Journal of information and
communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 18(2): 94-99, Jun. 2020 Regular paper

Hyperledger Blockchain Design for Sharing, Spreading, and Protecting National Cybersecurity Information

Dea-woo Park[1*] **and Sang-hyeon Lee**[2]

[1]Department of Convergence Engineering, Hoseo Graduate School of Venture, Seoul 06724, Republic of Korea
[2]Department of Convergence Engineering, Hoseo Graduate School of Venture, Seoul 06724, Republic of Korea

Abstract

Real cyberterrors are invisible and difficult to identify. Even after a cyberattack, its origin and cause are difficult to determine. Cyberterrorism results in invisible cyberwars, and it is believed that World War IV will begin with a cyberwarfare. For national cybersecurity, information on cybersecurity must be collected, shared, and disseminated. In this study, we investigate a blockchain system designed based on the World Cybersecurity Agreement. National cybersecurity information is linked to the hyperledger blockchain system network through the National Cybersecurity Center. National cybersecurity information designs and uses a secure protocol for protection; further, it is collected, shared, and disseminated to treaty countries. National cybersecurity information is shared and spread by the hyperledger blockchain system, and it uses a cyberdefense system that responds to the cyberattacks and their origin. This paper serves as a policy and legislation guideline for forming a World Cybersecurity Agreement between countries.

Index Terms: Blockchain, National Cybersecurity, Protecting, Sharing, Technical Information

I. INTRODUCTION

Statistically, 39% of all cyberattack attempts are web-based, 31% application vulnerability, and 9% scanning attacks. A “web-based attack” is a web vulnerability attack, in which the injection attack is ranked as the number one vulnerability in the list of Top 10 Open Web Application Security Project [1]. Cybernetworks, in particular, are used to operate and control social, national, traffic, telecommunications, electricity, and gas infrastructures. Personnel who decide the operation of the national infrastructure not only conduct business through cyber, but also perform transportation, communication, and finance. Owing to cyberterrorism such as APT(Advanced Persistent Threat) attacks [2] on the terminals of decision makers, Cyber attacks have occurred on the infrastructure of countries [3] around the world. Because of the importance of cybersecurity on cyberattacks, countries are developing strategies to maintain national cybersecurity [4], which affects individual cybersecurity. Hence, China’s General Staff of the People’s Liberation Army controls the civilian organization, providing optical communication network and IP at the state level [5]. Cyber-attacks in the world are active in fileless attacks. Microsoft announced in July 2019 that it has detected a fileless attack named Astaroth. Payload, a malicious code, operates directly from a computer’s memory to a process using a fileless technique. Malware PowerGhost infects workstations and servers on corporate networks to mine new cryptocurrencies. In other words, malware PowerGhost is not stored on the hard disk, but it is downloaded and executed.

The world’s Internet and communications are intercepted and hacked to perform cyberattacks and cyber operations,

Received 13 March 2020, **Revised** 25 June 2020, **Accepted** 25 June 2020
***Corresponding Author** Dea-woo Park (E-mail: prof_pdw@naver.com, Tel: +82-2-2059-2352)
Department of Convergence Engineering, Hoseo Graduate School of Venture, 06724, Republic of Korea .

Open Access **https://doi.org/10.6109/jicce.2020.18.2.94** print ISSN: 2234-8255 online ISSN: 2234-8883

e.g., advanced persistent threat attacks on the smart home system [6] and DoS(Denial of Service) attacks on the Internet of things (IoT) for 5G [7]. However, the United States declares that if damage is caused by an invisible cyberattack, its response must be comparable to that of a physical warfare in the visible world [8]. Cyberterrorism threatens national cybersecurity, resulting in an invisible cyberwarfare.

Herein, we propose the World Cybersecurity Agreement (WCA), which has national cybersecurity centers in every country. The national cybersecurity center collects, shares, and spreads national cybersecurity information, which is categorized into cyberattack, cyber vulnerability, and cyberattack response information.

To secure national cybersecurity, cyberweapons have been developed and used as cybertechnology. In addition, governments, academia, and industry in every country should research and develop their national cyberwarfare, cyberterrorism, cyberattack technology, and technology to perform cyberdefense as well as foster and train cyberwarfare agents. To determine the origin of cyberattacks between countries or to use cyberdefense systems that respond to cyberattacks, national cyber information collection, sharing, and dissemination, as well as information protection and cybertechnologies are required. The collection, sharing, dissemination, and protection of national cybersecurity information will eventually form a World Cybersecurity Agreement between nations and will be the foundation for establishing national cybersecurity. This study will serve as a basis for creating policies and legislations that will strengthen world and national cybersecurity as well as diminish concerns regarding the outbreak of World War IV.

