.1016/j.cose.2021.102436.

[26] L. Alevizos, V. T. Ta, M. H. Eiza. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. *Security and Privacy*, vol. 5, no. 1, Article number e191, 2022. DOI: 10.1002/spy2.191.

[27] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, R. Doss. Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access*, vol. 10, pp. 57143–57179, 2022. DOI: 10.1109/ACCESS.2022.3174679.

[28] Y. H. He, D. C. Huang, L. Chen, Y. Ni, X. J. Ma. A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, vol. 2022, Article number 6476274, 2022. DOI: 10.1155/2022/6476274.

[29] J. M. Pittman, S. Alaee, C. Crosby, T. Honey, G. M. Schaefer. Towards a model for zero trust data. *American Journal of Science & Engineering*, vol. 3, no. 1, pp. 18–24, 2022. DOI: 10.15864/ajse.3103.

[30] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, H. Kim. Security of zero trust networks in cloud computing: A comparative review. *Sustainability*, vol. 14, no. 18, Article number 11213, 2022. DOI: 10.3390/su141811213.

[31] E. Gilman, D. Barth. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*, O'Reilly Media, Inc., 2017.

[32] J. Garbis, J. W. Chapman. *Zero Trust Security: An Enterprise Guide*, Berkeley, USA: Apress, 2021.

[33] S. Dhar, I. Bose. Securing IoT devices using zero trust and blockchain. *Journal of Organizational Computing and Electronic Commerce*, vol. 31, no. 1, pp. 18–34, 2021. DOI: 10.1080/10919392.2020.1831870.

[34] L. F. Huang. The firewall technology study of network perimeter security. In *Proceedings of IEEE Asia-Pacific Services Computing Conference*, Guilin, China, pp. 410–413, 2012. DOI: 10.1109/APSCC.2012.23.

[35] S. Splaine. *Testing Web Security: Assessing the Security of Web Sites and Applications*, Indianapolis, USA: Wiley, 2002.

[36] K. Dadheech, A. Choudhary, G. Bhatia. De-militarized zone: A next level to network security. In *Proceedings of Second International Conference on Inventive Communication and Computational Technologies*, Coimbatore, India, pp. 595–600, 2018. DOI: 10.1109/ICICCT.2018.8473328.

[37] E. S. Hosney, I. T. A. Halim, A. H. Yousef. An artificial intelligence approach for deploying zero trust architecture (ZTA). In *Proceedings of 5th International Conference on Computing and Informatics*, New Cairo, Egypt, pp. 343–350, 2022. DOI: 10.1109/ICCI54321.2022.9756117.

[38] M. Saleem, M. R. Warsi, S. Islam. Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. *Journal of Information Security and Applications*, vol. 72, Article number 103389, 2023. DOI: 10.1016/j.jisa.2022.103389.

[39] J. W. Wang, X. Y. Jing, Z. Yan, Y. L. Fu, W. Pedrycz, L. T. Yang. A survey on trust evaluation based on machine learning. *ACM Computing Surveys*, vol. 53, no. 5, Article number 107, 2020. DOI: 10.1145/3408292.

[40] H. Lin, S. Garg, J. Hu, X. D. Wang, J. Piran, M. S. Hossain. Data fusion and transfer learning empowered granular trust evaluation for internet of things. *Information Fusion*, vol. 78, pp. 149–157, 2022. DOI: 10.1016/j.inffus.2021.09.001.

[41] N. C. Luong, D. T. Hoang, S. M. Gong, D. Niyato, P. Wang, Y. C. Liang, D. I. Kim. Applications of deep reinforcement learning in communications and networking: A survey. *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3133–3174, 2019. DOI: 10.1109/COMST.2019.2916583.

[42] R. S. Sandhu, P. Samarati. Access control: Principle and practice. *IEEE Communications Magazine*, vol. 32, no. 9, pp. 40–48, 1994. DOI: 10.1109/35.312842.

[43] S. Ravidas, A. Lekidis, F. Paci, N. Zannone. Access control in internet-of-things: A survey. *Journal of Network and Computer Applications*, vol. 144, pp. 79–101, 2019. DOI: 10.1016/j.jnca.2019.06.017.

[44] A. Ouaddah, H. Mousannif, A. A. Elkalam, A. A. Ouahman. Access control in the internet of things: Big challenges and new opportunities. *Computer Networks*, vol. 112, pp. 237–262, 2017. DOI: 10.1016/j.comnet.2016.11.007.

[45] Y. H. Zhang, R. H. Deng, S. M. Xu, J. F. Sun, Q. Li, D. Zheng. Attribute-based encryption for cloud computing access control: A survey. *ACM Computing Surveys*, vol. 53, no. 4, Article number 83, 2020. DOI: 10.1145/3398036.

[46] L. Zhou, C. H. Su, Z. Li, Z. Liu, G. P. Hancke. Automatic fine-grained access control in SCADA by machine learning. *Future Generation Computer Systems*, vol. 93, pp. 548–559, 2019. DOI: 10.1016/j.future.2018.04.043.

[47] K. Bibi, S. Naz, A. Rehman. Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. *Multimedia Tools and Applications*, vol. 79, no. 1–2, pp. 289–340, 2020. DOI: 10.1007/s11042-019-08022-0.

[48] R. Ryu, S. Yeom, S. H. Kim, D. Herbert. Continuous multimodal biometric authentication schemes: A systematic review. *IEEE Access*, vol. 9, pp. 34541–34557, 2021. DOI: 10.1109/ACCESS.2021.3061589.

[49] K. S. Germain, F. Kragh. Mobile physical-layer authentication using channel state information and conditional recurrent neural networks. In *Proceedings of the 93rd IEEE Vehicular Technology Conference*, Helsinki, Finland, pp. 1–6, 2021. DOI: 10.1109/VTC2021-Spring51267.2021.9448652.

