World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:17, No:12, 2023

A Practice of Zero Trust Architecture in Financial Transactions

L. Wang, Y. Chen, T. Wu, S. Hu

***Abstract*—**In order to enhance the security of critical financial infrastructure, this study carries out a transformation of the architecture of a financial trading terminal to a zero trust architecture (ZTA), constructs an active defense system for the cybersecurity, improves the security level of trading services in the Internet environment, enhances the ability to prevent network attacks and unknown risks, and reduces the industry and security risks brought about by cybersecurity risks. This study introduces Software Defined Perimeter (SDP) technology of ZTA, adapts and applies it to a financial trading terminal to achieve security optimization and fine-grained business grading control. The upgraded architecture of the trading terminal moves security protection forward to the user access layer, replaces VPN to optimize remote access and significantly improves the security protection capability of Internet transactions. The study achieves: 1. deep integration with the access control architecture of the transaction system; 2. no impact on the performance of terminals and gateways, and no perception of application system upgrades; 3. customized checklist and policy configuration; 4. introduction of industry-leading security technology such as single-packet authorization (SPA) and secondary authentication. This study carries out a successful application of ZTA in the field of financial trading, and provides transformation ideas for other similar systems while improving the security level of financial transaction services in the Internet environment.

***Keywords*—**Zero trust, trading terminal, architecture, network security, cybersecurity.

I. Introduction

WITH the continuous rise of cloud computing, big data, the Internet of Things and other emerging technologies, the IT environment is becoming more and more complex, and the IT architecture is changing from bounded to borderless. For financial transactions, users access financial terminals through the Internet to make large and high-frequency transactions, and any user of any device at any location may have access. How to ensure authorization and transaction security in this situation is crucial. With the development of digital trading, the disappearance of network boundaries has led to the inability of location-based security systems to meet the needs of cybersecurity, and financial trading infrastructures are facing the challenge to gradually migrating to a more flexible and secure ZTA.

This study is an application of zero trust security concept in the field of financial transactions, taking a trading terminal, the infrastructure of financial transactions, as the object of transformation, reinforcing the active cybersecurity defense system of the trading terminal and improving the level of financial infrastructure security. The aim is to achieve deep integration of zero trust concepts such as context-awareness with fine-grained access control architecture of the core trading terminal without affecting the performance of the trading terminal and gateway and the transparency of the application area. Specifically, it is proposed to accomplish the following tasks.

1) Build a multi-source trust assessment system.
2) Realize hierarchical and categorical security control for different businesses and different users.
3) Avoid malicious access to the trading system.

A. Zero Trust Architecture

The idea of ZTA was coined by John Kindervag in 2010 [1]. Zero trust entails having no trust in anyone, requiring everyone to authenticate, and enforcing stringent identity management and access control procedures to restrict access to the resources users require. There are three main concepts: the first is to validate and safeguard all sources; the second is to impose stringent access controls; and the third is to inspect and record all network traffic logs.

The essence of zero trust is to create a dynamically authorizable and fine-grained access control system that uses identity as a foundational link between the endpoint and the protected resources. The user has been granted "least adequate" access to the protected resources.

In the white paper "Zero Trust Architecture Standards" [2], NIST (National Institution of Standards and Technology) lists three technical solutions: the first is SDP; the second is Identity and Access Management (IAM); and the third is Micro-segmentation (MSG). Fig. 1 shows the system architecture of the standard ZTA.

SDP was introduced by the Cloud Security Alliance as a security architecture with dynamic protection features [3], [4]. SDP performs multi-factor authentication on the client before entering the user login phase. The client can only connect to the service when the authentication is accomplished. SDP has been proven to be efficient in preventing network attacks by requiring only slightly more time to establish a connection [5]. It has also been confirmed that adding SDP to real-time protocol monitoring can extend security beyond the initial authentication phase, thus enabling scalable security and reliability management of the system [6].

L. Wang is with CFETS Information Technology (Shanghai) Co., Ltd., China (corresponding author, phone: 86-15258851254; e-mail: wangliwen_zh@chinamoney.com.cn).

Y. Chen is with CFETS Information Technology (Shanghai) Co., Ltd. (phone: 86-13564634556; e-mail: chenyuting@chinamoney.com.cn).