II. ANALYSIS OF NATIONAL CYBERSECURITY INFORMATION DUE TO CYBERATTACK

A. Analysis of Worldwide Cyberattack Information

To analyze the major cyberattacks worldwide, Table 1 shows cyberattack occurrences by location and year.

A cyberattack infected Altran Technologies' systems with malware. Consequently, Altran Technologies shut down it networks and applications to protect customer data and company assets. The hacking attack was presumed to be performed using a new ransomware, LockerGoga.

Judging from the message of the publicly available attack evidence sample shown in Table 1, we conclude that it was a ransomware attack. The attack evidence sample was first uploaded to Romania's Virus Total on January 24, 2019. Subsequently, it was uploaded in the Netherlands. If the uploaded file is the same as that the attacked Altran file, it would be the ransomware LockerGoga [9].

Table 1. Cyber operation countries and cyberattacks

Year	Operation country	Occurrence of cyberattacks
2020		Continuous occurrence of ransomware attacks
2019		60% cybercrime hacked SW vulnerabilities and broken authentication
2018	North Korea	Hacked Indian Cosmos Bank and seized $ 13.5 million
2017	North Korea	WannaCry 2.0 Ransomware attacked 30 million computers
2016	North Korea	South Defense Network DIDC Vaccine Relay server hacking attack
2015	China	21.5 million information outflows from US federal officials
2014	Russia	US White House computer network penetration

B. Analysis of Organizations and Roles for National Cybersecurity in South Korea

As of 2020, the Ministry of the Interior and Safety of the South Korean government manages response to cybersecurity and information protection. The Ministry of the Interior and Safety includes the Infrastructure and Information Protection Policy Bureau. This bureau includes the Information Resource Policy Division, Information Infrastructure Protection Policy Division, Personal Information Protection Policy Division, and Personal Information Protection Cooperation Division.

As of 2020, the Minister of Science and ICT heads the Cyber Security and Network Policy Bureau, which is responsible for national cybersecurity response technologies and policies. The Cyber Security and Network Policy Bureau includes the Network Policy Division, Network Security Planning Division, Cyber Security Planning Division, Cyber Security and Threat Management Division, and Cyber Security Industry Division [10], which support South Korea's cybersecurity and information security policies and industries.

The South Korea Internet & Security Agency (KISA) contributes to cybersecurity in the private sector, including corporations and the general public. The KISA is managed by the Management Planning Group, South Korea Internet Security Center, Personal Data Protection Group, and Data Economy Promotion Division. Under the South Korea Internet Security Center, 14 teams in 4 departments are addressing cybersecurity in the private sector [11].

The Office of National Security is the central administrative body of the Republic of South Korea that assists the President in his duties regarding national security. It is located at 1 Cheongwa-daero, Jongno-gu, Seoul. The chief director is a minister-level government official, whereas the second deputy is a minister-level official.

C. Analysis of National Cybersecurity Information Collection and Sharing in South Korea

The President's Office of National Security analyzes and responds to national cybersecurity information through the National Intelligence Service, Department of Defense, and Armed Forces Cyber Command. The cybersecurity of public institutions is undertaken by the Ministry of the Interior and Safety, whereas public–private organizations including corporations are undertaken by the KISA. National cybersecurity policy development and technology research and development are undertaken by the Minister of Science and ICT.

In particular, the KISA operates Cyberthreat analysis and sharing (C-TAS), which serves as a hub for companies to respond quickly and share cyber information from dangerous cyberattacks. In C-TAS, indicators of compromise information are shared in malicious code samples and attacks for conducting cyberattacks against the general public, such as phishing and SMiShing. However, to collect and share information in C-TAS, it must be subscribed and responded to by donating information. In the first stage, C-TAS collects cyberthreat information; in the second stage, the information is analyzed comprehensively; and in the third stage, information is shared.

In Step 1 KISA and various cybersecurity breach information, IP information, and new malware information are collected to perform attacks that threaten cybersecurity.

In Step 2, the validity and reputation of the collected cyberthreat intelligence are verified, and high-risk cyberattack signs and correlations are analyzed. In addition, statistics regarding the sharing of collected information for each type of cyberthreat intelligence are prepared, and statistical analysis is performed based on the in-memory database.