[50] N. Xie, Z. Y. Li, H. J. Tan. A survey of physical-layer authentication in wireless communications. *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2021. DOI: 10.1109/COMST.2020.3042188.

[51] M. Conti, T. Dargahi, A. Dehghantanha. Cyber threat intelligence: Challenges and opportunities. *Cyber Threat Intelligence*, A. Dehghantanha, M. Conti, T. Dargahi, Eds., Cham, Switzerland: Springer, pp. 1–6, 2018. DOI: 10.1007/978-3-319-73951-9_1.

[52] X. J. Liao, K. Yuan, X. F. Wang, Z. Li, L. Y. Xing, R. Beyah. Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence. In *Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, pp. 755–766, 2016. DOI: 10.1145/2976749.2978315.

[53] A. Tundis, S. Ruppert, M. Mühlhäuser. On the automated assessment of open-source cyber threat intelligence sources. In *Proceedings of the 20th International Conference on Computational Science*, Amsterdam, The Netherlands, pp. 453–467, 2020. DOI: 10.1007/978-3-030-50417-5_34.

[54] P. Gao, X. Y. Liu, E. Choi, B. Soman, C. Mishra, K. Farris, D. Song. A system for automated open-source threat intelligence gathering and management. In *Proceedings of International Conference on Management of Data*, pp. 2716–2720, 2021. DOI: 10.1145/3448016.3452745.

[55] G. Cascavilla, D. A. Tamburri, W. J. Van Den Heuvel. Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, vol. 105, Article number 102258, 2021. DOI: 10.1016/j.cose.2021.102258.

[56] T. D. Wagner, K. Mahbub, E. Palomar, A. E. Abdallah. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, vol. 87, Article number 101589, 2019. DOI: 10.1016/j.cose.2019.101589.

[57] S. K. Anand, S. Kumar. Experimental comparisons of clustering approaches for data representation. *ACM Computing Surveys*, vol. 55, no. 3, Article number 45, 2022. DOI: 10.1145/3490384.

[58] M. Khader, G. Al-Naymat. Density-based algorithms for big data clustering using MapReduce framework: A comprehensive study. *ACM Computing Surveys*, vol. 53, no. 5, Article number 93, 2020. DOI: 10.1145/3403951.

[59] F. L. Gewers, G. R. Ferreira, H. F. De Arruda, F. N. Silva, C. H. Comin, D. R. Amancio, L. D. F. Costa. Principal component analysis: A natural approach to data exploration. *ACM Computing Surveys*, vol. 54, no. 4, Article number 70, 2021. DOI: 10.1145/3447755.

[60] X. R. Wang, J. Yang, Q. Y. Wang, C. X. Su. Threat intelligence relationship extraction based on distant supervision and reinforcement learning. In *Proceedings of the 32nd International Conference on Software Engineering and Knowledge Engineering*, pp. 572–576, 2020.

[61] M. Sewak, S. K. Sahay, H. Rathore. Deep reinforcement learning for cybersecurity threat detection and protection: A review. In *Proceedings of the 9th International Conference on Secure Knowledge Management In Artificial Intelligence Era*, San Antonio, USA, pp. 51–72, 2021. DOI: 10.1007/978-3-030-97532-6_4.

[62] J. Soldani, A. Brogi. Anomaly detection and failure root cause analysis in (micro) service-based cloud applications: A survey. *ACM Computing Surveys*, vol. 55, no. 3,

Article number 59, 2022. DOI: 10.1145/3501297.

[63] M. Landauer, F. Skopik, M. Wurzenberger, A. Rauber. System log clustering approaches for cyber security applications: A survey. *Computers & Security*, vol. 92, Article number 101739, 2020. DOI: 10.1016/j.cose.2020.101739.

[64] R. Chalapathy, S. Chawla. Deep learning for anomaly detection: A survey, [Online], Available: https://arxiv.org/abs/1901.03407, 2019.

[65] G. E. I. Selim, E. E. D. Hemdan, A. M. Shehata, N. A. El-Fishawy. Anomaly events classification and detection system in critical industrial internet of things infrastructure using machine learning algorithms. *Multimedia Tools and Applications*, vol. 80, no. 8, pp. 12619–12640, 2021. DOI: 10.1007/s11042-020-10354-1.

[66] J. Kindervag. No More Chewy Centers: The Zero Trust Model of Information Security, Combridge, UK: Forrester Research Inc., 2016.

[67] K. Zhao, L. Pan. A machine learning based trust evaluation framework for online social networks. In *Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Beijing, China, pp. 69–74, 2014. DOI: 10.1109/TrustCom.2014.13.

[68] X. Chen, Y. Y. Yuan, L. L. Lu, J. C. Yang. A multidimensional trust evaluation framework for online social networks based on machine learning. *IEEE Access*, vol. 7, pp. 175499–175513, 2019. DOI: 10.1109/ACCESS.2019.2957779.

[69] X. Chen, Y. Y. Yuan, M. A. Orgun. Using Bayesian networks with hidden variables for identifying trustworthy users in social networks. *Journal of Information Science*, vol. 46, no. 5, pp. 600–615, 2020. DOI: 10.1177/0165551519857590.

[70] Y. J. Wang. The trust value calculating for social network based on machine learning. In *Proceedings of the 9th International Conference on Intelligent Human-Machine Systems and Cybernetics*, Hangzhou, China, pp. 133–136, 2017. DOI: 10.1109/IHMSC.2017.145.

[71] H. El-Sayed, H. A. Ignatious, P. Kulkarni, S. Bouktif. Machine learning based trust management framework for vehicular networks. *Vehicular Communications*, vol. 25, Article number 100256, 2020. DOI: 10.1016/j.vehcom.2020.100256.

