symmetry

MDPI

Article

Preemptive Prediction-Based Automated Cyberattack Framework Modeling

Sungwook Ryu [1], Jinsu Kim [2], Namje Park [3,*] and Yongseok Seo [4]

[1] Master's Program in Future Strategy, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea; ryu76@kaist.ac.kr
[2] Department of Convergence Information Security, Graduate School, Jeju National University, Jeju 63293, Korea; kimjinsu@jejunu.ac.kr
[3] Department of Computer Education, Teachar's College, Jeju National University, Jeju 63293, Korea
[4] Department of Future Strategy, Graduate School, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea; manoa@kaist.ac.kr
* Correspondence: namjepark@jejunu.ac.kr

Abstract: As the development of technology accelerates, the Fourth Industrial Revolution, which combines various technologies and provides them as one service, has been in the spotlight, and services using big data, Artificial Intelligence (AI) and Internet of Things (IoT) are becoming more intelligent and helpful to users. As these services are used in various fields, attacks by attackers also occur in various areas and ways. However, cyberattacks by attackers may vary depending on the attacking pattern of the attacker, and the same vulnerability can be attacked from different perspectives. Therefore, in this study, by constructing a cyberattack framework based on preemptive prediction, we can collect vulnerability information based on big data existing on the network and increase the accuracy by applying machine learning to the mapping of keywords frequently mentioned in attack strategies. We propose an attack strategy prediction framework.

Keywords: attack strategy framework; attack strategy prediction; system attack; artificial intelligence

Citation: Ryu, S.; Kim, J.; Park, N.; Seo, Y. Preemptive Prediction-Based Automated Cyberattack Framework Modeling. *Symmetry* **2021**, *13*, 793. https://doi.org/10.3390/sym13050793

Academic Editor: Nikos Mastorakis

Received: 4 April 2021
Accepted: 29 April 2021
Published: 3 May 2021

1. Introduction

In modern society, where the development of technology accelerates, the Fourth Industrial Revolution combines a number of technologies, each of which has been an independent technology. In particular, as the use of technologies changes, techniques and methods to attack systems become varying and more intelligent. Most attack techniques are to access a system, leak data from the system or make it malfunction [1–3].

In particular, as the range of attacks expands, the scope of attack may broaden and ways of attacking become varying. This problem can be prevented for known signature-based attacks, while it is difficult to effectively prevent unknown attacks. In consideration of this system vulnerability, CHESS (Computers and Humans Exploring Software Security) was developed, and various attack inference processes are studied, such as Cyber Kill Chain, analyzing cyberattacks on a process and mitigating the attacker's activities in each stage of an attack [4–6].

This research analyzed structured data such as papers, patents and reports and non-structured data, including images, videos and audio, and also analyzed and learned processed data to combine attack scenarios on system vulnerabilities, thereby preemptively predicting cyberattacks and proposing a framework to provide administrators with vulnerabilities and attack strategies.

2. Related Research

2.1. Science of Security (SoS)

SoS, a short form of Science of Security, is a study in which hypotheses are established based on universal truths and principles that can be found from physical security, man-

agerial security and information security, terms are defined based on the results from the verification process, and a systematical knowledge is established [7].

In general, scientific research methods assume that basically no theories are perfect. Therefore, researchers establish hypotheses and infer based on the hypothesis and predict and verify using the inference. Based on the verification, new hypotheses are established. Through this repetitive structure, new theories are derived.

When applying the aforementioned scientific approach and verification procedure to security, the assumption that all security policies are not complete is established, and the assumption becomes a start point. After that, new security policies are designed based on which a security system is established and verified. If a new attack occurs in the verification stage, a new security design shall be conducted, and this procedure is repeated to improve security technology [8]. Figure 1 illustrates the concept of SoS.

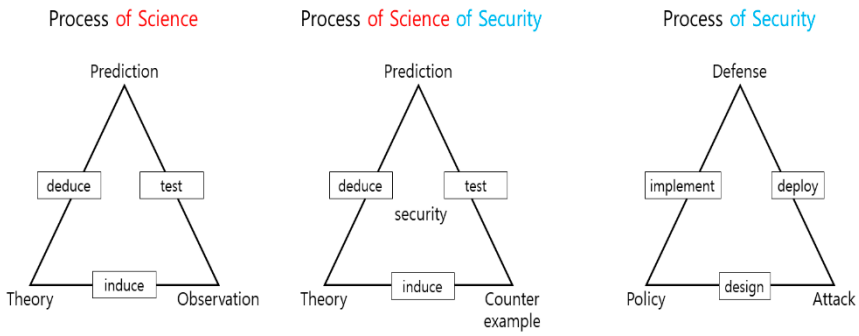

Figure 1. Comparison between the scientific approach and SoS.

