Federated Zero Trust Architecture using Artificial Intelligence

Mukhtar Hussain, Shantanu Pal, Zahra Jadidi, Ernest Foo, and Salil Kanhere

Abstract

Cloud computing services have become ubiquitous, and currently, every organization uses some form of cloud computing service. Furthermore, even if an organization does not allow BYOD for work, employees will still bring their own devices to manage their personal communication while at work. Moreover, in this post COVID-19 era, working from home has become common. These new trends have diminished the previously known boundary between the enterprise-owned trusted network and untrusted outside networks. Therefore, a new cybersecurity paradigm is emerging that is referred to as zero trust architecture (ZTA). A ZTA protects an enterprise infrastructure based on the principles of never trusting and always verifying. The core component of ZTA is a Zero Trust (ZT) algorithm which ensures dynamic access control and continuous monitoring to establish never trusting and always verifying principles. This article provides a novel research direction based on federated artificial intelligence to develop a ZT algorithm.

Introduction

With the advancements in cloud computing technology, a typical enterprise's infrastructure has grown increasingly complex. Most enterprises have a hybrid (combination of on-cloud and on-premise) network infrastructure. Moreover, teleworking has become common in the post-COVID-19 era. This complex enterprise network has limited use of traditional perimeter-based network security architecture because there is no easily identified boundary between the internal and the external parameters. However, this hybrid network complexity has led to the development of a new cybersecurity model known as Zero Trust Architecture (ZTA) which is based on the concept of never trusting and always verifying [1]. ZTA cannot be seen as a single technology. Instead, ZTA relies on various data sources, e.g., resource access policies, threat intelligence, subject database, and activity logs to improve an enterprise's security posture. Moreover, we also require a dynamic approach that continuously learns from varying data sources (e.g., threat intelligence and activity logs) to enforce ZTA. Hence, resorting to Artificial Intelligence (AI) techniques can provide a promising solution for ZTA because relying on humans to update the policies continuously is time-consuming and prone to error [2]. However, the prohibition of sensitive data circulation in ZTA makes federated AI techniques more suitable than traditional AI techniques because federated learning allows the collaborative training of an AI model without sharing the data [3].

The main goal of ZTA is to reduce the security risks to an enterprise's resources by hardening the access control process and using continuous detection and mitigation approaches. The National Institute of Standards and Technology (NIST) defines guiding principles that must be strategically implemented to secure enterprise assets to achieve the primary goal of ZTA. One of the ZTA guiding principles is having a dynamic policy to decide whether to grant or deny access to enterprise resources. Moreover, Zero Trust (ZT) policy enforcement should be moved closer to the resources and avoid the circulation of sensitive data, e.g., user credentials [1].

The core of ZTA is a "ZT algorithm" that enforces ZTA policies. ZT algorithm is powered by a variety of data sources, e.g., the policy database with observable information about subjects (i.e., human users or applications), subject attributes and roles, historical subject behavior patterns, and threat intelligence to implement dynamic access control and continuous monitoring [4]. However, the prohibition of data circulation forces the data to exist in isolated data silos. Therefore, a privacy-preserving AI technique, i.e., Federated Learning (FL), can be adopted to develop a dynamic ZT algorithm while solving the data isolation problem. FL builds models collaboratively by sharing the model parameters instead of the private data. In this article, we present a federated ZTA using AI. The major contributions of this article are as follows:

- We discuss the applicability of FL-based AI to enable ZTA.
- We argue that the potential adoption of the proposed ZTA would be beneficial for learning the zero-trust algorithm without the need to share private data.
- We argue that the data privacy and security concerns in ZTA can be appropriately overcome using FL.

Background

This section provides a brief background of ZTA,

Mukhtar Hussain, Zahra Jadidi, and Ernest Foo are with Griffith University, Australia; Shantanu Pal is with the School of Information Technology, Deakin University, Australia; Salil Kanhere is with the University of New South Wales (UNSW), Australia.