[72] W. Ma, X. Wang, M. S. Hu, Q. L. Zhou. Machine learning empowered trust evaluation method for IoT devices. *IEEE Access*, vol. 9, pp. 65066–65077, 2021. DOI: 10.1109/ACCESS.2021.3076118.

[73] M. P. Lokhande, D. D. Patil. Trust computation model for IoT devices using machine learning techniques. In *Proceeding of the 1st Doctoral Symposium on Natural Computing Research*, pp. 195–205, 2021. DOI: 10.1007/978-981-33-4073-2_20.

[74] W. Y. Zhang, B. Wu, Y. Liu. Cluster-level trust prediction based on multi-modal social networks. *Neurocomputing*, vol. 210, pp. 206–216, 2016. DOI: 10.1016/j.neucom.2016.01.108.

[75] M. Mishra, G. S. Gupta, X. Gui. Trust-based cluster head selection using the k-means algorithm for wireless sensor networks. In *Proceedings of International Conference on Smart Systems and Inventive Technology*, Tirunelveli, India, pp. 819–825, 2019. DOI: 10.1109/ICSSIT46314.2019.8987888.

[76] L. Yang, Y. Z. Lu, S. X. Yang, Y. C. Zhong, T. Guo, Z. F. Liang. An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks. *IEEE Sensors Journal*, vol. 21, no. 12, pp. 13935–13947, 2021. DOI: 10.1109/JSEN.2021.3070689.

[77] U. Jayasinghe, G. M. Lee, T. W. Um, Q. Shi. Machine learning based trust computational model for IoT services. *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 39–52, 2019. DOI: 10.1109/TSUSC.2018.2839623.

[78] G. J. Han, Y. He, J. F. Jiang, N. Wang, M. Guizani, J. A. Ansere. A synergetic trust model based on SVM in underwater acoustic sensor networks. *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11239–11247, 2019. DOI: 10.1109/TVT.2019.2939179.

[79] S. Sagar, A. Mahmood, Q. Z. Sheng, W. E. Zhang. Trust computational heuristic for social internet of things: A machine learning-based approach. In *Proceedings of IEEE International Conference on Communications*, Dublin, Ireland, 2020. DOI: 10.1109/ICC40277.2020.9148767.

[80] H. Mayadunna, L. Rupasinghe. A trust evaluation model for online social networks. In *Proceedings of National Information Technology Conference*, Colombo, Sri Lanka, 2018. DOI: 10.1109/NITC.2018.8550080.

[81] J. J. Guo, X. H. Li, Z. Q. Liu, J. F. Ma, C. Yang, J. W. Zhang, D. P. Wu. TROVE: A context-awareness trust model for VANETs using reinforcement learning. *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6647–6662, 2020. DOI: 10.1109/JIOT.2020.2975084.

[82] Y. He, G. J. Han, J. F. Jiang, H. Wang, M. Martínez-García. A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks. *IEEE Transactions on Mobile Computing*, vol. 21, no. 3, pp. 811–821, 2022. DOI: 10.1109/TMC.2020.3020313.

[83] Y. Y. Ren, W. Liu, A. F. Liu, T. Wang, A. Li. A privacy-protected intelligent crowdsourcing application of iot based on the reinforcement learning. *Future Generation Computer Systems*, vol. 127, pp. 56–69, 2022. DOI: 10.1016/j.future.2021.09.003.

[84] X. D. Zhuang, X. R. Tong. A local trust inferring algorithm based on reinforcement learning DoubleDQN in online social networks. In *Proceedings of the 13th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics*, Chengdu, China, pp. 1064–1069, 2020. DOI: 10.1109/CISP-BMEI51763.2020.9263509.

[85] S. A. Siddiqui, A. Mahmood, W. E. Zhang, Q. Z. Sheng. Machine learning based trust model for misbehaviour detection in internet-of-vehicles. In *Proceedings of the 26th International Conference on Neural Information Processing*, Sydney, Australia, pp. 512–520, 2019. DOI: 10.1007/978-3-030-36808-1_56.

[86] M. Ghavipour, M. R. Meybodi. Trust propagation algorithm based on learning automata for inferring local trust in online social networks. *Knowledge-Based Systems*, vol. 143, pp. 307–316, 2018. DOI: 10.1016/j.knosys.2017.06.034.

[87] M. Hammad, S. Z. Zhang, K. Q. Wang. A novel two-dimensional ECG feature extraction and classification al-

gorithm based on convolution neural network for human authentication. *Future Generation Computer Systems*, vol. 101, pp. 180–196, 2019. DOI: 10.1016/j.future.2019.06.008.

[88] S. Aziz, M. U. Khan, Z. A. Choudhry, A. Aymin, A. Usman. ECG-based biometric authentication using empirical mode decomposition and support vector machines. In *Proceedings of IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference*, Vancouver, Canada, pp. 906–912, 2019. DOI: 10.1109/IEMCON.2019.8936174.

[89] Y. T. Li, H. L. Hu, Z. Q. Zhu, G. Zhou. SCANet: Sensor-based continuous authentication with two-stream convolutional neural networks. *ACM Transactions on Sensor Networks*, vol. 16, no. 3, Article number 29, 2020. DOI: 10.1145/3397179.

[90] H. Kong, L. Lu, J. D. Yu, Y. Y. Chen, F. L. Tang. Continuous authentication through finger gesture interaction for smart homes using WiFi. *IEEE Transactions on Mobile Computing*, vol. 20, no. 11, pp. 3148–3162, 2021. DOI: 10.1109/TMC.2020.2994955.

[91] M. P. Centeno, A. Van Moorsel, S. Castruccio. Smartphone continuous authentication using deep learning autoencoders. In *Proceedings of the 15th Annual Conference on Privacy, Security and Trust*, Calgary, Canada, pp. 147–1478, 2017. DOI: 10.1109/PST.2017.00026.