T. Wu is with CFETS Information Technology (Shanghai) Co., Ltd.. He is the head of Product Department (phone: 86-13564688164; e-mail: wutong@chinamoney.com.cn).

S. Hu is with CFETS Information Technology (Shanghai) Co., Ltd. (phone: 86-15221851371; e-mail: hushaolei_zh@chinamoney.com.cn).

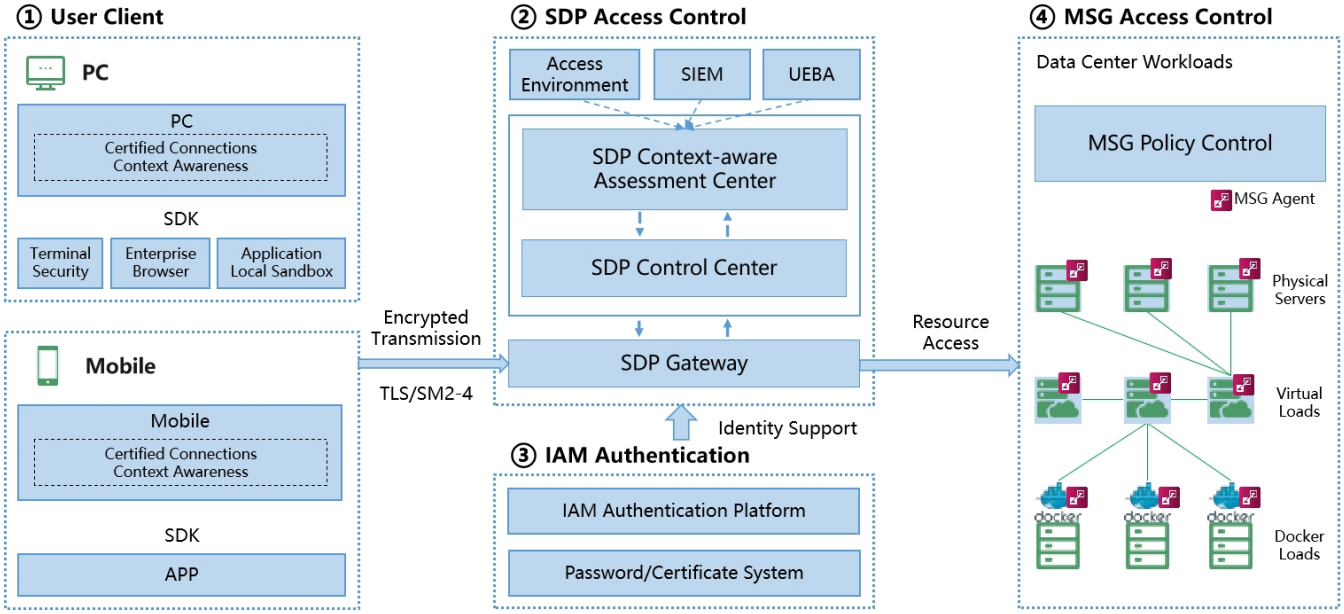


Fig. 1 The standard ZTA

IAM has the functions of single sign-on, authentication management, centralized policy-based authorization, as well as dynamic authorization. It decides who can access, how to access, and which operations to perform. With the unified and intelligent technology of IAM, organizations can simplify administration and optimize security and compliance by condensing each user's multiple identities into one and establishing a unified set of roles and rules, such as authentication through multi-factor or password management [7], [8].

MSG is a fine-grained network isolation technology that can cope with traffic isolation in traditional, virtualized, hybrid cloud, and docker environments, and stop attackers from entering the enterprise data center network after lateral penetration. It is a method of dividing a network into smaller logical segments with the goal that only authorized endpoints can access resources on that segment. Experiments have proven that micro-segmentation is resilient to port scanning and malware propagation, and can effectively reduce the attack surface [9], [10].

These three technologies are also the main technical means to implement zero trust. However, in the actual implementation of ZTA, many other supporting technologies must be included depending on the application scenario. When implementing ZTA, financial institutions need to make multiple technical selections in terms of architecture, strategy, and model.

