

A Private Blockchain System based on Zero Trust Architecture

Yao-Chung Chang ^a, Yu-Shan Lin ^b, Arun Kumar Sangaiah^c and Hsin-Te Wu ^a

^a Department of Computer Science and Information Engineering, National Taitung University, Taitung, Taiwan

^b Department of Information Science and Management Systems, National Taitung University, Taitung, Taiwan

^c Department of International Graduate School of Artificial Intelligence, National Yunlin University of Science and Technology, Yunlin, Taiwan

Email: ycc.nttu@gmail.com, ysl.nttu@gmail.com, arunks@yuntech.edu.tw, wuhsinte@nttu.edu.tw

Abstract— During the outbreak of COVID-19, many enterprises massively created Virtual Private Networks (VPNs) for companies to cooperate; however, these accounts lacked efficient management after the epidemic, leading to data leakage or the suffering of malicious attacks. Consequently, several firms have started to build private blockchains for data preservation and verification. Private blockchains are usually built internally in companies; once a firm's internal network opens for massive external logins, many servers and private blockchains cannot work properly to protect data. In general, private blockchains store critical personal information or relevant confidential data; once a private blockchain opens to external access, all the information in the network nodes will be exposed, making private them lose their protection functions.

This paper proposes a security mechanism using a private blockchain system based on zero trust architecture. The zero trust architecture tracks every user's network conditions and analyses whether their behaviors are authorized. Additionally, the system utilizes micro-segmentation to divide the private blockchain, preventing the system from malicious attacks. The proposed system employs user multi-factor authentication to identify users, and the zero trust architecture tracks and analyzes if users' behaviors are reasonable. This method effectively ensures corporate networks' security and enables private blockchain to filter legal and authorized users to access and verify.

Keywords— Zero Trust Architecture, Virtual Private Networks, Blockchain

I. INTRODUCTION

Despite the rapid development of technology and the Internet, corporate network architectures are mostly conventional types. However, many technological companies require information access across external and internal networks, making corporate networks even more unsafe. Moreover, many employees and partner suppliers have started working remotely, and firms massively create VPN accounts to maintain their business operations, lowering corporate networks' protection. As a result, once hackers access a company's internal network through VPNs to attack or tap, they will cause network paralysis or data breaches of various vital servers. Private blockchains protect networks internally,

preventing external users from accessing or adding data. When the internal protection fails, external users can access information on private blockchains freely. As companies usually build private blockchains for storing confidential data, the function of a private blockchain can avoid servers' misfunctions that stop the users who genuinely need to access important data. The setup of private blockchains allows specific groups of users to access data; therefore, it is necessary to develop more authentication methods and protection measures to secure the safety of private blockchains.

This research presents a private blockchain mechanism based on zero trust architecture using an intrusion-detection system and firewall. We also utilize the intrusion-detection system to construct the micro-segmentation mechanism, which will separate high-risk equipment and make malicious attacks fail to penetrate the separated parts. The operation of micro-segmentation prevents unauthorized users from accessing the specific equipment. Meanwhile, this study further analyzes user behaviors to judge the rationality of each user; when discovering unusual actions, the intrusion-detection system will terminate the user's access. The multi-factor authentication mechanism used in this research verifies if a user possesses the authorization to access the private blockchain. The experiment proves that the proposed approach of this article can enhance the safety of private blockchains; in other words, the research implements network attacks using popular techniques to confirm whether the attacks invade the separated equipment. Consequently, the experimental result has proven that the proposed method is effective.

II. RELATED WORK

Literature [1] demonstrates a method to store patients' electronic medical records and the Internet of bodies' data in blockchains, resolving the massive storage issue of medical data; furthermore, blockchains possess the features of verification and distribution, which can ensure data safety and completeness. In Literature [2], the article presents a lightweight blockchain mechanism that employs a chameleon hash function to verify user identities and data completeness; the function allows users to generate a secret key freely

between themselves and verify data completeness directly. The experimental result of the research proves that the approach has reached a level of data security with lightweight encryption and decryption. On the other hand, Literature [3] constructs a blockchain system to deliver employees' performance; the system establishes records for employees to prove their monthly workloads and confirms credibility through data authentication. In the future, enterprises can evaluate and conduct employees' job appraisals by reviewing their historical workload records. The eVoting system presented in Literature [4] suggests a secured technique to evaluate voters' identities; afterward, blockchains in the system, which have features of better immutability and completeness, will process the voting, achieving the goal of an eVoting system. Meanwhile, the traceable agricultural products system developed in Literature [5] combines blockchain technology to tackle the conventional supply chain issues of agricultural products effectively; additionally, the system designs a user-friendly interface for farmers to input data easily. Literature [6] aims to improve the source verification of vaccines; the system uses blockchains to inspect vaccine distribution, and users can review relevant information through the system. Finally, Literature [7] builds a peer-to-peer energy trading system; the immutability characteristic of blockchains enables users to process peer-to-peer transactions without seeking a third-party certification.