[92] K. Bicakci, O. Salman, Y. Uzunay, M. Tan. Analysis and evaluation of keystroke dynamics as a feature of contextual authentication. In *Proceedings of International Conference on Information Security and Cryptology*, Ankara, Turkey, pp. 11–17, 2020. DOI: 10.1109/ISCTURKEY51113.2020.9307967.

[93] M. Smith-Creasey, F. A. Albalooshi, M. Rajarajan. Context awareness for improved continuous face authentication on mobile devices. In *Proceedings of the 16th IEEE International Conference on Dependable, Autonomic and Secure Computing, the 16th International Conference on Pervasive Intelligence and Computing, the 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress*, Athens, Greece, pp. 644–652, 2018. DOI: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00115.

[94] M. Abuhamad, T. Abuhmed, D. Mohaisen, D. H. Nyang. AUTo*sen*: Deep-learning-based implicit continuous authentication using smartphone sensors. *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5008–5020, 2020. DOI: 10.1109/JIOT.2020.2975779.

[95] S. Vhaduri, C. Poellabauer. Multi-modal biometric-based implicit authentication of wearable device users. *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3116–3125, 2019. DOI: 10.1109/TIFS.2019.2911170.

[96] X. Zhang, L. N. Yao, C. R. Huang, T. Gu, Z. Yang, Y. H. Liu. DeepKey: A multimodal biometric authentication system via deep decoding gaits and brainwaves. *ACM Transactions on Intelligent Systems and Technology*, vol. 11, no. 4, Article number 49, 2020. DOI: 10.1145/3393619.

[97] M. Hammad, Y. S. Liu, K. Q. Wang. Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. *IEEE Access*, vol. 7, pp. 26527–26542, 2018. DOI: 10.1109/ACCESS.2018.2886573.

[98] S. H. Choudhury, A. Kumar, S. H. Laskar. Biometric authentication through unification of finger dorsal biometric traits. *Information Sciences*, vol. 497, pp. 202–218, 2019. DOI: 10.1016/j.ins.2019.05.045.

[99] D. Sivasankaran, M. Ragab, T. Sim, Y. Zick. Context-aware fusion for continuous biometric authentication. In *Proceedings of International Conference on Biometrics*, Gold Coast, Australia, pp. 233–240, 2018. DOI: 10.1109/ICB2018.2018.00043.

[100] Y. Lin, X. L. Zhu, Z. G. Zheng, Z. Dou, R. L. Zhou. The individual identification method of wireless device based on dimensionality reduction and machine learning. *The Journal of Supercomputing*, vol. 75, no. 6, pp. 3010–3027, 2019. DOI: 10.1007/s11227-017-2216-2.

[101] G. X. Shen, J. Q. Zhang, A. Marshall, L. N. Peng, X. B. Wang. Radio frequency fingerprint identification for LoRa using spectrogram and CNN. In *Proceedings of IEEE INFOCOM Conference on Computer Communications*, Vancouver, Canada, 2021. DOI: 10.1109/INFOCOM42981.2021.9488793.

[102] G. W. Qing, H. F. Wang, T. P. Zhang. Radio frequency fingerprinting identification for zigbee via lightweight CNN. *Physical Communication*, vol. 44, Article number 101250, 2021. DOI: 10.1016/j.phycom.2020.101250.

[103] Q. Wang, H. Li, D. Zhao, Z. Chen, S. Ye, J. S. Cai. Deep neural networks for CSI-based authentication. *IEEE Access*, vol. 7, pp. 123026–123034, 2019. DOI: 10.1109/ACCESS.2019.2938533.

[104] J. Yoon, Y. Lee, E. Hwang. Machine learning-based physical layer authentication using neighborhood component analysis in MIMO wireless communications. In *Proceedings of International Conference on Information and Communication Technology Convergence*, Jeju Island, Republic of Korea, pp. 63–65, 2019. DOI: 10.1109/ICTC46691.2019.8939862.

[105] K. S. Germain, F. Kragh. Physical-layer authentication using channel state information and machine learning. In *Proceedings of the 14th International Conference on Signal Processing and Communication Systems*, Adelaide, Australia, 2020. DOI: 10.1109/ICSPCS50536.2020.9310070.

[106] M. K. Oh, S. Lee, Y. Kang. Wi-SUN device authentication using physical layer fingerprint. In *Proceedings of International Conference on Information and Communication Technology Convergence*, Jeju Island, Republic of Korea, pp. 160–162, 2021. DOI: 10.1109/ICTC52510.2021.9620899.

[107] I. Deliu, C. Leichter, K. Franke. Collecting cyber threat intelligence from hacker forums via a two-stage, hybrid process using support vector machines and latent dirichlet allocation. In *Proceedings of IEEE International Conference on Big Data*, Seattle, USA, pp. 5008–5013, 2018. DOI: 10.1109/BigData.2018.8622469.

[108] M. Kadoguchi, S. Hayashi, M. Hashimoto, A. Otsuka. Exploring the dark web for cyber threat intelligence using machine leaning. In *Proceedings of IEEE International Conference on Intelligence and Security Informatics*, Shenzhen, China, pp. 200–202, 2019. DOI: 10.1109/ISI.2019.8823360.

[109] P. Koloveas, T. Chantzios, S. Alevizopoulou, S. Skiadopoulos, C. Tryfonopoulos. INTIME: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. *Electronics*, vol. 10, no. 7,

Article number 818, 2021. DOI: 10.3390/electronics10070818.

[110] L. M. Kristiansen, V. Agarwal, K. Franke, R. S. Shah. CTI-twitter: Gathering cyber threat intelligence from twitter using integrated supervised and unsupervised learning. In *Proceedings of IEEE International Conference on Big Data*, Atlanta, USA, pp. 2299–2308, 2020. DOI: 10.1109/BigData50022.2020.9378393.