Digital Object Identifier: 10.1109/MWC.001.2300405

FL, and Distributed Learning (DL) and an overview of existing AI-based ZTA approaches.

Zero Trust Architecture

Zero trust is a term commonly used to describe various cybersecurity solutions that focus on evaluating the identity of the user on a per-transaction basis instead of implied trust based on the network location (i.e., local area networks versus the Internet) or based on asset ownership (enterprise or personally owned). A ZTA uses zero-trust principles to plan an enterprise's network infrastructure [2].

Components of ZTA: The ZTA proposed by the NIST has three main components as shown in Fig. 1.

- Policy Engine (PE): It hosts a ZT algorithm which is responsible for the decision to grant, deny, or restrict access to the resource for a user. The inputs to the ZT algorithm are enterprise policy and external sources, e.g., Continuous Diagnostic and Mitigation (CDM) systems, threat intelligence services, and activity logs. The PE is linked with the policy administrator (PA) component to execute a decision.
- Policy Administrator (PA): It is closely linked with the PE and policy enforcement point (PEP) to ultimately allow or deny a session. The PA configures the PEP to allow or deny a session based on the input from the PE. For instance, the PA would generate an authentication token or a session-specific credential for a user to access an enterprise resource.
- Policy Enforcement Point (PEP): It acts as a communication portal between two sides, i.e., untrusted subject/user and enterprise resources. The PEP is responsible for dynamic access management by enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.

Trust Algorithm: The PE uses the trust algorithm to decide whether to grant or deny access to a resource. If the PE is considered the brain of ZTA then the trust algorithm can be viewed as the primary thought process of the brain. A ZTA provides assurance that no subject can be trusted even after initial authentication and authorization. Hence, each request is individually authorized and monitored during the access period. Therefore, the trust algorithm must be continuously updated to ensure dynamic access and authorization instead of static pre-defined policies.

According to the NIST ZTA standard [1], resources required to shape a dynamic ZT algorithm are broadly categorized based on the information they provide to the trust algorithm as shown in Fig. 2. A brief overview of these resources is provided as follows.

- Subject Database: This database contains a set of enterprise or collaborator subjects (i.e., credentials of human users or applications) and subject information, e.g., attributes and privileges assigned to them.
- Asset Database: This database contains the observable status, e.g., OS versions, software, device integrity, and the location (geographical and network) of each resource owned by the enterprise and possibly non-enterprise resources. Access to assets can be granted, restricted, or denied based on the state of the asset.
- Resource Requirements: This database contains the set of enterprise policies to complement subject and asset databases. These policies may include minimum requirements to access an enterprise resource, e.g., multifactor authentication, data sensitivity, and authenticator assurance levels.
- Threat Intelligence: This is an information feed or feeds from various sources about cyber threats to protect information technology (IT) systems preemptively. These feeds include information, e.g., active malware operating on the Internet, attack signatures, or suspected queries from malicious device(s). An enterprise can gather threat intelligence from external services as well as internal scans and discoveries to plan ahead.

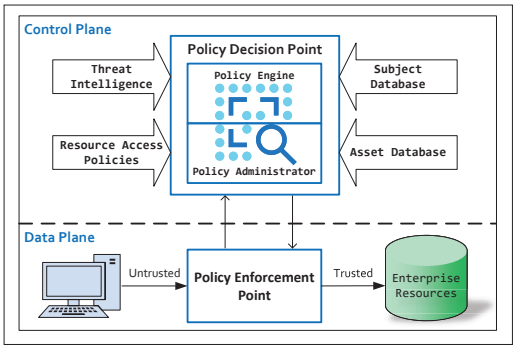

FIGURE 1. Zero trust architecture.