III. THE PROPOSED SYSTEM

A. System Model

In our research, the zero trust architecture developed by an intrusion-detection system and a firewall is utilized to establish a security mechanism using private blockchains, as shown in Figure 1. Firstly, the firewall divides equipment into different parts and verifies identities; afterward, the intrusion-detection system creates Virtual Local Area Networks (VLANs) for separation, preventing malicious users from accessing critical equipment. Meanwhile, the intrusion-detection system will also track users' online behaviors; when detecting unusual behaviors, the system temporarily suspends the user's action. Users' unusual behaviors vary; for example, when a user's login location changes dramatically within one hour, it probably means the user has experienced hackers' invasion and conducted attacks in many countries using IP hopping. The proposed design also contains a multi-factor authentication mechanism, using various identity authentication methods to verify legal users. For instance, users can access private blockchains to conduct further actions when confirmed and authorized; if they fail to pass the verification three times, the system will lock their IP locations. This study aims to create a complete network security architecture, making private blockchains safer and avoiding data leakage.

B. Zero Trust Architecture

The next-generation firewall can operate on the first layer of the open systems interconnection model, namely the physical layer, without needing to change the setting of other

adjacent network equipment; moreover, the firewall works on the connection modes of the first through the third layers. As shown in Figure 2, the setup of the next-generation firewall is the same as setting up a core switch; the next-generation firewall distributes network interfaces, and the cables connect to related office equipment, such as network switches and wireless network devices. Unlike a core switch in a conventional network setup, where server cables can connect directly to a core switch, the average port cost of the next-generation firewall is higher. Furthermore, because the port numbers are fewer after transferring to the next-generation firewall, several servers have to share 1 Gbps of bandwidth. Hence, engineers must consider whether the network bandwidth is sufficient to fulfill business needs. The study enhances the transmission bandwidth using the Link Aggregation Control Protocol standard to enrich access efficiency, reserving the original architecture with the defined VLAN and allowing the next-generation firewall to distribute the routing among VLANs.

C. Multi-factor authentication

The multi-factor authentication mechanism used in this study primarily employs the APP-ID technique developed by Palo Alto Networks, a precise traffic identification and classification system. Unlike the conventional fourth-layer firewall, the APP-ID technology does not rely on port connection or communication protocols to identify applications but utilizes various mechanisms to check them. Such a technique provides visibility, operational status, behavior traits, and relevant risk information regarding the applications, preventing the possible methods of evading inspection used by hackers. Furthermore, the system builds security rules by application types to initiate, inspect, or block unnecessary applications, as shown in Figure 3. Apart from the APP-ID technique, the proposed mechanism further checks users' personal information using different authentication methods, such as birthdays and phone numbers; users who pass the authentication can access the private blockchain system.

IV. EXPERIMENT RES

The experimental environment is set in an intranet; we employ three devices to attack the system and test if the micro-segmentation can effectively reduce attack ranges and risks. Additionally, our research further connects the system to Palo Alto Networks, simulating hackers' attacks on the Internet to evaluate the firewall performance on threat defense. Finally, we conduct lateral movement to the data center; Table 1 presents the attack approaches utilized in this study. In sum, our research implemented various malicious attacks and found that all the attack ranges were within the areas of micro-segmentation, proving that the proposed method can effectively reduce attack ranges.

Table 1、Experiment type

Attack model	coping strategies		
Antivirus/anti-malware	Firewall	IPS	Intrusion Prevention
Network intrusion prevention	Firewall	IPS	Intrusion Prevention
Restrict web-based content	Firewall	IPS	Intrusion Prevention
Endpoint behavior prevention	Firewall	IPS	Intrusion Prevention
Implement prevention	Firewall	IPS	Intrusion Prevention
Password policy	Multi-factor authentication		
Network traffic filtering	Firewall	IPS	Intrusion Prevention
Restrict access to resources over the network	Firewall	IPS	Intrusion Prevention