[111] M. M. Li, R. F. Zheng, L. Liu, P. Yang. Extraction of threat actions from threat-related articles using multi-label machine learning classification method. In *Proceedings of the 2nd International Conference on Safety Produce Informatization*, Chongqing, China, pp. 428–431, 2019. DOI: 10.1109/IICSPI48186.2019.9095885.

[112] S. Xun, X. Y. Li, Y. L. Gao. AITI: An automatic identification model of threat intelligence based on convolutional neural network. In *Proceedings of the 4th International Conference on Innovation in Artificial Intelligence*, Xiamen China, pp. 20–24, 2020. DOI: 10.1145/3390557.3394305.

[113] B. Ampel, S. Samtani, H. Y. Zhu, S. Ullman, H. Chen. Labeling hacker exploits for proactive cyber threat intelligence: A deep transfer learning approach. In *Proceedings of IEEE International Conference on Intelligence and Security Informatics*, Arlington, USA, pp. 1–6, 2020. DOI: 10.1109/ISI49825.2020.9280548.

[114] X. R. Wang, R. Chen, B. H. Song, J. Yang, Z. W. Jiang, X. Q. Zhang, X. M. Li, S. Q. Ao. A method for extracting unstructured threat intelligence based on dictionary template and reinforcement learning. In *Proceedings of the 24th IEEE International Conference on Computer Supported Cooperative Work in Design*, Dalian, China, pp. 262–267, 2021. DOI: 10.1109/CSCWD49262.2021.9437858.

[115] M. Du, F. F. Li, G. N. Zheng, V. Srikumar. DeepLog: Anomaly detection and diagnosis from system logs through deep learning. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, Dallas, USA, pp. 1285–1298, 2017. DOI: 10.1145/3133956.3134015.

[116] Y. M. Wang, Z. X. Ji. Design and implementation of a semi-supervised anomaly log detection model DDA. In *Proceedings of International Conference on Computer Communication and Artificial Intelligence*, Guangzhou, China, pp. 86–90, 2021. DOI: 10.1109/CCAI50917.2021.9447533.

[117] S. Y. Lu, X. Wei, Y. D. Li, L. Q. Wang. Detecting anomaly in big data system logs using convolutional neural network. In *Proceedings of the 16th IEEE International Conference on Dependable, Autonomic and Secure Computing, the 16th International Conference on Pervasive Intelligence and Computing, the 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress*, Athens, Greece, pp. 151–158, 2018. DOI: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00037.

[118] A. Wadekar, T. Gupta, R. Vijan, F. Kazi. Hybrid CAE-VAE for unsupervised anomaly detection in log file systems. In *Proceedings of the 10th International Conference on Computing, Communication and Networking Technologies*, Kanpur, India, pp. 1–7, 2019. DOI: 10.1109/ICCCNT45670.2019.8944863.

[119] Y. L. Yuan, S. S. Adhatarao, M. K. Lin, Y. C. Yuan, Z. L. Liu, X. M. Fu. ADA: Adaptive deep log anomaly detector. In *Proceedings of IEEE INFOCOM Conference on Computer Communications*, Toronto, Canada, pp. 2449–2458, 2020. DOI: 10.1109/INFOCOM41043.2020.9155487.

[120] S. Bursic, V. Cuculo, A. D'Amelio. Anomaly detection from log files using unsupervised deep learning. In *Proceedings of International Symposium on Formal Methods*, Porto, Portugal, pp. 200–207, 2019. DOI: 10.1007/978-3-030-54994-7_15.

[121] L. Yang, J. J. Chen, Z. Wang, W. J. Wang, J. J. Jiang, X. Y. Dong, W. B. Zhang. Semi-supervised log-based anomaly detection via probabilistic label estimation. In *Proceedings of the 43rd IEEE/ACM International Conference on Software Engineering*, Madrid, Spain, pp. 1448–1460, 2021. DOI: 10.1109/ICSE43902.2021.00130.

[122] S. Yen, M. Moh, T. S. Moh. CausalConvLSTM: Semi-supervised log anomaly detection through sequence modeling. In *Proceedings of the 18th IEEE International Conference On Machine Learning And Applications*, Boca Raton, USA, pp. 1334–1341, 2019. DOI: 10.1109/ICMLA.2019.00217.

[123] R. Chen, S. L. Zhang, D. W. Li, Y. Z. Zhang, F. R. Guo, W. B. Meng, D. Pei, Y. Z. Zhang, X. Chen, Y. Q. Liu. LogTransfer: Cross-system log anomaly detection for software systems with transfer learning. In *Proceedings of the 31st IEEE International Symposium on Software Reliability Engineering*, Coimbra, Portugal, pp. 37–47, 2020. DOI: 10.1109/ISSRE5003.2020.00013.

[124] J. J. Chen, S. Y. Guo, W. C. Li, J. Shen, X. S. Qiu, S. J. Shao. Network abnormal behavior detection method based on affinity propagation. In *Proceedings of the 6th International Conference on Artificial Intelligence and Security*, Hohhot, China, pp. 582–591, 2020. DOI: 10.1007/978-981-15-8086-4_55.

[125] H. H. Peng, W. Wang. Detecting masqueraders by profiling user behaviors. In *Proceedings of the 8th International Conference on Instrumentation & Measurement, Computer, Communication and Control*, Harbin, China, pp. 454–458, 2018. DOI: 10.1109/IMCCC.2018.00101.

[126] Y. Gao, Y. Ma, D. D. Li. Anomaly detection of malicious users' behaviors for web applications based on web logs. In *Proceedings of the 17th IEEE International Conference on Communication Technology*, Chengdu, China, pp. 1352–1355, 2017. DOI: 10.1109/ICCT.2017.8359854.

