Journal of Multimedia Information System VOL. 6, NO. 3, September 2019 (pp.139-146): ISSN 2383-7632(Online)
http://dx.doi.org/10.33851/JMIS.2019.6.3.139

Apply Blockchain to Overcome Wi-Fi Vulnerabilities

Seong-Kyu (Steve) Kim[1,*]

Abstract

This paper, wireless internet such as Wi-Fi has a vulnerability to security. Blockchain also means a 'Ledger' in which transaction information that occurs on a public or private network is encrypted and shared among the network participants. Blockchain maintains information integrity by making it impossible for a particular node to tamper with information arbitrarily, a feature that would result in changes in the overall blockchain hash value if any one transaction information that constitutes a block was changed. The complete sharing of information through a peer-to-peer network will also cripple hacking attempts from outside, targeting specialized nodes, and prepare for the "single point of failure" risk of the entire system being shut down. Due to the value of these Blockchain, various types of Blockchain are emerging, and related technology development efforts are also actively underway. Various business models such as public block chains such as Bitcoin, as well as private block chains that allow only certain authorized nodes to participate, or consortium block chains operated by a select few licensed groups, are being utilized. In terms of technological evolution, Blockchain also shows the potential to grow beyond cryptocurrency into an online platform that allows all kinds of transactions with the advent of 'Smart Contract'. By using Blockchain technology, the company makes suggestions to overcome the vulnerability of wireless Internet.

Key Words: Blockchain, Big-data, Artificial Intelligence, Smart Contract, Wi-Fi.

I. INTRODUCTION

Public free Wi-Fi is now available in many places. The airport, hotels and cafes all offer free Internet access as an additional benefit of using the service. It's really good for many people to have free access to the Internet. In particular, office workers who frequent business trips or work outside of the country can send e-mails via free Wi-Fi or share documents online. However, contrary to the opinion of most Internet users, using public Wi-Fi is quite dangerous, and most of the wireless Internet's also associated with people trying to make mid-term attacks Middleman Man refers to the communication with the Middle of malice [1-3]. There are two, in, and various types of intermediary attacks that people intercept between groups, but the most common method is to intercept a user's request to access a website and send a response to a fraudulent webpage that appears to be legitimate. For example, a hacker who intercepts her communications to an email that Alice is about to access may use a private conversation to trick users into entering important data into a fake website, since there are many cases where her hacker receives Alice's information and login, such as phishing a contact email to a list of more malicious acts, such as sending her password to a list of the Wi-Fi. This wireless Wi-Fi system has many vulnerabilities. Therefore, this paper proposes blockchain-based Wi-Fi service for safe and fast communication using blockchain technique.

II. Related Research

This paper deals with the weak points in Wi-Fi's wireless communication and the improvements in blockchain and various problems. Also, the concept and characteristics of blockchain are reviewed to deal with the direction of overcoming vulnerabilities in the use of open blockchain and certain blockchain services in order. Also, the Wi-Fi system, blockchain system, and blockchain application methods are studied in advance [4-6].

2.1. Wi-Fi

Wi-Fi is a technology that allows electronic devices to connect to a wireless LAN (WLAN), mainly using the 2.4 gigahertz (12-centimeter) UHF and 5 gigahertz (6-centimeter) SHF ISM radio bands. Although wireless LANs are generally password protected, they are also open to any device located within the band to access the resources of the wireless LAN network. Wi-Fi Alliance

Manuscript received September 16, 2019; Revised September 25, 2019; Accepted September 29, 2019. (ID No. JMIS-19M-09-029)
Corresponding Author (*): Seong-Kyu (Steve) Kim, GOB Universal PTE., LTD, Singapore, guitara77@gmail.com.
[1]CEO/Ph.D of GOB Universal PTE., LTD, Singapore.

defines Wi-Fi as any "WLAN" product based on the Electronic Engineers Association (IEEE) 802.11 standards.Wi-Fi is one of the trademarks of Wi-Fi Alliance [7-9].