B. Security Risks of Financial Trading Infrastructure

With the rapid development of big data, cloud computing, Internet of Things, and mobile Internet technologies in recent years, most institutions are using big data platforms and private cloud platforms as the underlying support for financial services, resulting in a high concentration of data and service security risks, such as a lack of meticulous and effective internal controls, difficulties in meeting regulatory requirements, etc.

Financial institutions must carry out a number of tasks when implementing ZTA. Technology used can differ significantly since distinct financial application scenarios can differ significantly from one another, and thus the zero trust technologies used to meet the security protection requirements may also vary greatly. Institutions must act in accordance with the actual requirements of their own business. To implement ZTA, the institution must choose the appropriate technology from a variety of options.

The following security problems exist in the financial trading terminal to be renovated in this study.

1) There are hidden dangers in security monitoring and response, the coverage, accuracy and timeliness of security monitoring need to be optimized, and the protection efficiency needs to be improved.
2) In the Internet environment, users have more diversified access subjects and methods, and the risk concentration of core business systems will be further aggravated.
3) Generic security products cannot meet the personalized application security needs of trading terminals.

Therefore, the following research questions are proposed.

1) How to deeply integrate zero trust modules with the architecture of the trading terminal?
2) How not to affect the performance of terminals and gateways, and to achieve the application system upgrade without user perception?
3) How to meet the numerous application compliance and system security requirements for the financial industry?
4) How to hide core business assets, ensure core business security, and not affect the original business process?

II. Method

The core idea of the zero trust transition in this study is to achieve dynamic access control with zero trust concept at user login and access to services by integrating the capability of

context awareness in the financial trading terminal. The technical path is to transit to ZTA at the user layer (terminal) and the access layer (REST gateway), by integrating the security information of the endpoint collected by the context-aware SDK, which is evaluated in real time by the SDP control center and then subscribed by the REST gateway, thus realizing the dynamic control of resource access requests. The specific process is as follows:

1) The trading terminal obtains the unique endpoint ID through the integrated context-aware SDK in the context-aware agent and prompts the user risk information during the service access process.
2) The gateway server queries the user score (in the range of 0-100) to the context-aware server through the endpoint ID passed when the user logs in or accesses the business, and the gateway determines whether to allow the user to log in or access the services based on the predefined security score threshold.

Fig. 2 shows the ZTA for the financial trading terminal in this study. The Rest gateway is the execution point for dynamic access authorization to the demilitarized zone (DMZ) and the most central component in the entire architecture. The context-aware server is deployed as a bypassed component and communicates with the endpoint through a separate data channel without directly impacting the original business data channel. It has the following functions:

1) When the Rest gateway is initialized, it obtains the endpoint score, endpoint login policy and resource access policy from Redis inside the cluster and loads them locally for use. Meanwhile, it subscribes to the endpoint score and permission setting information channel in Redis and receives the latest score information and permission setting for local update.
2) When a user logs in, the Rest gateway queries the context-aware server for policies related to login authority information based on the endpoint ID of the login request, and determines whether the endpoint's score is higher than the threshold value, and allows the user to perform subsequent login operations only if the requirements are met. If the policy related to the login authority information is not available, the gateway will block or release the login request according to the local configuration.
3) When a user accesses a service, the Rest gateway checks whether the endpoint score is higher than the threshold value based on the latest locally stored resource access policy, and allows access to the service only when the requirements are met.
4) When the score or policy of an endpoint changes, the Rest gateway uses the latest score and policy to make a judgment on the endpoint request.