[127] M. Singh, B. M. Mehtre, S. Sangeetha. User behavior profiling using ensemble approach for insider threat detection. In *Proceedings of the 5th IEEE International Conference on Identity, Security, and Behavior Analysis*, Hyderabad, India, pp. 1–8, 2019. DOI: 10.1109/ISBA.2019.8778466.

[128] M. Singh, B. M. Mehtre, S. Sangeetha. User behaviour based insider threat detection in critical infrastructures. In *Proceedings of the 2nd International Conference on Secure Cyber Computing and Communications*, Jalandhar, India, pp. 489–494, 2021. DOI: 10.1109/ICSCCC51823.2021.9478137.

[129] B. Sharma, P. Pokharel, B. Joshi. User behavior analytics for anomaly detection using LSTM autoencoder-insider threat detection. In *Proceedings of the 11th International Conference on Advances in Information Technology*, Bangkok, Thailand, Article number 5, 2020. DOI: 10.1145/3406601.3406610.

[130] T. M. Li, L. M. Yan. SIEM based on big data analysis. In *Proceedings of the 3rd International Conference on Cloud Computing and Security*, Nanjing, China, pp. 167–175, 2017. DOI: 10.1007/978-3-319-68505-2_15.

[131] J. Lee, J. Kim, I. Kim, K. Han. Cyber threat detection based on artificial neural networks using event profiles. *IEEE Access*, vol. 7, pp. 165607–165626, 2019. DOI: 10.1109/ACCESS.2019.2953095.

[132] S. El Hajji, N. Moukafih, G. Orhanou. Analysis of neural network training and cost functions impact on the accuracy of IDS and SIEM systems. In *Proceedings of the 3rd International Conference on Codes, Cryptology, and Information Security*, Rabat, Morocco, pp. 433–451, 2019. DOI: 10.1007/978-3-030-16458-4_25.

[133] S. M. M. Hossain, R. Couturier, J. Rusk, K. B. Kent. Automatic event categorizer for SIEM. In *Proceedings of the 31st Annual International Conference on Computer Science and Software Engineering*, Toronto, Canada, pp. 104–112, 2021.

[134] H. Hindy, D. Brosset, E. Bayne, A. Seeam, X. Bellekens. Improving SIEM for critical SCADA water infrastructures using machine learning. In *Proceedings of International Workshop on Security and Privacy Requirements Engineering*, Barcelona, Spain, pp. 3–19, 2019. DOI: 10.1007/978-3-030-12786-2_1.

[135] C. Feng, S. N. Wu, N. W. Liu. A user-centric machine learning framework for cyber security operations center. In *Proceedings of IEEE International Conference on Intelligence and Security Informatics*, Beijing, China, pp. 173–175, 2017. DOI: 10.1109/ISI.2017.8004902.

[136] G. H. Wang, Y. Wu. BIBRM: A Bayesian inference based road message trust model in vehicular ad hoc networks. In *Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Beijing, China, pp. 481–486, 2014. DOI: 10.1109/TrustCom.2014.137.

[137] Z. Yan. *Trust Management in Mobile Environments: Autonomic and Usable Models*, Hershey, USA: IGI Global, 2013.

[138] Y. Zhang, B. Song, P. Zhang. Social behavior study under pervasive social networking based on decentralized deep reinforcement learning. *Journal of Network and Computer Applications*, vol. 86, pp. 72–81, 2017. DOI: 10.1016/j.jnca.2016.11.015.

[139] D. J. He, C. Chen, S. Chan, J. J. Bu, A. V. Vasilakos. A distributed trust evaluation model and its application scenarios for medical sensor networks. *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1164–1175, 2012. DOI: 10.1109/TITB.2012.2199996.

[140] J. F. Jiang, G. J. Han, F. Wang, L. Shu, M. Guizani. An efficient distributed trust model for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015. DOI: 10.1109/TPDS.2014.2320505.

[141] Y. Dou, H. C. B. Chan, M. H. Au. A distributed trust evaluation protocol with privacy protection for intercloud. *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 6, pp. 1208–1221, 2019. DOI: 10.1109/TPDS.2018.2883080.

[142] M. Ashtiani, M. A. Azgomi. A novel trust evolution algorithm based on a quantum-like model of computational trust. *Cognition, Technology & Work*, vol. 21, no. 2, pp. 201–224, 2019. DOI: 10.1007/s10111-018-0496-9.

[143] M. Ashtiani, M. A. Azgomi. A formulation of computational trust based on quantum decision theory. *Information Systems Frontiers*, vol. 18, no. 4, pp. 735–764, 2016. DOI: 10.1007/s10796-015-9555-4.

[144] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, S. Lloyd. Quantum machine learning. *Nature*, vol. 549, no. 7671, pp. 195–202, 2017. DOI: 10.1038/nature23474.

[145] M. Schuld, I. Sinayskiy, F. Petruccione. An introduction to quantum machine learning. *Contemporary Physics*, vol. 56, no. 2, pp. 172–185, 2015. DOI: 10.1080/00107514.2014.964942.

[146] P. Mitra. *Recent Advances in Cryptography and Network Security*, Intechopen, 2018. DOI: 1015772/intechopen.71917.

[147] E. Al Alkeem, S. K. Kim, C. Y. Yeun, M. J. Zemerly, K. F. Poon, G. Gianini, P. D. Yoo. An enhanced electrocardiogram biometric authentication system using machine learning. *IEEE Access*, vol. 7, pp. 123069–123075, 2019. DOI: 10.1109/ACCESS.2019.2937357.

[148] F. H. Al-Naji, R. Zagrouba. A survey on continuous authentication methods in internet of things environment. *Computer Communications*, vol. 163, pp. 109–133, 2020. DOI: 10.1016/j.comcom.2020.09.006.