The Wi-Fi Certified trademark is only available for Wi-Fi products that are fully qualified for Wi-Fi Alliance interoperability certification tests. Devices using Wi-Fi technology include personal computers, video game consoles, smartphones, digital cameras, tablet computers, digital audio players and modern printers. Wi-Fi-compatible devices can access the Internet through WLAN networks and wireless access points. These access points (hotspots) have a band of approximately 20 meters (66 feet) indoors and larger outdoors. The hotspot support range can be supported only by small rooms with walls that block radio waves, and can be extended to several square kilometers by overlapping access points.

Wi-Fi is less secure than wired connections such as Ethernet because intruders do not need to make physical connections. Web pages using TLS are secure, but unencrypted Internet access can be easily found by intruders. For this reason, Wi-Fi is adopting a variety of encryption technologies. The initial encryption WEP could be easily penetrated. Higher quality protocols (WPA, WPA2) were later added. The optional feature added in 2007 - Wi-Fi protection setup (WPS) - had serious flaws that enabled an attacker to identify the router's password. Since then, Wi-Fi Alliance has updated its test plan and certification programs to ensure that newly certified devices can resist attacks [10-14].

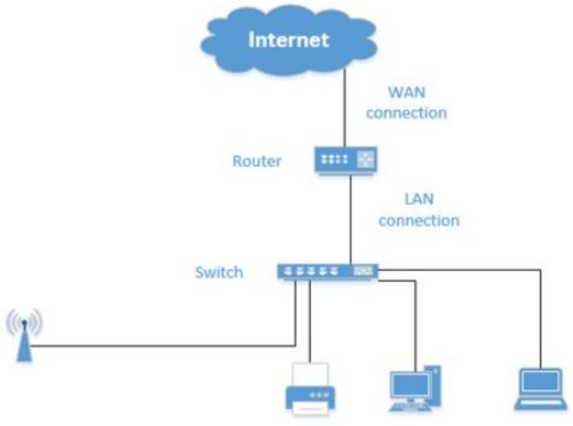

Fig. 1. Architecture for Wi-Fi.

2.2. Blockchain

Blockchain is a technology that ensures integrity and reliability without authorized third parties by jointly verifying, recording, and storing transaction information by all participants in the network. Based on Distributed Ledger technology, it features a ledger that holds all transactional information that occurs in peer-to-peer networks (P2P) networks, all nodes store and update, and maintain the integrity of the data. Because of this, Goldman Sachs also defines blockchain as a "shared and distributed transaction database designed to increase transparency, security and efficiency of transactions." Although the definition of blockchain varies slightly from institution to institution, most of the features have something in common. In other words, it has something in common in that it enabled the implementation of various application services based on a distributed network infrastructure utilizing security technologies such as hash, electronic signature and encryption. In addition, blocks stored on each node include information from the previous block (hash values), current transaction information, and hash values, which are difficult to manipulate and enable transparent management of transaction information [15-19]. It presents characteristics (center) of blockchain technology at the PWC and what can be improved by doing so (correcting the problems on the left as shown on the right). Based on encryption, blockchain can "see the scope of its services that are programmable (or programmable) such as Smart Contracts while aiming (or supporting) for Immutable, Transparent, Distant, and Consensus." Due to the possibility that it can be "expanded," there are expectations for various industrial applications. Looking at this around tasks that are being applied with blockchain, one can see more clear characteristics. In another report, McKinsey identified blockchain utilization as "Record Keeping" and "Transaction." Record keeping is also based on the integrity of the blockchain. As a static storage area, information such as reference day sites (real estate registration, patents) or identity information (citizenship, voting rights) and smart contracts are recorded. While smart-system drugs may contain a variety of content, once defined contracts do not change frequently. On the other hand, transaction related data are viewed [11]. If record keeping focuses on safe storage, the transaction is considered relatively dynamic and a registry for managing the change. This addresses the ongoing updates to the books, such as asset exchanges and payments. Blockchain-based payment services such as bitcoin are available because the blocks that are created are still connected and traceable to the transaction details. Therefore, this application may also be used to assist in activities such as improving the status of changes in ownership or visibility of the supply chain. summarizes major blockchain services by industry/task based on two basic functions presented by McKinsey [20-22].