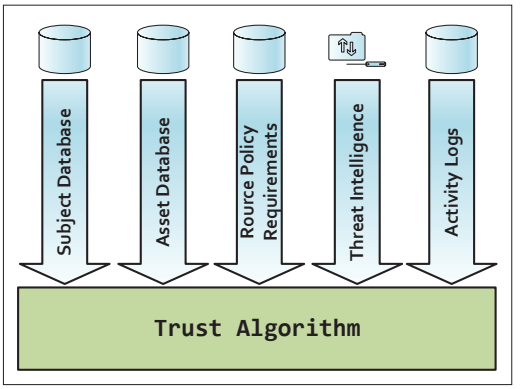

FIGURE 2. Zero trust algorithm.

The resort to AI techniques seems to provide promising solutions to automatically build a ZT algorithm, considering the variety and volume of data. However, the privacy of users and securing private information is a prime concern for organizations implementing AI-based ZTA [4]. For instance, it is challenging to manage access control in large-scale enterprises with geographically dispersed database resources that are not joined by an enterprise-owned network connection such that employees from one location may need access to the enterprise-owned resources in another location. On the other hand, collecting subject or asset data in a centralized location to facilitate access control is costly and raises privacy concerns. Another scenario is where multiple enterprises collaboratively work on a project. However, the project participants may not agree to share their subject and asset databases with each other for privacy and security concerns [1]. In such scenarios, we believe Distributed Artificial Intelligence (DAI) approaches can be beneficial for developing an intelligent trust algorithm.

The resort to AI techniques seems to provide promising solutions to automatically build a ZT algorithm, considering the variety and volume of data.

The concept of FL is rooted in the principles of developing intelligent and privacy-enhanced systems. Unlike traditional AI approaches, which require data from various organisations or devices needs to be aggregated in a central server,

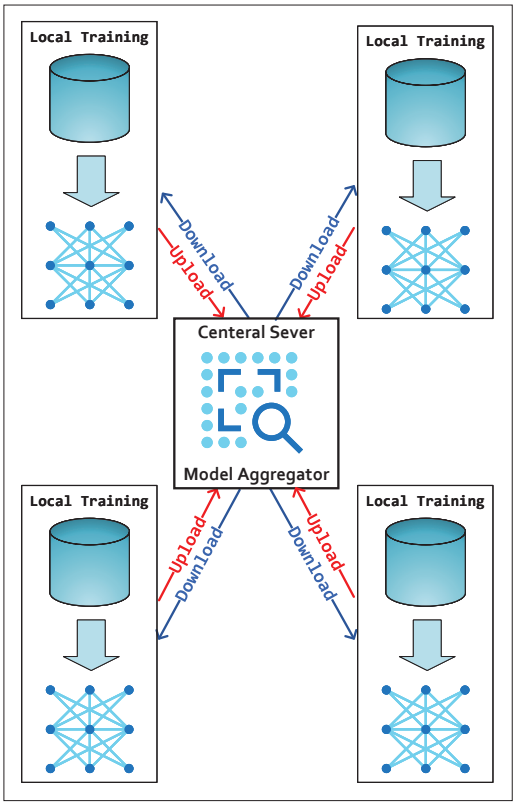

FIGURE 3. Centralised federated learning.

Distributed AI

Distributed Artificial Intelligence (DAI) is where model training and inference can be performed in a distributed manner nearby the data sources instead of collecting data under single central authority for model training. Hence, DAI is secure, trusted, and efficient compared to the traditional AI. The concept of DAI was first introduced in the 1980s. Since then, extensive growth has been seen in this area. At its core, DAI is a way of learning AI models by exploiting parallelism technologies. The parallelism mechanisms adopted in DAI can be broadly classified into two categories, explained as follows:

- Data parallelism solves the problem in case the data set is too big to be computed by the single node by partitioning the data and distributing each batch to multiple computing nodes [3]. This approach is quite useful for Internet of Things (IoT) devices. However, we assume an enterprise has sufficient resources to compute an AI model closer to each database. Moreover, we suggest that an AI model of ZT algorithm must be developed closer to each database rather than to ensure data privacy and security in a ZTA.
- Model parallelism is an approach that splits an AI model into several submodels trained by multiple nodes. One way to split a large AI model or achieve model parallelism is by deploying different neural network layers on different nodes. We believe the model parallelism technique is most suitable for learning a ZT algorithm because model parallelism can ensure data privacy, unlike the data parallelism technique. An example of a model parallelism-based DAI approach that ensures data privacy is known as FL [3] discussed in the following section.