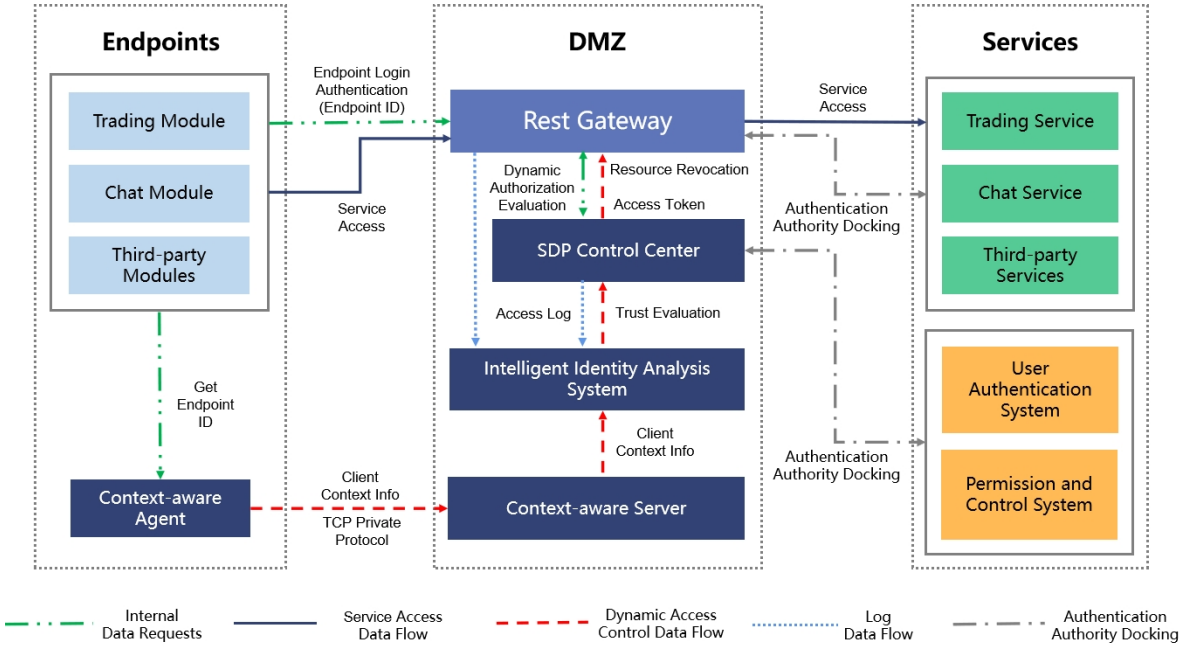


Fig. 2 The ZTA for the financial trading terminal in this study

The key technical features of the architecture introduced in this study are described in the following four sections.

A. Deep Integration with the Core Service Access Control Architecture

In a standard ZTA, legacy endpoints and endpoints equipped with context-aware capabilities tend to co-exist, while zero trust access control consoles and Rest gateways are mostly deployed in series. The zero trust transition project of this study is based on the implementation of the architecture of the existing financial trading terminal and the REST gateway, maintaining the existing "one terminal, one gateway" architecture (see Fig. 2).

In terms of terminal integration, the context-aware SDK adopts asynchronous design and decouples from business modules to realize instant reading and reporting of contextual

information, so as to balance terminal performance and security. At the same time, it fully considers the characteristics of different transaction modules with different security requirements and supports dynamic service access and graded security protection to adapt to various business services.

In terms of gateway integration, the Rest gateway introduces a third-party policy injection mechanism, and the zero trust security policy can be injected into the gateway cluster through a standardized interface to take effect in real time, ensuring uninterrupted security.

B. No Impact on the Performance of Terminals and Gateways and No Sense of Application System Upgrade

Firstly, there is no impact on terminal performance. The context-aware SDK integrated in the terminal adopts the independent agent integration mode, and the sensing data are reported asynchronously and in real time through the SM2-4 data security tunnel without additional consumption of terminal resources, with an average CPU resource occupation rate of < 0.1% and memory usage of < 4 M.

Secondly, there is no impact on the performance of the Rest gateway, which achieves zero trust with its memory-based asynchronous filtering mechanism. The main flow of front and backend calls is not affected, and the performance of the gateway is not lost (excluding the message header parsing logic, which is only reduced by about 1%). The TPS reaches nearly 70,000/sec, and the latency is < 1 ms (see Table I). There is no increase in OS resource usage and no performance loss.

TABLE I
PERFORMANCE TEST RESULTS OF THE REST GATEWAY WITH ZERO TRUST

Scenarios	Number of Concurrent Threads	Average Response Time (Milliseconds)	TPS
Rest Gateway Business Message (without zero trust)	50	<1	68650
	70	**<1**	**69604**
	90	<1	69332
Rest Gateway Business Message (with zero trust)	50	<1	67211
	70	**<1**	**68817**
	90	<1	68503

Thirdly, the application system upgrade is user-perception-free. The terminal realizes no user perception when upgrading and running through automatic update and perception-free authentication and operation technology. The new services added to the server side are completely isolated from the services in the existing application area, realizing no interference with the existing transaction business services.