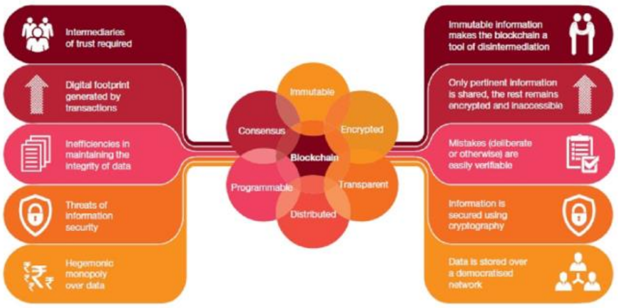
Intermediaries of trust required
Digital footprint generated by transactions
Inefficiencies in maintaining the integrity of data
Threats of information security
Hegemonic monopoly over data
Immutable
Consensus
Encrypted
Blockchain
Programmable
Transparent
Distributed
Immutable information makes the blockchain a tool of disintermediation
Only pertinent information is shared, the rest remains encrypted and inaccessible
Mistakes (deliberate or otherwise) are easily verifiable
Information is secured using cryptography
Data is stored over a democratised network

Fig. 2. Advantage of Blockchain.

2.3. Blockchain Application

The Harvard Business Review suggested that blockchain has the potential to create a new foundation for economic and social institutions as a Foundational technology, just like TCP/IP did in the past. The underlying technology needs a little more time before it has a clear effect, but its ripple effect is relatively large. The most devastating advantage that blockchain can provide is that it can replace the role of existing third-party trust organizations through the formation of technology-based trust. This requires not only blockchain technology, but also overall changes from the role of business ecosystem members and the way they work. It can be expected that it will be a base technology that supports digital switching society along with issues such as spreading IoT and digitizing assets, growth of big data industries that are linked to personal identification rights and GDPR, cloud-based SW services, and AI [23-25]. Therefore, more time may be needed for the visible effect. In a report released in 2015, the WEF saw the full-fledged ignition point of blockchain Surveyor (Tippoint) as the time when the value of 10 percent of global GDP was stored on blockchain platforms. Based on the timing of the report's announcement, the report is expected to be around 2025, about 10 years later. As to when blockchain will be activated, Gartner offers a similar opinion. Blockchain is passing through a "Through of Disposal" for technology, which means that time and support are needed for large-scale spread and commercial success cases [12]. Together, the Katner Heif cycle and Geoffrey Moore's Kasms curve confirm that it is time for the blockchain to reduce the gap to enter the mainstream market. And that period is viewed by most agencies as around the next five to 10 years. In times when excessive expectations about technology are removed, however, early products are known to fail, leading to a sudden drop in market interest or a shift away from public attention. Deloitte also announced at Githeub (github.com) that only about 6 percent of the 86,000 blockchain projects under way could last. Therefore, a business model that can bring about gradual changes is also needed to minimize the space of the casserole and quickly access the liquor market. This can lead to a process of securing a variety of use cases and embedding technologies that can be applied in real business environments. Through such a technology re-lighting system, the system continues to stabilize, and if the entire blockchain ecosystem-scale economy is achieved, innovative services can also develop to the level of commercialization. Blockchain is not merely an improvement in the process, but it is considered to be a disruptive technology as soon as its potential is maximized. To this end, the market should be created along with innovative services and gradual models. In fact, blockchain is an infrastructure technology that is used to improve business processes through a sustainable business model, along with a disruptive business model. If disruptive and innovative changes can give startups new opportunities, gradual process improvements can help existing firms continue their competitive advantage.