Federated Learning

Federated Learning (FL) is a DAI approach in which a model is trained from multiple data sources without sharing the training data [6]. The concept of FL is rooted in the principles of developing intelligent and privacy-enhanced systems. Unlike traditional AI approaches, which require data from various organizations or devices needs to be aggregated in a central server, FL enables model training close to the location from where the data originated, and model parameters from local models are shared and aggregated under the coordination of a central server [3].

Classification of FL: FL can be classified into two broad categories based on the network architecture as follows:

- **Centralized Federated Learning (CFL)** is the most common architecture of FL systems. This architecture includes a centralized server and a set of distributed clients as shown in Fig. 3. The centralized server act as a coordinator to aggregate and distribute the global model among the clients. The main drawback of centralized federated learning is a single point of failure, i.e., the centralized server.
- **Distributed Federated Learning (DFL)** is a relatively new architecture of FL systems that do not contain a centralized aggregator and distributor; instead, all the participants (clients) are connected in a peer-to-peer model as shown in Fig. 4. In fact, there is no concept of a global model in DFL; each participant improves their model by sharing the parameters of their model with neighbors.

Characteristics of FL for ZTA: Several characteristics and benefits of FL are discussed in the literature [6]. Here we discuss some of the FL characteristics that make FL an ideal approach for the automated development of the ZT algorithm.

- **Privacy and Data Protection:** FL is a decentralized technology that enables an enterprise to train a collaborative AI model from scattered data resources without the need to collect any raw data [6]. Hence, enabling the development of an effective zero-trust algorithm following the NIST guidelines for implementing ZTA, i.e., limiting the data and privacy risks in an organization.
- **Open Source Framework:** The FL concept has attracted extensive attention from academia and industry. There are several open-source FL frameworks, e.g., FATE, PySyft6, PaddleFL7, FedML now up and available to support large-scale deployment of FL tasks [6]. These frameworks can be used as the basis for building ZT algorithms.

Motivating Scenarios

There can be several ways to deploy ZTA based on each enterprise environment in mind. Therefore, before discussing our approach in detail, we provide the motivational scenario, i.e., an enterprise environment that can benefit from our proposed ZTA.

One specific enterprise environment considered in our approach involves an enterprise with a single headquarters and one or more geographically dispersed offices connected over the Internet

[1]. Employees' credentials are stored locally for data security reasons. Although the local offices have their own network infrastructure, employees still require remote access to enterprise resources available in another location. Likewise, employees may be teleworking using enterprise-owned or personally-owned devices. In remote access scenarios, an enterprise may set policies to grant access to some resources but deny or restrict access to more sensitive resources.

Another scenario considered for applying our approach is a cross-enterprise collaboration [1]. An example of it can be a private agency collaborating with a government agency or a government agency that has outsourced some of its projects to private agencies. Let's government agency operates the database used for the project, but access to the database must be provided to some or all members of private agencies. Meanwhile, the government agency must restrict/deny access to all other resources.

There are several challenges an enterprise can face in the above-mentioned scenarios. A major challenge is the authentication of employees from other enterprises for cross-enterprise collaboration. A simple solution for cross-enterprise authentication could be that the enterprise can set up specialized accounts for the employees of other enterprises that need access to their resources. However, it is very challenging to manage specialized accounts. Another option is to use federated identities for authentication. However, the main challenge in implementing a federated identity management system is user privacy concerns because it involves the transfer of user credentials from one enterprise to another [10]. Another challenge is the authentication of geographically dispersed enterprise resources while having a centralized authentication system is that it becomes a single point of failure. Therefore, we present a ZTA solution with distributed authentication systems such that authentication is provided near to the resources.