C. Customized Checklist and Policy Configuration for the Financial Industry

Context-aware check items are the source for determining the trustworthiness of user terminals. The checklist for this study is configured with customized checklist and corresponding policies for financial industry compliance and security requirements (see Table II).

On one hand, the check items in this study are well diversified and flexibly configured. The check items cover two categories including application compliance and system security, with more than 20 sub-categories and 80 items in total, which meet the specific security specification requirements of the financial industry and have proven to be compatible with the common security policies of financial institutions. All check items can be customized with threat levels, distinguishing between veto items and potential risk items. The authentication supports certificate signature verification to ensure that it will not be tampered with and bypassed.

On the other hand, the architecture designed in this study features real-time acquisition and encrypted transmission, which meets the specific security specifications of the financial industry. It has a system-level acquisition engine with two-way authentication and data encryption technology for client-server communication certificates to ensure the integrity and security of context-aware polices and data uploads.

TABLE II
CUSTOMIZED CHECKLIST FOR THE FINANCIAL INDUSTRY

Type	Check Items
Application compliance	Process list (blacklist and whitelist)
	Software list (blacklist and whitelist)
	System patch check
System security	Host check
	Account login failure restriction
	System firewall status check
	Inbound domain check
	Local identity theft prevention
	Password maintenance requirements
	Account access control
	Account permission control
	Remote assistance configuration detection
	Network settings detection
	Remote desktop service detection
	Event log service detection
	Windows update detection
	Windows remote management (WinRM)
	Auto play detection
	File explorer detection
	Windows installer detection
	Network access configuration detection
	User permission assignment configuration detection

D. Introduction of Cutting-Edge Security Technology SPA and Secondary Authentication

Firstly, the SPA technique is introduced. The SPA port knocking key and target address distributed by the SDP control center are received and assembled into UDP messages to initiate port knocking authentication to the SDP Gateway, which hides core business assets behind the SDP Gateway protection layer, effectively reducing the external exposure of business and stopping DDoS attacks and replay attacks. The specific process is as follows (see Fig. 3):

1) The endpoint initiates authentication (high-strength two-factor authentication) to the SDP control center, and the authentication can dock to the user's existing AD, LDAP and other identity sources.
2) After successful authentication, the SDP control center distributes a single packet knocking key (seed key) to the

terminal and synchronizes the knocking target address (the SDP gateway address and port).

3) The SDP control center distributes the port knocking key to the corresponding SDP gateway (knocking destination service) at the same time.
4) The terminal uses the port knocking key to assemble UDP messages for knocking verification, and then establishes a secure transmission channel for service access.