In Step 3, cyberthreat information of C-TAS is shared by downloading through an API and homepage that can be shared automatically in real time. The policy of information sharing can be differentiated between the object and scope of institutional information sharing through authority management. Shared information is categorized into eight groups: single indicator, analysis report, trend information, continuous information, duplicate information, trend information, key information, and brokerage fee. The shared information include malware, C & C, infected IP, dissemination, phishing, farming, SMiShing, information leak, malicious e-mail and security notice, and doc. In addition, information on threat information is shared on a daily, weekly, and monthly basis.

In C-TAS, cyberthreat information sharing is performed to protect endpoints that guard the cyber infrastructure, including the enterprise. Malware samples provided by C-TAS can be used to update their antivirus engines to prevent malware infection. By identifying the unique identification value of new malicious codes, it can detect and block malicious file infections and transmissions.

D. Cyberattack Information of National Cybersecurity

Cyberweapons that attack the cyberworld can be classified into software and hardware types [12]. Hardware-type cyberweapons conduct cyberattacks on networks and computer systems that constitute the infrastructure of the state and society. Software-type attacks attack software against the operating system or operating system that constitute the infrastructure of a country and society.

Cyberattacks begins by receiving the associated cyberattacks and identifying the signs of the attack; the forensic evidence of cyberattack and spear phishing scenarios will begin the backtracking of cyberattacks through cyberattack and cybervulnerability analyses.

After analyzing the router table via the intermediate zombie PC or C & C server and finally obtaining IoT forensic evidence, the attack origin IP and Mac address are analyzed. Once the origin of the cyberattack is identified, the offensive response is to use the preemptive cyber response strategy. First, we identify the system vulnerability of the national infrastructure and it with computer viruses using social engineering methods. Infected systems, in part, cause functional failures, which ultimately result in suspensions and failures of state and social infrastructure systems as well as failures and deletions of control system functions.

III. SHARING, SPREADING, AND PROTECTING NATIONAL CYBERSECURITY INFORMATION USING HYPERLEDGER BLOCKCHAIN

A. World Cybersecurity Agreement Performs National Cybersecurity with Blockchain

Each country in the world joins the World Cybersecurity Agreement. Blockchain technology is used in the distributed ledger. If the transaction information of the distributed ledger is encrypted and recorded in the blockchain, even if the distributed ledger's transaction is arbitrarily modified or deleted, transaction records of other ledgers exist such that the ledger's records can remain deceived.

B. Feasibility Analysis of Hyperledger Blockchain

Herein, we propose the World Cybersecurity Agreement, in which the blockchain to be used in is designed as a hyperledger blockchain, as shown in Fig. 1.

The peer-to-peer distributed ledger of the hyperledger blockchain records transaction details by time, and the details are formed in blocks and interconnected while forming a chain, thereby improving security in hacking attacks. The smart contract of the hyperledger blockchain is a proof of contract. Unlike financial institutions, smart contract platforms such as Ethereum do not involve financial institutions but form a blockchain with contracting parties to create smart contracts. When the supplier's product arrives at the consumer, an IoT sensor is activated and the supplier receives the payment.

Cyberattacks can violate cybersecurity by launching malware or malware attacks that can infect software. The hyperledger blockchain can track the process steps and save decisions such as voting records to enhance the authenticity and reliability of the process, which can then be used as evidence for settlement and voting. Furthermore, product history and distribution channels can be traced back. The distributed ledger of the hyperledger blockchain proves the copyright and allows user tracking and content usage. Audit trail software is an immutable record that is used as evidence in forensic trials.

C. Protecting Spread of National Cybersecurity Information Sharing

The functional design of the hyperledger blockchain is designed to share, spread, and protect national cybersecurity information.

1) User Terminal Design

Design terminals such as mobiles and PCs for users using the hyperledger blockchain use a mobile PC graphical interface. Users are not only authorized PCs, but also designed to receive and share information via the mobile interface to the user's terminal, such as a smartphone. The secure network protocol is used for communication between terminals. The user's access control is authenticated through three steps: identity authentication, headquarter authentication, and third-party authentication. If the authentication identification (ID) password PW) or the like is identified as biometric or random number authentication, then read–write–execution can be performed according to the security level of the user. Biometrics such as the ID PW for authentication or random number authentication values are encrypted and transmitted. The authentication value is confirmed by comparing the hash function values of SHA-1, SHA256, and SHA512 according to the terminal type.