Proposed Zero Trust Learning Algorithm

We have previously discussed the requirements of ZTA and how they can be addressed using FL-based AI approaches. In this section, we present our FL-based ZTA approach. Our FL-based ZTA approach is divided into two components that provide dynamic authentication and continuous diagnostics and mitigation (CDM) as shown in Fig. 1. Our approach reaps the benefits of both CFL and DFL as shown in Fig. 5.

The core component of our proposed ZTA is a Federated AI-based authentication and authorization system as shown in Fig. 5. It is a combination of ZTA components, PDP and PEP, that ultimately decides whether a subject can or cannot access the requested enterprise resource. We employ the CFL approach to ensure fast dynamic authentication of users in a distributed environment without the need for cross-enterprise sharing of user IDs. The working of this component can be seen as a federated identity management system without the need to share user ID or security context. Hence, our approach addresses the privacy concerns within traditional federated identity management systems. The specific AI algorithm we suggest a support vector machine (SVM)-based classifier to train local models to ensure

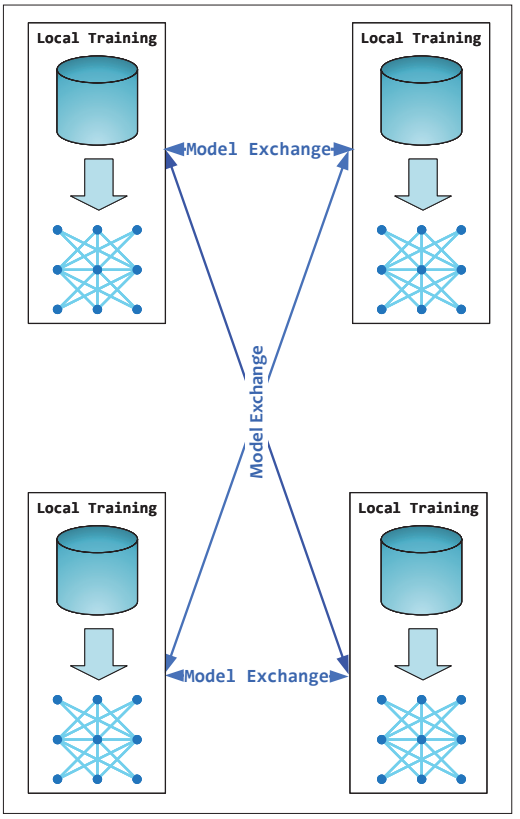

FIGURE 4. Distributed federated learning.

fast authentication and the least privilege-based access to enterprise resources based on subject attribute [11].

The second component of our approach complements the PDP/PEP system by including time-varying features such as threat intelligence and subject behaviors as shown in Fig. 5. It provides fine-grained access recommendations such as session time allocation and the resource access level to the policy engine for continuous detection and mitigation based on external and internal resources, e.g., threat intelligence, activity logs, asset database, and resource requirement policies. To train local models we suggest using natural language processing to convert policy documents into access rules [12] and SVM-based classifier to learn fine-grained access rules. We employ the DFL approach to share local model parameters instead of sharing or collecting the data to a central location [13]. Hence, avoiding privacy and security concerns with cross-enterprise sharing of sensitive data, e.g., CTIs. The main challenge for creating a global AI model from various data sources is dealing with data heterogeneity because each database may contain a completely different feature space. We understand that FL is most suitable in scenarios where data is partitioned horizontally along the sample dimension, i.e., all the databases contain homogeneous data with the same set of feature spaces [3]. However, there has been growing interest in FL from heterogeneous data, also referred to as federated transfer learning [14]. Federated transfer learning combines FL and transfer learning [3] to enable all parties to transfer the knowledge of feature space among the trained models. One such approach is using Homomorphic encryption [14].

A major challenge is the authentication of employees from other enterprises for cross-enterprise collaboration. A simple solution for cross-enterprise authentication could be that the enterprise can set up specialised accounts for the employees of other enterprises that need access to their resources.