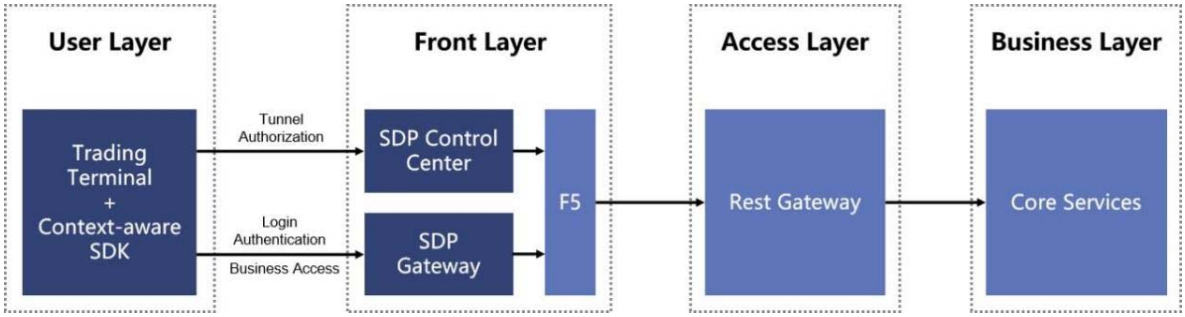


Fig. 3 SPA process

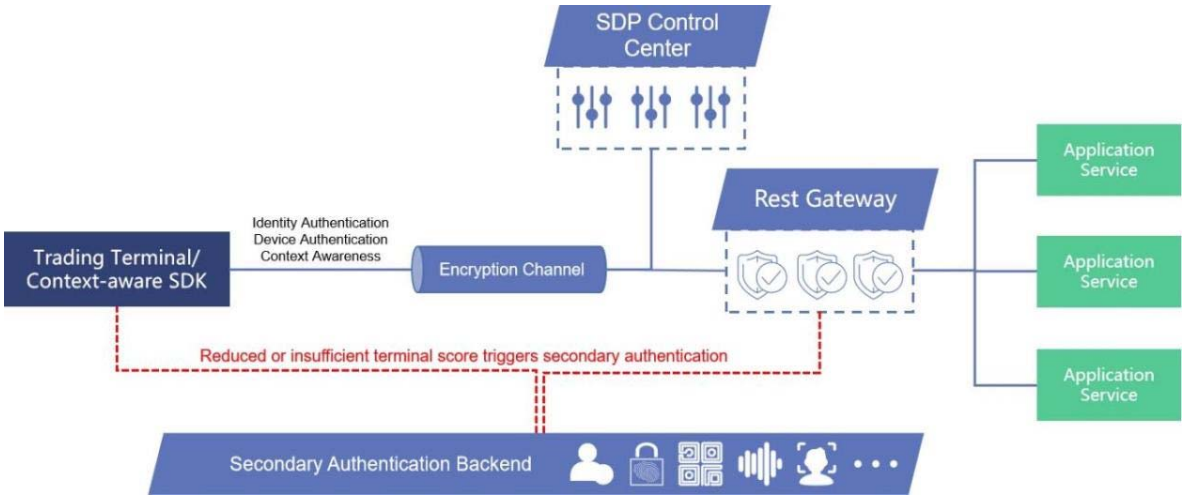


Fig. 4 Technical architecture diagram for secondary authentication

TABLE III
COMPARISON OF THE RESULTS OF SIMULATED ATTACKS BEFORE AND AFTER ZERO-TRUST DEPLOYMENT

Attack Techniques	Without Zero Trust	With Zero Trust	Protection Principles
Client-side application reverse debugging	Memory data and internal operational logic leakage	Instant access blocking	Continuous dynamic detection of threat process and application
Client-side application module tampering	Binary code instruction tampering	Instant access blocking	
Client-side process injection	Malicious module code running in the process address space	Instant access blocking	
Client-side page reverse debugging	Risk of page memory objects, data, network request packets, account data leakage, etc.	Instant access blocking	
Terminal risk: - System firewall status - Login failure restrictions - Local identity theft prevention - Password maintenance requirements	Risk of system brute force cracking, account impersonation, etc.	Terminal access downgrading	Baseline continuous dynamic detection
System vulnerability risk	Risk of ransomware, mining virus propagation, SMB horizontal attack, etc.	Instant access blocking	Real-time high-risk system vulnerability detection

Data are authenticated and authorized through the transmission tunnel to ensure data transmission security and performance. The data tunnel supports standard TLS, RSA 128, RSA 256, SM2-4 and other encryption methods. A single endpoint establishes only one secure tunnel, eliminating the need for repeated tunnel creation/destruction processes and significantly improving tunnel transmission performance. The datagram transmission protocol removes unneeded information from the header, effectively reducing the message size and improving transmission efficiency.

Secondly, a secondary authentication mechanism is introduced to ensure core business security (see Fig. 4). Based on the endpoint score, the user access area is divided into security zone, buffer zone and high-risk zone, which

correspond to three scenarios: accessing normal business, triggering secondary authentication and blocking business access, respectively. The SDP control center determines the endpoints with potential risks, and the system can provide grayscale disposal plan without forcibly blocking access and increasing operation and maintenance costs by affecting business.

III. Experiment and Results

To verify the effectiveness of zero trust protection, simulated attacks on the trading terminal are conducted without and with zero trust, respectively. The simulated attacks concluded that the system with zero trust can detect and block threats at the access layer.