MIT Sloan School has presented a business model that utilizes blockchain in the media industry with a disruptive form, as well as a sustainable model. A disruptive model is a service model that can pose a potential threat to existing businesses. The first may take the form of a "Stemit" that "provides revenue to both creators and managers." Stimit's creator can be rewarded for writing in itself, and curators who work on sites and make recommendations for good articles will also be rewarded. If existing blogging services relied on advertising revenue from power bloggers, they could be differentiated in that they could focus more on the content itself. The second form of a disruptive model, "One-Stop Content Shop," can also be seen as a business model that can change the distribution process of existing digital content. Wojo Music (https://ujomusic.com) is an example of an artist's goal of securing profitability. For songwriters or performers, the profit ratio can be adjusted through smart contracts and the profit structure can be improved by selling songs directly to end consumers. If the disruptive model could have been an opportunity for new companies to grow, the "Sustaining" model can be used to strengthen the competitiveness of existing companies or target niche markets. The first example is to improve the content distribution process and provide revenue through copyright with the aim of "protecting IP" the creator. Kodak once introduced a service called Kodak One based on blockchain. Here, it tracks the use of images registered with AI-based Web crawling and image recognition technology and protects the rights of photographers to return copyright fees by detecting illegal use. Kodak announced that it has made $1 million worth of revenue from revenue from copyright rates since 2018. The second "digitalization of the value chain" is aimed at optimizing the value chain to proceed the revenue distribution process more quickly and accurately. This model is similar to Uzzo Music, but it can be seen as a model that is being offered to participants in the value chain of the existing music industry. Sportipay said it will take over blockchain technology firm Media Chain Lab in 2017 and introduce blockchain in resolving issues such as copyright management and royalty payments. The third is a case in which ownership of a particular game item in the form of "transaction of game assets" can be utilized without being limited to that game. By doing so, it can improve the utilization of digital assets through cryptocurrency such as Kryptonite and Game item transactions.

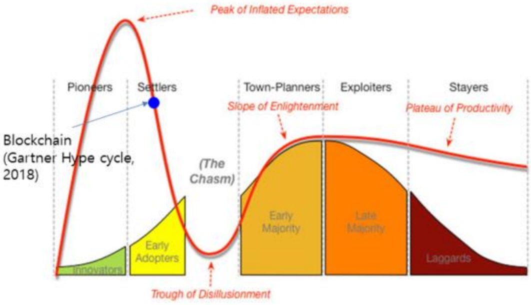

Fig. 3. Tetradian Consulting (Tom Graves Linkedin page).

III. A Security Model Based on Blockchain-Based Wi-Fi

Given that blockchain is an important value in enabling inter-participant transactions without the need for intermediaries or trusted third-party trust parties, one of the key aspects of the blockchain-based business model is, after all, technological substitution of the role of intermediary pipe. Therefore, a two-sided, market-driven platform business that connects two types of user groups, such as suppliers and consumers, is one pillar. The key to the two-sided market is to first grow the size of one of the two types and thus create a virtuous circle structure in which the other group grows the size. Stimit or Uzzo Music in the disruptive enemy model we discussed earlier can be seen as a business that should take particular account of the characteristics of these platform businesses. It is essential to present new markets or values and elaborate implementation of a reward system called token to the group of participants. In addition, considering a fully distributed format, the substantial coordination cost to implement and maintain a system of agreement among p2p participants should also be considered. At the same time, there is the difficulty of presenting better value than similar platform service models based on the existing Internet economy. In fact, public blockchain-based services offer the ideal business, but they are still making various attempts at the level of white paper or proof of concept (PoC). However, we want to use these Wi-Fi wireless Internet vulnerabilities to apply them to the security model [13].

In addition, in order to lead a sustainable business, an accurate analysis of the problem (Pain Point) and a value proposition must be made. Companies such as IBM and PWC are proposing methodologies to identify problems. To limit the area or task to which blockchain technology will be applied, conduct workshops to identify the business flow and key participants to identify the problems that customers are currently facing. In addition, a similar use case with each industry customer presents a specific approach that includes the ideas and application priorities that can be used for the project. Subsequently, prototype (or PoC) is carried out around the selected priority tasks to verify blockchain technology within 2-3 months. Until now, problems and value propositions based on systematic methodologies must be presented properly to proceed to the actual stage of deployment. Successful blockchain projects require the participation of experts with knowledge of the industry or task, as well as technology. Therefore, the focus should be on securing various 'build' cases through pilot projects, as well as the development of systematic 'procedures' and 'processes' that derive these business process problems and apply methodologies. In addition, a variety of attack methods based on the wireless Internet are emerging and this is to be overcome by blockchaining [14].