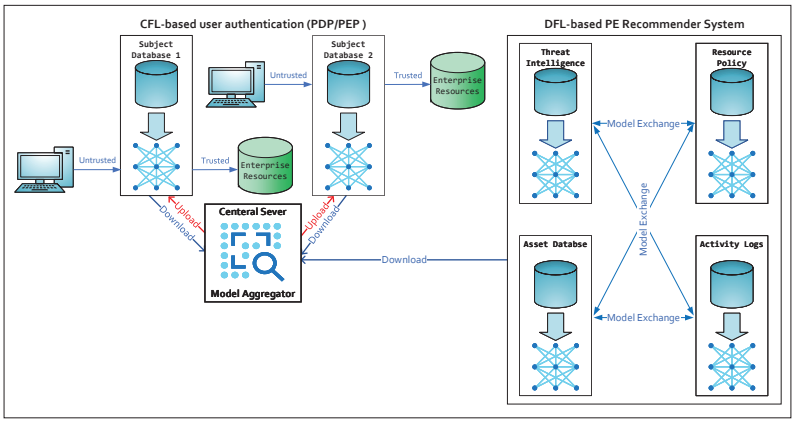

FIGURE 5. Proposed FL-based intelligent zero trust architecture.

For communication between the two components of our proposed ZTA, we suggest using a context-aware recommendation approach [15]. In this proposed communication scheme, the first component, i.e., PDP/PEP as shown in Fig. 5 provides basic authorization (i.e., grant or deny) while the second component, as shown in Fig. 5 provides the context for resources based on the activity of a user, time, location, and resource access policies. The context provides additional security context and trust awareness to grant, restrict, or deny a user's access.

In our proposed ZTA, the information/attributes from subject databases form the basis of resource access policies. At the same time, PE recommender system minimizes the uncertainty to ensure the least privilege per request based on the current information from multiple sources such as threat intelligence and activity logs. Hence, our proposed ZTA model enables a dynamic attribute-based access control (ABAC) mechanism by ensuring that both ABAC rules and trust levels are evaluated concurrently for each request.

Discussion

In this section, we provide a comparison of our proposed ZTA with the recent state-of-the-art schemes. Moreover, we discuss the challenges associated with the implementation of our approach.

Comparison with Existing ZTA Models

To demonstrate the benefit of adopting our proposed ZTA, we provide a comparison of our approach with the recent state-of-the-art ZTA models based on a set of criteria (in Table 1). The first criterion is the inclusion of static rules such as subject attributes, organization's resource access policy, and asset attributes. The second criterion is the inclusion of dynamic rules in ZTA such as threat intelligence and behavior analysis (activity logs). The third, fourth, and fifth criteria are related to the implementation of ZTA, i.e., design architecture, the process is automated using AI or requires human intervention, and the computational resources required respectively. The final criterion is the integration of ZTA into the existing infrastructure.

Hosney *et al.* [7] proposed the use of a classification approach to automate the ZT algorithm. However, their approach is not useful for the effective implementation of ZTA because does not take into consideration the dynamic environment variables such as threat intelligence or activity logs. Ramezanpour and Jagannath proposed an AI-based ZTA (i-ZTA) for next-generation communication networks [2]. Their approach enables the automation of the ZT algorithm using reinforcement and joint learning approaches. The main limitation of their work is that it requires centralized access to all the databases to learn AI-based ZT algorithms. Hence, raises user data privacy and security concerns.

Chen *et al.* [8] proposed a hierarchical ZTA model based on subject attributes, trust levels, and security policies. The dynamic aspect in their model is the trust level calculated using a trustworthy weighting method. The resource access is granted only when the trust level of a subject reaches a certain level. Safwa *et al.* [5] proposed the integration of ZT in a traditional policy, enforcement, and implementation framework. Their approach [5] also adopts a score-based trust assessment method. The main challenge of both techniques [5, 8] is to automatically establish risk scores to assess a subject's trust level.