The attack preparation is as follows:

1) Load the Intranet terminal with penetration testing tools such as Apktool, IDA, ADB, Burp Suite, XRay, SQLMap, etc.
2) Launch the trading terminal.

It has been proved that the deployed zero trust module effectively reduces the risk of terminals running malicious programs or security penetration tools through dynamic detection, instant access blocking and access permission downgrading, and prevents threats such as system internal operation logic and data leakage, program instruction tampering, and system cracking. A comparison of the results of simulated attacks without and with ZTA is shown in Table III.

IV. Discussion

A comparison between the standard ZTA and the ZTA deployed in the financial trading terminal in this study is shown in Table IV. Compared to the standard ZTA, the ZTA in this study achieves upgrades in terms of instantly triggered trusted authentication at login, the most granular business hierarchy control, no performance impact and no user perception. However, this study still has the following limitations. First, this study has not yet applied the micro-segmentation technology of zero trust; second, the access of mobile terminals has not yet been retrofitted with zero trust; third, the behavior analysis module of trading users has not yet been deployed and landed.

V. Conclusion

In this study, the architecture of a financial trading terminal is renovated to meet the requirements of zero trust. The ZTA modules are integrated in the user layer (terminal) and access layer (REST gateway), and the terminal security information is collected by deploying a context-aware SDK, evaluated by the SDP control center in real time, and then subscribed by the REST gateway, so as to achieve dynamic control of resource access requests.

TABLE IV
Comparison of the standard ZTA and the ZTA in this study

Type	Security Capabilities	Standard ZTA	ZTA in this study	Security Technology Support
Multi-source security policy	Identity security	√	√	Authentication by username, password, certificate, etc.
	Device security	√	√	Terminal device baseline check
	Application compliance	√	√	Software and process exclusion
Continuous trusted access	Network invisibility	√	√	Use SPA to hide critical services and narrow the exposure
	Personalized check items	-	√	Combine member organization security policies and support custom configurations
	Login to trust	-	√	Login page triggers security assessment
Dynamic intelligent permissions	Dynamic access control	√	√	Dynamically adjust user access rights to protect business data assets
	Business hierarchy protection	√	√	Access policies with different security levels for businesses of different sensitivities
	Minimum authorization	-	√	Fine-grained control of business interface access level
	Enhanced authentication	-	√	Support for secondary authentication to enhance user experience
Integrated deployment convergence	Financial transaction applications	-	√	Application of zero trust in core financial transaction scenarios
	Minimalist and lightweight architecture	√	√	Build a minimalist architecture with end, gateway and control plane as core components
	High performance	-	√	Terminal and gateway performance are unaffected and updates are user-perception-free

The results of the simulated attacks prove that the deployed zero trust modules can effectively reduce the risk of terminals running malicious programs or security penetration tools by dynamically detecting and instantly blocking access and degrading terminal access, preventing threats such as internal operation logic and data leakage of the system, tampering with program instructions, and using terminal risks to crack the system.

The revamped architecture strengthens the active network security defense system of the trading terminal and improves the security level of the financial infrastructure without affecting the performance of the trading terminal and gateway as well as the transparency of the application area.

This study is a successful practice of ZTA in the field of financial transactions, improving the security level of the financial trading services of our institution via Internet while providing ideas for similar infrastructures.

In the future, we will promote the application of the zero trust in more core business systems, the pilot application of alternative VPN solutions in office networks, the transformation of zero trust in mobile terminals, the introduction of micro-segmentation access control solutions,

and the study of user behavior analysis modules.