3.1. Wi-Fi Eavesdropping

Wi-Fi eavesdropping is a type of intermediate-person attack in which hackers use public Wi-Fi to monitor the activities of connected people. Interception information ranges from personal information to Internet traffic and search patterns.

Generally, eavesdropping begins by creating a fake Wi-Fi network with a legally-appearing name. Fake hotspots are often very similar to the names of nearby stores and companies. It is also known as Evil Twin. For example, when a consumer enters a cafe, they see three Wi-Fi with a similar name. Café, Cafe 1 and Cafe 2 One of the three Wi-Fi options is likely to be the con artist's Wi-Fi. Hackers can use the technology to collect data from any device that establishes an Internet connection, eventually stealing login credentials, credit card information and other important data. Wifi eavesdropping is just one of the risks associated with public networks, so we recommend you not use it. If you really need to use a public Wi-Fi, make sure you check with the staff to see if it's real and safe.

3.2. Packet Sniffing

Sometimes criminals use certain computer programs to steal data. These programs are known as packet sniffer, and are often used by legitimate IT professionals to record digital network traffic, making it easier to detect and analyze problems. However, many of these packet analysts are abused by cybercriminals who want to collect sensitive data and engage in illegal activities. Even if nothing bad happened at first, the victims would later notice that someone had committed identity fraud against them or that the company's confidential information had somehow been leaked.

3.3. Cookies Theft and Session Hijacking

In wireless Wi-Fi, cookies are small data packets that web browsers collect from websites as a way to keep some search information. These data packets are usually stored locally on the user's computer so that the website recognizes the user when he or she returns. Cookies are useful because they make it easy to communicate between users and the websites they visit. For example, cookies allow users to log in without entering their credentials whenever they visit a particular webpage. Online stores use cookies to record items customers have previously added to their shopping carts or to manage their search activities. Cookies are simple text files, so they won't harm your computer because keys or malware won't fit in. However, cookies are dangerous in terms of privacy and are often used for intermediate-term attacks.

If a malicious person can steal a cookie that he or she is using to communicate with you on the website, you can use that information against you. This is called cookie theft and is often associated with session hijacking. Successful session hijacking allows an attacker to disguise himself as a victim and communicate with the website instead. This means attackers can use the victim's current session to access personal e-mails or other websites that may contain sensitive data. Session hijacking generally occurs in public Wi-Fi hotspots because they are easy to monitor and much more vulnerable to intermediate-magnetic attacks.

3.4. Hijacking Method to prevent intermediate-level attack

- Turn off all settings that allow you to automatically connect to the Wi-Fi network available on your device
- Turn off file sharing and log out any unused accounts.
- Use a password-protected Wi-Fi network if possible. If a public Wi-Fi network is forced to be used, send important information or prevent access.
- The operating system and virus vaccine should be continuously updated.
- Avoid all economic activities, including cryptocurrency transactions, when using public networks.
- Use websites that utilize the HTTPS protocol. However, some hackers keep in mind that the move is not the perfect solution because of the spoofing of HTTPS.
- Virtual private networks (VPNs) are recommended if they are particularly important or require access to business-related data.
- Watch out for fake Wi-Fi networks. Don't trust Wi-Fi names because they are similar to store or company names. In case of doubt, ask the staff to verify the authenticity of the network. Or you can ask them if they can borrow a security network.
- Turn off Wi-Fi and Bluetooth when not in use. If you do not really need a public network, do not connect to a public network.