D'Silva and Ambawade [9] proposed a ZTA for a Kubernetes-based containerized environment. Their work relies on a human to define policies for subject attributes for access control which is challenging in a continuously changing IT environment. Moreover, their approach does not take into consideration dynamic rules-based continuous monitoring.

Challenges for Using FL for ZTA

Our approach mainly relies on FL, which was first introduced in 2016, and since then, there has been extensive research conducted in this area by academics and industry experts. However, challenges still hinder the mass adoption of FL for practical applications [6]. We summarize some of these challenges concerning its application in ZTA as follows:

- **Model Update Time:** The main bottleneck in FL is the high model update time. As mentioned earlier, a ZTA involves dynamic authentication and continuous monitoring after access, which requires a very short model update time. Several factors influence the model update time, including the model upload time and the model aggregation on the server side or in a peer-to-peer network. Advanced communication technologies, e.g., 5G or 6G can reduce model upload time. However, developing an efficient model aggregation is still an open challenge.
- **Data Heterogeneity:** FL is most suitable in scenarios where data is partitioned horizontally along the sample dimension, i.e., all the databases contain homogeneous data with the same set of feature space. This issue has been recently considered in several publications as vertical FL and federated transfer learning, where the non-overlapping features are learned. However, FL with heterogeneous data is still in its infancy and requires further attention regarding privacy and optimization.
- **Privacy Risks:** FL was introduced as a distributed privacy-preserving machine learning or AI approach such that the data remains private and is never shared among the participants. However, some revelations have been made recently that retrieval of data is possible in the FL framework [6]. Data retrieval may allow an attacker to target the ZTA. One solution sug-

Test Case	Case Studies					
	Hosney *et al.* [7]	Ramezanpour *et al.* [2]	Chen *et al.* [8]	Safwa *et al.* [5]	D'Silva *et al.* [9]	[Our ZTA]
Static Rules	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Rules	No	Yes	Yes	Yes	No	Yes
Architecture	Centralised	Centralised	Centralised	Centralised	Centralised	Distributed
Automation	Decision Tree	GNN	Score-Based	Score-Based	Manual	FL
Computational Resources	Medium	High	Medium	Medium	Low	High
Integration	No	No	No	No	Yes	No

TABLE 1. Comparison of our proposed ZTA framework with existing frameworks.

gested in the literature is to use Homomorphic encryption to improve the security of FL [6]. However, further investigation is required in this direction.

- **Verification of Non-Enterprise Data Sources:** Another challenge for the enforcement of our ZTA is the verification of non-enterprise data sources (e.g., threat intelligence or activity logs) such that it does not contain any malicious data, either targeted or non-targeted towards the enterprise.

Conclusion and Future Work

In this article, we have presented an FL-based approach to implement a ZTA. Our approach is based on a decentralized AI to ensure data privacy and minimize security risks following the NIST guidelines for ZTA. We believe that our proposed ZTA model may serve as potential future directions for combining ZTA and AI. In the future, we aim to evaluate our approach in a real-life environment. Extending our ZTA to deal with the limitations of AI, for instance, An AI system can generate false negatives which can undermine ZTA model. We also consider integrating our proposed ZTA in legacy systems such as SCADA.

References

[1] S. Rose *et al.*, "Zero Trust Architecture," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., 8 2020; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[2] K. Ramezanpour and 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, 2022, pp. 1389–1286.

[3] S. Duan *et al.*, "Distributed Artificial Intelligence Empowered by End-Edge-Cloud Computing: A Survey," *IEEE Commun. Surveys and Tutorials*, vol. 25, no. 1, 2023, pp. 591–624.

[4] Y. He *et al.*, "A Survey on Zero Trust Architecture: Challenges and Future Trends," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[5] S. Ameer *et al.*, "BlueSky: Towards Convergence of Zero Trust Principles and Score-Based Authorization for IoT Enabled Smart Systems," *Proc. 27th ACM on Symp. Access Control Models and Technologies (SACMAT '22)*, 2022.