[149] N. Bala, R. Gupta, A. Kumar. Multimodal biometric system based on fusion techniques: A review. *Information Security Journal: A Global Perspective*, vol. 31, no. 3, pp. 289–337, 2022. DOI: 10.1080/19393555.2021.1974130.

[150] S. K. Choudhary, A. K. Naik. Multimodal biometric authentication with secured templates-a review. In *Proceedings of the 3rd International Conference on Trends in Electronics and Informatics*, Tirunelveli, India, pp. 1062–1069, 2019. DOI: 10.1109/ICOEI.2019.8862563.

[151] D. Dasgupta, A. Roy, A. Nag. Multi-factor authentication. In *Advances in User Authentication*, D. Dasgupta, A. Roy, A. Nag, Eds., Cham, The Netherlands: Springer, pp. 185–233, 2017. DOI: 10.1007/978-3-319-58808-7_5.

[152] S. W. Shah, N. F. Syed, A. Shaghaghi, A. Anwar, Z. Baig, R. Doss. LCDA: Lightweight continuous device-to-device authentication for a zero trust architecture (ZTA). *Computers & Security*, vol. 108, Article number 102351, 2021. DOI: 10.1016/j.cose.2021.102351.

[153] A. Candore, O. Kocabas, F. Koushanfar. Robust stable radiometric fingerprinting for wireless devices. In *Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust*, San Francisco, USA, pp. 43–49, 2009. DOI: 10.1109/HST.2009.5224969.

[154] J. Q. Zhang, R. Woods, M. Sandell, M. Valkama, A. Marshall, J. Cavallaro. Radio frequency fingerprint identification for narrowband systems, modelling and classification. *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3974–3987, 2021. DOI: 10.1109/TIFS.2021.3088008.

[155] Z. J. Wang, W. W. Dou, M. J. Ma, X. X. Feng, Z. H. Huang, C. M. Zhang, Y. J. Guo, D. Chen. A survey of user authentication based on channel state information. *Wireless Communications and Mobile Computing*, vol. 2021, Article number 6636665, 2021. DOI: 10.1155/2021/6636665.

[156] K. Riad, T. Huang, L. S. Ke. A dynamic and hierarchical access control for IoT in multi-authority cloud storage. *Journal of Network and Computer Applications*, vol. 160, Article number 102633, 2020. DOI: 10.1016/j.jnca.2020.102633.

[157] C. Esposito. Interoperable, dynamic and privacy-preserving access control for cloud data storage when integrating heterogeneous organizations. *Journal of Network and Computer Applications*, vol. 108, pp. 124–136, 2018. DOI: 10.1016/j.jnca.2018.01.017.

[158] J. Li, X. F. Chen, S. S. M. Chow, Q. Huang, D. S. Wong, Z. L. Liu. Multi-authority fine-grained access control with accountability and its application in cloud. *Journal of Network and Computer Applications*, vol. 112, pp. 89–96, 2018. DOI: 10.1016/j.jnca.2018.03.006.

[159] A. Sentuna, A. Alsadoon, P. W. C. Prasad, M. Saadeh, O. H. Alsadoon. A novel enhanced naive Bayes posterior probability (ENBPP) using machine learning: Cyber threat analysis. *Neural Processing Letters*, vol. 53, no. 1, pp. 177–209, 2021. DOI: 10.1007/s11063-020-10381-x.

[160] S. L. Zhang, Z. Y. Zhong, D. W. Li, Q. L. Fan, Y. Q. Sun, M. Zhu, Y. Z. Zhang, D. Pei, J. Y. Sun, Y. L. Liu, H. Yang, Y. Q. Zou. Efficient KPI anomaly detection through transfer learning for large-scale web services. *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 8, pp. 2440–2455, 2022. DOI: 10.1109/JSAC.2022.3180785.

[161] S. Hu, Z. H. Xiao, Q. Rao, R. T. Liao. An anomaly detection model of user behavior based on similarity clustering. In *Proceedings of the 4th IEEE Information Technology and Mechatronics Engineering Conference*, Chongqing, China, pp. 835–838, 2018. DOI: 10.1109/ITOEC.2018.8740748.

[162] X. H. Sun, G. H. Yang, J. L. Zhang. A real-time detection scheme of user behavior anomaly for management information system. In *Proceedings of the 4th IEEE Information Technology, Networking, Electronic and Automation Control Conference*, Chongqing, China, pp. 1054–1058, 2020. DOI: 10.1109/ITNEC48623.2020.9084982.

[163] Y. P. Tang, B. X. Ma, Z. Wu. Research on user clustering algorithm based on software system user behavior trajectory. In *Proceedings of the 2nd International Conference on Big Data Technologies*, Jinan, China, pp. 11–14, 2019. DOI: 10.1145/3358528.3358572.

[164] S. Marchal, X. Y. Jiang, R. State, T. Engel. A big data architecture for large scale security monitoring. In *Proceedings of IEEE International Congress on Big Data*, Anchorage, USA, pp. 56–63, 2014. DOI: 10.1109/BigData.Congress.2014.18.

[165] G. M. Køien. Zero-trust principles for legacy components. *Wireless Personal Communications*, vol. 121, no. 2, pp. 1169–1186, 2021. DOI: 10.1007/s11277-021-09055-1.

[166] X. J. Wu, L. W. Xiao, Y. X. Sun, J. H. Zhang, T. L. Ma, L. He. A survey of human-in-the-loop for machine learning. *Future Generation Computer Systems*, vol. 135, pp. 364–381, 2022. DOI: 10.1016/j.future.2022.05.014.

[167] Y. P. Hu, W. X. Kuang, Z. Qin, K. L. Li, J. L. Zhang, Y. S. Gao, W. J. Li, K. Q. Li. Artificial intelligence security: Threats and countermeasures. *ACM Computing Surveys*, vol. 55, no. 1, Article number 20, 2021. DOI: 10.1145/3487890.