IV. CONCLUSION

There are many security vulnerabilities in the Wi-Fi wireless Internet. However, efforts have been made to apply them to industries around public and private block chains. In addition, the governance system, which extends its influence in the industry group through global consortiums, etc., is rapidly advancing. The reason why private blockchain projects are progressing faster than public blockchain is because of the regulatory aspects of cryptocurrency, but it is starting to address clear problems with ROI in mind. The participation of market leaders and big businesses is accelerating even more, despite concerns by Boston Consulting or McKinsey that the scale has yet to show results. It also confirmed that blockchain-based services do not necessarily have to be a disruptive business model and that existing leading companies may be used to further consolidate entry barriers. In addition, in the blockchain business model, business governance is supported by technology/platforms, and the areas and methods of business consortium can be expanded in a variety of ways, which can further accelerate competition across industries and borders. To ensure successful implementation of the blockchain project, consider from establishing an implementation strategy to future scalability (Scale). To that end, each project should also be interested in organizing "procedures" and "methodology" that identify and analyze problems along with "builds" such as PoC and Pilots. If systematic methodologies such as Information Strategy Planning (ISP) consulting are developed, applied, and shared in blockchain support projects, the ability of domestic demand and suppliers may also be supported. The Korean ecosystem related to blockchain needs to be competitive in technology and services before related markets reach tipping points. To this end, policies and efforts by the ecosystem will need to continue to expand the momentum gained through the "Blockchain Technology Development Strategy".

Cybercriminals are always looking for new ways to access people's data. Therefore, it is important to be careful and alert. Here we've covered some of the risks that public

Wi-Fi can present. While most of these risks can be mitigated by just using password-protected security connections, it is important to understand how these attacks work and how to prevent them from becoming the next victim. Therefore, Wi-Fi wireless Internet has many vulnerabilities. So this paper proposes on a blockchain basis.

References

[1] Nakamoto S., “Bitcoin: a peer-to-peer electronic cash system,” pp 1-9, 2008.

[2] J-H Huh and K Seo, “Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing,” The Journal of Supercomputing, Springer, pp.1-17, 2018.

[3] Y Nir Kshetri, “Blockchain’s roles in meeting key supply chain management objectives,” International Journal of Information Management, Elsevier, 80-82., 2018.

[4] Alexander Savelyev, “Copyright in the Blockchain era: Promises and challenges,” Computer Law & Security Review, Elsevier, 2018.

[5] J.H. H, Otgonchimeg S., and Seo K., “Advanced metering infrastructure design and test bed experiment using intelligent agents: focusing on the PLC network base technology for Smart Grid system,” The Journal of Supercomputing, 72(5), 1862-1877, 2018.

[6] Nir Kshetri, “Blockchain's roles in strengthening cybersecurity and protecting privacy,” Telecommunications Policy, pp 20-23, 2017.

[7] S-K Kim, U-M Kim, J-H Huh, “A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security,” Energies, MDPI, Vol.12, No.3, pp.1-29, 2019.

[8] J-H Huh and K Seo, “A Typeface Searching Technique Using Evaluation Functions for Shapes and Positions of Alphabets Used in Ancient Books for Image Searching,” International Journal of Hybrid Information Technology, SERSC, Vol.9, No.9, pp. 283-292, 2016.

[9] Richard B. Levin, Peter Waltz, and Holly LaCount, “Betting Blockchain Will Change Everything – SEC and CFTC Regulation of Blockchain Technology, Handbook of Blockchain,” Digital Finance, and Inclusion, Elsevier, Vol. 2, 187-212, 2017.

[10] J-H Huh, “Server Operation and Virtualization to Save Energy and Cost in Future Sustainable Computing,” Sustainability, MDPI, Vol.10, No.6, pp.1-20, 2018.

[11] Christoph Prybila, Stefan Schulte, Christoph Hochreiner, and Ingo Webe, “Runtime verification for business processes utilizing the Bitcoin Blockchain,” Future Generation Computer Systems, Elsevier, 2017.

[12] S-K Kim and J-H Huh, “A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective,” Energies, MDPI, Vol.11, No.7, pp.1-22, 2018.

[13] Yan Chen, “Blockchain tokens and the potential democratization of entrepreneurship and innovation,” SSRN, pp.12-13, 2017.

[14] Bogner, A., Chanson, M., & Meeuw, A., “A decentralised sharing app running a smart contract on the ethereum blockchain,” In Proceedings of the 6th International Conference on the Internet of Things, pp. 177-178. ACM, 2016.