[6] Y. Liu *et al.*, "A Secure Federated Learning Framework for 5G Networks," *IEEE Wireless Commun.*, vol. 27, no. 4, 8 2020, pp. 24–31.

[7] E. Hosney, I. Halim, and A. Yousef, "{An Artificial Intelligence Approach for Deploying Zero Trust Architecture (ZTA)}," *5th Int'l. Conf. Computing and Informatics, ICCI 2022*, 2022, pp. 343–50.

[8] B. Chen *et al.*, "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture," *IEEE Internet of Things J.*, vol. 8, no. 13, 7 2021, pp. 10,248–63.

[9] D. D'Silva and D. D. Ambawade, "Building A Zero Trust Architecture Using Kubernetes," *2021 6th Int'l. Conf. Convergence in Technology (I2CT)*, Maharashtra, India, 2021.

[10] Z. Khattak, S. Sulaiman, and J. Manan, "A Study on Threat Model for Federated Identities in Federated Identity Management System," *Int'l. Symp. Info. Tech.*, 2010, pp. 618–23.

[11] H. Fang, A. Qi, and X. Wang, "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement," *IEEE Network*, vol. 34, no. 3, 5 2020, pp. 24–29.

[12] M. Narouei, H. Takabi, and R. Nielsen, "Automatic Extraction of Access Control Policies from Natural Language Documents," *IEEE Trans. Dependable and Secure Computing*, vol. 17, no. 3, 1 May-June 2020, pp. 506–17.

[13] M. Sarhan *et al.*, "Cyber Threat Intelligence Sharing Scheme Based on Federated Learning for Network Intrusion Detection," *J. Network and Systems Management*, vol. 31, no. 1, 2023, pp. 3.

[14] Y. Liu *et al.*, "A Secure Federated Transfer Learning Framework," *IEEE Intelligent Systems*, vol. 35, no. 4, 7 2020, pp. 70–82.

[15] M. Unger, A. Tuzhilin, and A. Livne, "Context-Aware Recommendations Based on Deep Learning Frameworks," *ACM Trans. Management Information Systems*, vol. 11, no. 2, 6 2020, pp. 1–15.

Biographies

Mukhtar Hussain (mukhtar.hussain@griffith.edu.au) is associated with Griffith University, Brisbane, Australia. He received his PhD from the Queensland University of Technology (QUT), Brisbane, Australia. His research interests are securing cyber systems from the engineering and design perspective, such as physical layer security of wireless communication systems and behavioural modelling of industrial control systems for anomaly detection.

Shantanu Pal [SM] (shantanu.pal@deakin.edu.au) is associated with the School of Information Technology, Deakin University, Melbourne, Australia. Shantanu has extensive research experience and knowledge in Internet of Things, big data and distributed smart applications, access control, trust management, blockchain technology, mobile and cloud computing, etc.

Zahra Jadidi (z.jadidi@griffith.edu.au) is associated with the School of Information and Communication Technology, Griffith University, Brisbane, Australia. She received her PhD degree in network security from Griffith University. Her research interest is cybersecurity, security of cyber physical systems, machine learning applications in security analysis, and security of machine learning algorithms. She is a Fellow of the Higher Education Academy (FHEA), Australia.

Ernest Foo [SM] (e.foo@griffith.edu.au) is associated with the School of Information and Communication Technology, Griffith University, Brisbane, Australia. His research interests can be broadly grouped into the field of secure cryptographic protocols with an active interest in network security applications.

Salil Kanhere [SM] (salil.kanhere@unsw.edu.au) is associated with the School of Computer Science and Engineering, University of New South Wales, Sydney, Australia. His research interests include the Internet of Things, cyber-physical systems, blockchain, pervasive computing, cybersecurity, and applied machine learning. He is also affiliated with the UNSW Institute of Cybersecurity (IFCYBER). He is a Senior Member of the ACM.