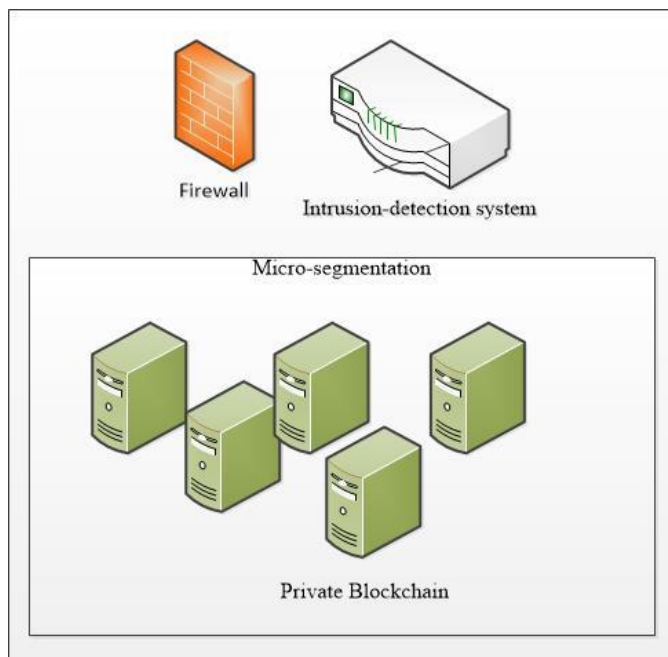


Figure 1. System Model

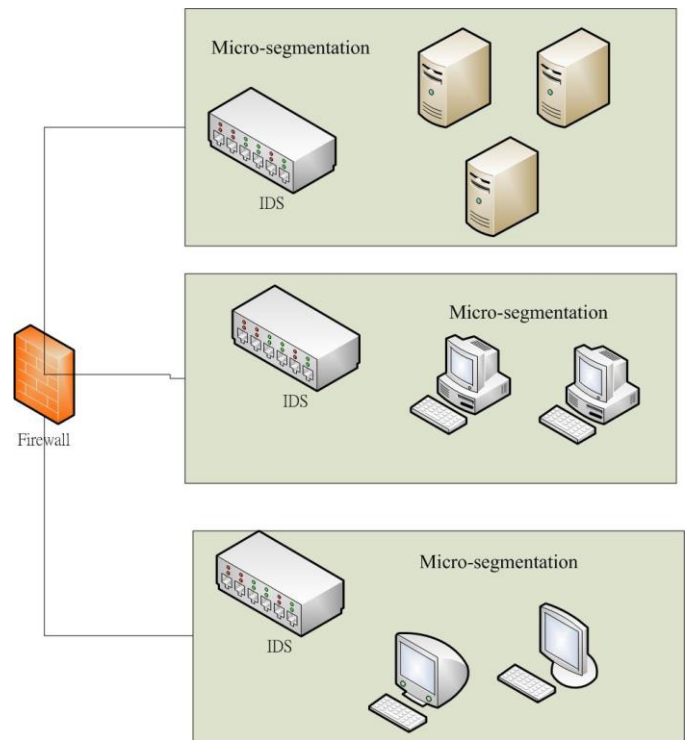


Figure 2. Zero Trust Architecture

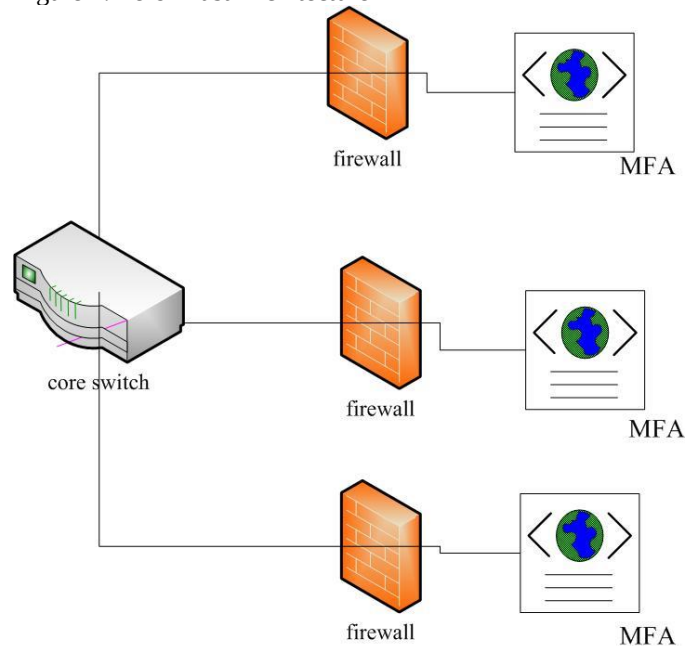


Figure 3. Multi-factor authentication

V. CONCLUSIONS

With the advance of emerging technologies, conventional network architectures cannot fulfill today's technical needs; moreover, those corporate VPN accounts created during the outbreak of COVID-19 might increase the risks of cyberattacks if hackers invade. This article presents a security mechanism using a private blockchain system based on zero trust architecture, utilizing micro-segmentation and user

behavior analytics to fight against the vulnerability attacks of emerging technologies. We have also combined multi-factor authentication to verify user legality. The experimental result proves that the proposed method can effectively withstand different cyberattacks, preventing separated equipment from relevant attacks.