[15] Casino, F., Dasaklis, T. K., & Patsakis, C., “A systematic literature review of blockchain-based applications: current status, classification and open issues.” Elsevier, Telematics and Informatics, 2018.

[16] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V., “To blockchain or not to blockchain: That is the question,” IT Professional, 20(2), 62-74, 2018.

[17] Guo, Y., & Liang, C., “Blockchain application and outlook in the banking industry,” Financial Innovation, 2(1), 24, 2016.

[18] J. H Huh, Koh, T, Seo, K., “Design of a shipboard outside communication network and the test bed using PLC: for the Workers' safety management during ship-building process,” In Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication (p. 1-6). ACM, 2016.

[19] Herian, R., “Regulating disruption: Blockchain, Gdpr, and questions of data sovereignty,” Journal of Internet Law, 22(2), 1, 2018.

[20] Andoni, M., et al., “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” Renewable and Sustainable Energy Reviews, Elsevier, 100, 143-174 2019.

[21] J.H Huh., T Koh., and K Seo, “NMEA2000 ship area network design and test bed experiment using power line communication with the 3-phase 3-line delta connection method,” International Journal of Applied Engineering Research, Research India Publications, 10(11), 27789-27797, 2015.

[22] Schwerin, S., “Blockchain and privacy protection in the case of the european general data protection regulation (GDPR): a delphi study,” The Journal of the British Blockchain Association, 1(1), 3554, 2018.

[23] J-H Huh and K Seo, “RUDP design and implementation using OPNET simulation,” Computer science and its applications. Springer, 913-919, 2015.

[24] J. Park et al., “Design of the real-time mobile push system for implementation of the shipboard smart working,” In Advances in Computer Science and

Ubiquitous Computing, Springer, 541-548, 2015.

[25] Fabiano, N., "The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard," In 2017 IEEE International Conference on Internet of Things for the Global Community (IoTGC), pp. 1-7, 2017.

Author

Seong-Kyu (Steve) Kim has born in Seoul, Republic of Korea. In Feb. 2006, he graduated from Sungkyunkwan University at Seoul, Department of Information Communication Engineering in Korea and received his master degree. In August 2019, he graduated (Ph. D) from Sungkyunkwan University at Suwon, Department of Electronic and Electrical Computer Engineering. He started his career as a ICT in 1999, and he was before worked Hyundai Information Technology,

He has worked on Hyundai Motor IT R & D Research, Hyundai Construction IT R & D Research, Korea Railroad IT Project, Korea Highway Corporation IT Project, and Ministry of Public Administration and Security IT Project.

He worked at Samsung during 1999 ~ 2017. He was responsible for Saudi Aramco security (physical and information protection) projects, Kuwait KNPC security (physical and information protection) projects, and Singapore Changi Airport security (physical and information protection) projects.

He also lectured on "Introduction to Public Computers" at Songdam University, Yongin. (2010 ~ 2011). Lectured "Security System" at Sungkyunkwan University Graduate School of Information and Communication (2015)

CISA, PMP, CISSP, and CPPG lectures were conducted at Wise Road, an accredited Ministry of Employment and Labor (2010-2016). Computer Engineering Lecture at the Hackers Lab, an accredited Ministry of Employment and Labor (2016), Lectured on industrial security management at "Olwin Edu" educational institution certified by Ministry of Employment and Labor (2010 ~ 2016). In addition, he received the Best Paper Award at the Korea Multimedia Society (MITA) in 2019.

He has international certifications such as CISA (Certified Information Systems Auditor), CISSP (Certified Information Systems Security Professional), PMP(Project Management Professiona), ITIL Foundation, CCNP, SCJP, ISE, CPPG, ISO 27001, ISO 20000, ISO 9000, ISO 22301 has etc..

Currently he is CEO of "Geoblue Lab" Republic of Korea and "GOB Universal PTE,. LTD" in Singapore. His research interests are Blockchain, AI, Big Data, Smart Grid, Network Security, IoT, App, System Architecture.