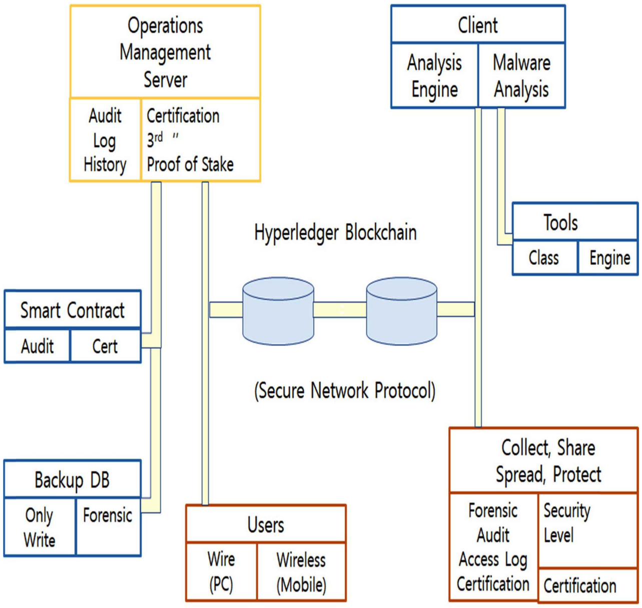

Fig. 1. Comparison of hash values using Quick hash.

2) Hyperledger Blockchain Operations Management Server Design

The hyperledger blockchain operations management server creates a blockchain. Through blockchain mining, tokens can be issued and third-party certifications can be sent to the management server to create and maintain a blockchain as well as design an application program interface of the manager. Various programs that are required for blockchain creation and operation management are written using the application program interface and designed to be easily managed. It is designed to utilize the mashup function and upgrade the blockchain operation management server.

A blockchain can reduce the number of nodes. However, only a limited user who manages national cybersecurity information is subscribed, and smart contracts are issued for each limit, period, and allocated capacity exceeding the capacity of cybersecurity information. Information that is issued separately by the smart contract, or that with low usage rate and less security, is designed to be accessed using a third database separately. The collection, sharing, and dissemination of information are performed by the construct blockchain operation.

Identity management, which accesses the operation management server, uses the application programming interface. In other words, an identification PW from a trusted certification authority can be used. However, third-party authentication and headquarter authentication require a one-time password and headquarter authentication, such as biometric authentication through a smartphone.

3) Hyperledger Blockchain Client Design

Clients of each country that have subscribed to record the collected and analyzed cyberattack, vulnerability, cyberattack response information in distributed ledger using distributed ledger framework. Design client engine to handle national cybersecurity information in server. In particular, malware and malware analysts, or investigators who trace back cyberattack infection contents and paths, are designed to use the client engine. Malware use signature analysis to design client engines and user applications for computer antivirus manufacturing after the analysis of malware.

4) Collecting, Sharing, and Spreading National Cybersecurity Information

Each country collects cyberattack, cybervulnerability, and cyberattack response information and records them in a distributed ledger. After sharing the information, it is spread to manage services based on urgency.

Non-face-to-face blockchain users on a distributed network are untrusted nodes. They are designed to use algorithms that guarantee the integrity of the hyperledger blockchain system by mutually verifying the mathematically calculated result value for users connected to the blockchain.

Proof of work uses computing power to derive consensus by calculating and verifying the value of a nonce by hashing the hash of a particular difficulty. However, to reduce computing power wastage by connecting the wireless user of proof of work from a user or client, it is designed as an algorithm to derive consensus and distribute reward through the proof of stake.

A user's access control is saved in the only-read mode through the og history and cannot be modified. Authentication and access control ca be designed using forensic tools; The accessor's ID and PW comprising 10 characters or more, including special characters, are set. The set PW is designed to program the encryption setting method to change periodically. After identity verification, the company undergoes three stages: headquarter certification and third-party certification. If authentication or the like is confirmed as biometric or random number authentication, then read–write–execution can be performed according to the security level of the user.

The disadvantage of the blockchain is that to prevent a high processing time when the numbers of nodes and information volume increase, the one-year cyber information leaves label and log records through the smart contract engine, but the details of the directory under the server designed are supplied separately.

It is designed such that an administrative user with operation authority can authenticate it for the hyperledger blockchain and issue a smart contract according to the security level after access. A smart contract is designed as an algorithm to derive an agreement through the proof of stake. When the user is authorized, the hyperledger blockchain consensus algorithm is used to perform the work with the general consent and the center director's agreement.

5) Vulnerability Analysis Design

Cyberattack, cybervulnerability, and cyberattack response information are designed to be classified into relevant information by analyzing big data. We conducted a (semi) automatic behavior analysis and infringement incident analysis for cyberattacks and responses using artificial intelligence algorithms. The cyberattack response information corresponded with the big data analysis and the artificial intelligence algorithm to respond to cyberattacks in real time.

IV. CONCLUSIONS

Cyberterrorism has resulted in an invisible cyberwar, and it is believed that World War IV would begin with a cyberwarfare. As APT attacks cause cyberterrorism, countries worldwide are emphasizing more on cybersecurity.