ACKNOWLEDGMENT

This paper was supported by the National Center for High-Performance Computing and National Science and Technology Council, Taiwan, under grant no. NSTC 111-2410-H-143 -023, NSTC 111-2222-E-224 -004, NSTC 111-2221-E-143 -006 -MY2, NSTC 111-2410-H-143 -007, NSTC 112-2622-H-143 -001 and NSTC 111-2622-H-006 -004.

REFERENCES

- [1] J. Liu et al., "Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain," in *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 5, pp. 2231-2242, May 2023, doi: 10.1109/JBHI.2022.3183397.
- [2] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang and L. Gao, "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things," in *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4371-4384, 15 March 15, 2022, doi: 10.1109/JIOT.2021.3103275.
- [3] F. Wilhelmi, S. Barrachina-Muñoz and P. Dini, "End-to-End Latency Analysis and Optimal Block Size of Proof-of-Work Blockchain Applications," in *IEEE Communications Letters*, vol. 26, no. 10, pp. 2332-2335, Oct. 2022, doi: 10.1109/LCOMM.2022.3194561.
- [4] F. D. Giraldo, B. Milton C. and C. E. Gamboa, "Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept," in *IEEE Latin America Transactions*, vol. 18, no. 10, pp. 1743-1751, October 2020, doi: 10.1109/TLA.2020.9387645.
- [5] A. Tharatipyakul and S. Pongnumkul, "User Interface of Blockchain-Based Agri-Food Traceability Applications: A Review," in *IEEE Access*, vol. 9, pp. 82909-82929, 2021, doi: 10.1109/ACCESS.2021.3085982.
- [6] L. Cui, Z. Xiao, F. Chen, H. Dai and J. Li, "Protecting Vaccine Safety: An Improved, Blockchain-Based, Storage-Efficient Scheme," in *IEEE Transactions on Cybernetics*, vol. 53, no. 6, pp. 3588-3598, June 2023, doi: 10.1109/TCYB.2022.3163743.
- [7] J. Abdella, Z. Tari, A. Anwar, A. Mahmood and F. Han, "An Architecture and Performance Evaluation of Blockchain-Based Peer-to-Peer Energy Trading," in *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3364-3378, July 2021, doi: 10.1109/TSG.2021.3056147.



Yao-Chung Chang (M'03) received the Ph.D. degree from National Dong Hwa University, Hualien, Taiwan, in 2006.

He is a Professor of the Department of Computer Science and Information Engineering, National Taitung University, Taitung, Taiwan. His primary research interests include intelligent communication System, IoT, and cloud computing.

Dr. Chang is a recipient of the subsidization program in universities for encouraging exceptional talent, Ministry of Science and Technology, Taiwan



Yu-Shan Lin received the Ph.D. degree from National Sun Yat-sen University, Kaohsiung, Taiwan, in 2006.

She is a Professor of the Department of Information Science and Management Systems, National Taitung University, Taitung, Taiwan. Her research interesting areas include Digital Learning, Information Technology Education, Marketing Management, Internet

Marketing, and Tourism Marketing. Dr. Lin had the honor to get the Subsidy for College and University Research Rewarding from Ministry of Science and Technology (MOST).



Prof. Arun Kumar Sangaiah received his Ph.D. from School of Computer Science and Engineering, VIT University, Vellore, India. He is currently a Full Professor with National Yunlin University of Science and Technology, Taiwan. He has published more than 300 research articles in refereed journals (IEEE TII, IEEE TITS, IEEE TNSE, IEEE TETCI, IEEE SysJ, IEEE SensJ, IEEE IOTJ, ACM TOSN) 11 edited

books, as well as 1 patents (held and filed) and 3 projects, among one funded by National Science and Technology Council (NSTC), Taiwan, Ministry of IT of India and few international projects (CAS, Guangdong Research fund, Australian Research Council) cost worth of 500000 USD. Dr. Sangaiah has received many awards, Yushan Young Scholar, Clarivate Highly Cited Researcher (2021,2022), Top 2% Scientist (Standord Report-2020,2021,2022), PIFI-CAS fellowship, Top-10 outstanding researcher, CSI significant Contributor etc. Also, he is responsible for Editor-in-Chief, and Associate Editor of various reputed ISI journals. Dr. Sangaiah is a visiting scientist (2018-2019) with Chinese Academy of Sciences (CAS), China and visiting researcher of Université Paris-Est (UPEC), France (2019-2020) and etc. His Google Scholar Citations reached 19800+ with h-index: 78 and i10-index: 298.



HSIN-TE WU is an Associate Professor of Department of Computer Science and Information Engineering from National Taitung University, Taiwan. He has served as Associate Editor for International Journal of Big Data and Analytics in Healthcare. He has served as Special Issue Guest Editor of Journal of

Supercomputing and IET Networks. His research interests include computer networks, wireless network, speech compression, network security, blockchain and Internet of things.