[168] M. N. Islam, R. Colomo-Palacios, S. Chockalingam. Secure access service edge: A multivocal literature review. In *Proceedings of the 21st International Conference on Computational Science and its Applications*, Cagliari, Italy, pp. 188–194, 2021. DOI: 10.1109/ICCSA54496.2021.00034.

[169] K. Ramezanpour, J. Jagannath. Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, vol. 217, Article number 109358, 2022. DOI: 10.1016/j.comnet.2022.109358.

[170] S. Li, M. Iqbal, N. Saxena. Future industry internet of things with zero-trust security. *Information Systems Frontiers*, to be published. DOI: 10.1007/s10796-021-10199-5.

[171] N. H. Mahmood, S. Böcker, I. Moerman, O. A. López, A. Munari, K. Mikhaylov, F. Clazzer, H. Bartz, O. S. Park, E. Mercier, S. Saidi, D. M. Osorio, R. Jäntti, R. Pragada, E. Annanperä, Y. H. Ma, C. Wietfeld, M. Andraud, G. Liva, Y. Chen, E. Garro, F. Burkhardt, C. F. Liu, H. Alves, Y. Sadi, M. Kelanti, J. B. Doré, E. Kim, J. S. Shin, G. Y. Park, S. K. Kim, C. Yoon, K. Anwar, P. Seppänen. Machine type communications: Key drivers and enablers towards the 6G era. *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, Article number 134, 2021. DOI: 10.1186/s13638-021-02010-5.

Yang Cao received the B. Sc. degree in information technology from Monash University, Australia in 2020, the M. Sc. degree in data science at Deakin University, Australia in 2021. He is currently a Ph.D. degree candidate in Deakin University, Australia.

His research interests include clustering analysis, anomaly detection and their application in renewable energy.

E-mail: charles.cao@ieee.org

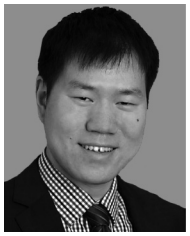
ORCID iD: 0000-0003-2184-4491

Shiva Raj Pokhrel received the Ph.D. degree in information communication technology engineering from the Swinburne University of Technology, Australia in 2017. He is a lecturer of Mobile Computing with Deakin University, Australia. He was a Research Fellow with the University of Melbourne, and a network engineer with Nepal Telecom, Nepal from 2007 to 2014. Dr. Pokhrel was a recipient of the prestigious Marie Skłodowska-Curie Grant Fellowship in 2017 and the finalist of the IEEE Future Networks′ Connecting the Unconnected Challenge in 2021. He serves/served as the Workshop Chair/Publicity Co-Chair for several IEEE/ACM conferences, including IEEE INFOCOM, IEEE GLOBECOM, IEEE ICC, and ACM MobiCom.

His research interests include multiconnectivity, federated learning, Industry 4.0 automation, blockchain modeling, optimization, recommender systems, 6G, cloud computing, dynamics control, Internet of Things, and cyber–physical systems as well as their applications in smart manufacturing, autonomous vehicles, and cities.

E-mail: shiva.pokhrel@deakin.edu.au (Corresponding author)

ORCID iD: 0000-0001-5819-765X



Ye Zhu received the Ph.D. degree in artificial intelligence with a Mollie Holman Medal for the best doctoral thesis of the year from Monash University, Australia in 2017. He is a senior lecturer at the School of Information Technology, Deakin University, Australia. He has published more than 40 papers in AI-related top international conferences or journals, including SIGKDD, AAAI, IJCAI, VLDB, AIJ, TKDE, PRJ, JAIR, ISJ and MLJ. He is on the program committee of SIGKDD, AAAI, IJCAI, PAKDD and ADMA. He has also secured several large research grants for multi-disciplinary research. He is an IEEE Senior Member.

His research interests include clustering analysis, anomaly detection, and their applications for pattern recognition and information retrieval.

E-mail: ye.zhu@ieee.org
ORCID iD: 0000-0003-4776-4932

Robin Doss received the Ph.D. degree in wireless network from Royal Melbourne Institute of Technology (RMIT) University, Australia in 2004. He is currently the Research Director of the Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Australia. In addition, he also leads the "Next Generation Authentication Technologies" theme within the National Cyber Security Cooperative Research Centre (CSCRC). His research program has been funded by the Australian Research Council (ARC), government agencies such as the Defence Signals Directorate (DSD), Department of Industry, Innovation and Science (DIIS), and industry partners. He has an extensive research publication portfolio. He is a member of the Executive Council of the IoT Alliance Australia (IoTAA). He was a recipient of the "Cyber Security Researcher of the Year Award" from the Australian Information Security Association (AISA) in 2019. He is an IEEE Senior Member.

His research interests include system security, protocol design, and security analysis with a focus on smart, cyber-physical, and critical infrastructures.

E-mail: robin.doss@deakin.edu.au
ORCID iD: 0000-0001-6143-6850

Gang Li received the Ph.D. degree in computer science from Institute of Software, Chinese Academy of Sciences, China in 2005. He is currently a professor with the School of Information Technology, Deakin University, Australia. He served on the Program Committee for over 200 international conferences in artificial intelligence, data mining and machine learning, tourism, and hospitality management. He is currently an Associate Editor of *Decision Support Systems* (Elsevier) and has been the Guest Editor of *Enterprise Information Systems* (Taylor & Francis), *Chinese Journal of Computers*, *Concurrency and Computation*: *Practice and Experience* (Wiley), and *Future Generation Computer Systems* (Elsevier).

His research interests include data mining, machine learning and business intelligence.

E-mail: gang.li@deakin.edu.au
ORCID iD: 0000-0003-1583-641X