We proposed the World Cybersecurity Agreement to collect, share, and spread cybersecurity information for national cybersecurity. As countries worldwide enter the World Cybersecurity Agreement, cyber alliances must share cyberattack, vulnerability, and cyber information regarding cyberattack response. To protect the system while collecting, sharing, and disseminating national cybersecurity information, it must be built as a secure blockchain system. In this study, we analyzed the security of blockchain and designed a hyperledger blockchain system for the World Cybersecurity Agreement.

National cybersecurity information is linked to the hyperledger blockchain system network through the National Cybersecurity Center. National cybersecurity information designs and uses the security protocol for protection. National cybersecurity information is designed as an algorithm that derives consensus and distributes rewards through the proof of stake in user terminal design, and hyperledger blockchain client design such that the hyperledger blockchain system can be shared and spread. For vulnerability analysis, we conducted a (semi) automatic behavior analysis and an infringement incident analysis for cyberattacks and responses using an artificial intelligence algorithm, which is designed to respond to cyberattacks in real time.

In future studies, the cyberdefense system should be policy driven and passed into legislation to operate in real time under the World Cybersecurity Agreement to respond to cyberattacks.

ACKNOWLEDGEMENTS

This study was supported by the Academic Research Fund of Hoseo University in 2019 (No. 2019-0411).

REFERENCES

[1] OWASP Top Ten, Top 10 Web Application Security Risks [Internet], Available: https://owasp.org/www-project-top-ten/, 2020.

[2] W. Phillip and C. D. Brunst, "Terrorism and the Internet: new threats posed by cyberterrorism and terrorist use of the Internet, in Marianne Wade and Almir Maljevic´ (eds.), a war on terror?: the European stance on a new threat," in *Changing Laws and Human Rights Implications*, New York, NY: Springer, 2010.

[3] T. Anna-Maria, "Cyberterrorism: in theory or in practice?," *Defense Against Terrorism Review*, vol. 3, no. 2, pp. 63-64, 2010.

[4] D. W. Park, "Draft of national cybersecurity act," *International Journal of Security and Its Applications*, vol. 9, no. 11, pp 105-112, 2015.

[5] D. W. Park, "National cyber security organization system," in *The National Cybersecurity Forum, National Cyber Safety Federation*, National Assembly of the Republic of Korea, 2017.

[6] C. D. Cho and D. W. Park, "Building an overseas infrastructure offices of the information security industry," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 20, no. 1, pp. 102-109, 2016.

[7] L. W. Santoso, R. Lim, and K. Trisnajaya, "Smart home system using Internet of things," *Journal of Information and Communication Convergence Engineering*, vol. 16, no. 1, pp. 60–65, 2018.

[8] K. Rim and D. Lim, "DoS attack control design of IoT system for 5G Era," *Journal of Information and Communication Convergence Engineering*, vol. 16, no. 2, pp. 93–98, 2018.

[9] BLEEPINGCOMPUTER New LockerGoga Ransomware Allegedly Used in Altran Attack. [Internet], Available: https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/, 2020.

[10] Minister of Science and ICT Organization, [Internet], Available: https://www.msit.go.kr/english/msipContents/contents.do?mId=Mjg1. 2020.

[11] KISA Organization. [Internet], Available: https://www.kisa.or.kr/eng/aboutkisa/organization.jsp. 2020.

[12] S. H. Bae and D. W. Park, "Cyber weapon model for the national cybersecurity," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 23, no. 2, pp. 221-228, 2019.

Dea-woo Park

He is an Associate Professor in the Hoseo Graduate School of Venture at Hoseo University in South Korea. Professor Park studies cybersecurity, hacking, forensic, and convergence of information communication technology in the HFICT Lab at the Hoseo Graduate School. Professor Park received the B.S. degree in computer science from the Soongsil University in 1995, and the M.S. degree in 1998. He received the Ph.D. degree from the computer science department of the Soongsil University in 2004. He has been appointed the Secretary General of Forum of National Cybersecurity Policy, Chair of Korea Information Security Forum, and Vice-Chairman of Korea Institute of Information Security & Cryptology, Korea, Information and Communications Society.

Snag-hyeon Lee

As a police officer, he served as the head of the Jongam Police Station and as a Senior Superintendent at the Seoul Metropolitan Police Agency.

He graduated from law school at the Korean National Police University. In 1989, he received a master's degree in the Department of Forensic Science from Kyungpook National University In 2008. His interests include cybersecurity, cyber investigation, digital forensics, and national cyber policy.