REFERENCES

[1] J. Kindervag, *Build Security into your Network's DNA: the Zero Trust Network Architecture*. Forrester Research Inc 27, 2010.
[2] S. Rose, O. Borchert, S. Mitchell, S. Connelly, *Zero Trust Architecture. NIST Special Publication (SP)*. pp. 800–207, 2020.
[3] Software Defined Perimeter Working Group, *SDP Specification 1.0*. Cloud Security Alliance, 2014.
[4] Software Defined Perimeter Working Group-Cloud Security Alliance (CSA), *Software Defined Perimeter*, 2013.
[5] P. Kumar, A. Moubayed, A. Refaey, A. Shami, J. Koilpillai, "Performance Analysis of SDP for Secure Internal Enterprises," in *Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC'19)*, pp. 1–6, 2009.
[6] S. Nair, "SDP Based Zero-Trust Architectures," in *Proceedings of the 2022 ACM on International Workshop on Security and Privacy Analytics (IWSPA '22)* , New York, 2022.
[7] I. A. Mohammed, "Identity and Access Management System: A Web-Based Approach for an Enterprise," *International Journal of Advanced and Innovative Research*, 1(4), pp, 1–7, 2011.
[8] I. A. Mohammed, "Intelligent Authentication for Identity and Access Management: a Review Paper," *International Journal of Management, IT and Engineering (IJMIE)*, 3(1), pp. 696–705, 2013.
[9] N. Sheikh, M. Pawar, V. Lawrence, "Zero trust using Network Micro Segmentation," *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1–6, 2021.
[10] M. Mujib, R. F. Sari, "Design of implementation of a zero trust approach to network micro-segmentation," *International Journal of Advanced Science and Technology*, 29(7), pp. 3501–3510, 2020.

Liwen Wang (Shanghai, China, 1988) holds a bachelor in Software Engineering and a bachelor in Japanese (Dalian University of Technology, China, 2010), and a Ph.D. in Computer Science and Technology (Zhejiang University, China, 2018).

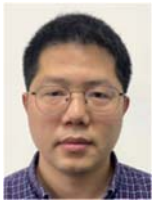
She is currently in charge of research management in CFETS Information Technology (Shanghai) Co., Ltd., which is a subsidiary of China Foreign Exchange Trade System (CFETS). Her main research fields include Human-Computer Interaction and System Design. She has published many academic conference and journal papers as *What People Inquire about Locations? A Study on the Taxonomy of Location based Questions in Campus* (CHI, 2014), *Understanding User Behavior of Asking Location Based Questions on Microblogs* (IJHCI, 2016), *Uncertainty Visualization for Mobile and Wearable Devices Based Activity Recognition Systems* (IJHCI, 2016), *A Comparative Study of Map Exploration Interfaces for Multi-Touch Tabletops (IJHCI, 2017) and Investigating the User Behaviors of Sharing Health and Fitness Related Information Generated by Mi Band on Weibo* (IJHCI, 2018).

Yuting Chen (Shanghai, China, 1985) holds a bachelor in Information Security and a bachelor in Finance (Shanghai Jiao Tong University, China, 2007), and a master in Communication and Information Systems (Shanghai Jiao Tong University, China, 2010).

He is currently in charge of project management in CFETS Information Technology (Shanghai) Co., Ltd., which is a subsidiary of China Foreign Exchange Trade System (CFETS). His main research fields include the inter-bank market data exchange platform and the unified terminal technology. He has published many international papers such as *Speaker Identification Based on Deep Learning in FX iDeal system, Journal of Physics: Conference Series, 2018* and *A reliable messaging middleware for financial institutions, ICCIP, 2017*. He also holds a number of invention patents.

Tong Wu (Shanghai, China, 1984) holds a master and a bachelor in Computer Science and Technology (Fudan University, China, 2020 and 2007). He is an expert member of ISO20022, and a member of the China Computer Federation (CCF).

He is currently in charge of project and technology management in CFETS Information Technology (Shanghai) Co., Ltd., which is a subsidiary of China Foreign Exchange Trade System (CFETS). His main research fields include core transaction system design, financial infrastructure construction, middleware and technology framework design, and AI. He has published many academic conference papers and reports such as *Co-Attentive Multi-Task Learning for Explainable Recommendation* (IJCAI, 2019), Research on Compliance Supervision Data Analysis Model Based on Mass Chat Records in the Inter-Bank Market (ICBAIE, 2021) and *In-memory Replication Clustering Matching System* (Experience Report). He also holds a number of invention patents.



Shaolei Hu (Shanghai, China, 1984) holds a bachelor in Software Engineering (Chongqing University, China, 2007).

He is currently in charge of system architecture design in CFETS Information Technology (Shanghai) Co., Ltd., which is a subsidiary of China Foreign Exchange Trade System (CFETS). His main research fields include core transaction system design, middleware and technical framework design and transaction terminal architecture design. He also holds a number of invention patents.