The SoS-based research method is supported by the US National Security Agency (NSA). SoS focuses on foundation research, which develops policies and approaches fundamental changes in cybersecurity rather than the practical approach conducted by the government and companies. SoS projects aim at organizing academic research groups for base studies, promoting scientific principles and forming and fostering SoS communities. The research scope has been also expanded with the application of scientific principles through cooperation among the academia, government and industry.

2.2. Breach and Attack Simulation (BAS)

BAS means simulating a multistage cyberattack scenario in an automated way. BAS models attack chains to which the actual attacker is estimated to apply for attack in the IT environment. The most significant difference from the existing simulators is that BAS is capable of automating and implementing the attack scenario that the user has selected and implementing attacks to vulnerabilities, in practice, based on the agent installed at the subject system [9–11].

Performance indicators of BAS may include the safety level (whether the attack impacts on the existing property or service), accuracy of the attack simulation results and time and performance required from product placement to implementation of the attack and result report. The key point of this approach is how many attack scenarios it can support, and it is an open platform in which experts' participation is assumed [12,13].

For cyberattacks, hackers implement a cyber kill chain comprised of reconnaissance, weaponization, delivery, exploitation, installation, C&C (command and control) and actions on objectives. Before implementing attacks, one plans an attack scenario expressly or implied to use various attack techniques and methods, depending on one's abilities. As such, BAS establishes an attack scenario to simulate a cyberattack, and one of data used at that time is the ATT&CK framework provided by MITRE. The ATT&CK framework provides the knowledgebase in which information on attack techniques actually used is divided into PRE-ATTACK, Enterprise and Mobile by objective and sector, and each

sector offers attack tactics and skills used by attackers. Figure 2 is a conceptual diagram of BAS [14,15].

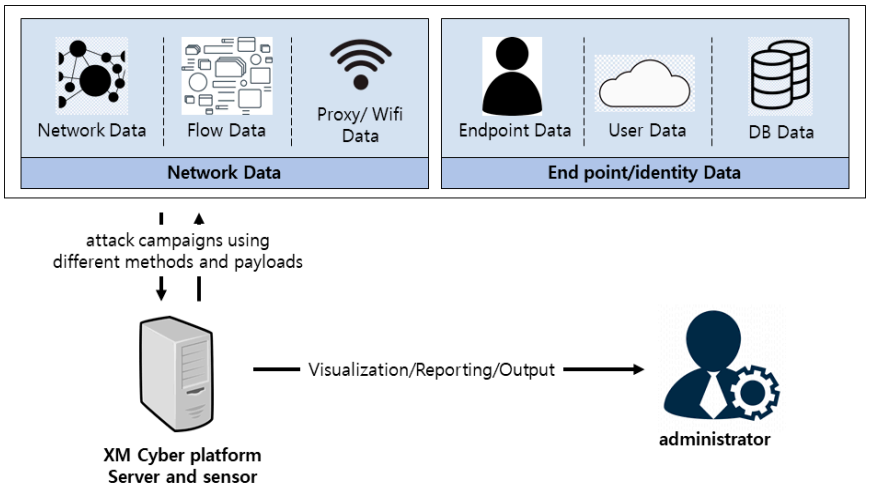

Figure 2. Breach and attack simulation conceptual diagram.

2.3. CHESS (Computers and Humans Exploring Software Security)

The CHESS project owned by the Defense Advanced Research Projects Agency (DARPA) aims to develop functions for finding and resolving all types of vulnerabilities in a scalable, timely and consistent manner. The objective of the CHESS project is to develop a computer-human system that can discover all kinds of vulnerabilities from complicated software. It focuses on identifying gaps of system information that requires the use by the system user, creating appropriate gap descriptions for the user and software patch synchronization [16,17].

Figure 3 shows technical classifications of CHESS. This project is largely divided into five areas from TA1 to TA5. TA1 focuses on capturing and discomposing all of program hacker workflows and other human–computer interactions (HCI). TA2 develops technology to discover and patch the vulnerabilities designated in the source code and binary. TA3 explains vulnerability classes and the function and scope of Common Weakness Enumeration (CWE). TA4 deals with TA3 assignments using the existing tools and technologies and provides standards to measure the improvement of CHESS. TA5 conducts evaluation and management of the government and commercial partners [18].

2.4. Cyber Kill Chain

In the cybersecurity area, the concept of Cyber Kill Chain was first used by Lockheed Martin Corporation, which has published white paper on the APT defense in 2009. It established the standards for identifying advanced attack activities and provided explanations on countermeasures using the existing infrastructure defense systems. Lockheed Martin called the concept Intrusion Kill Chain, which became a foundation of the company's infra protection. The white paper says, "When understanding the attacker's threat itself, intention, capabilities, principles, and operating patterns, by using Kill Chain, resilience of the organization can be secured even with traditional processes and systems with vulnerabilities." [19–21].

The strategic objective of Kill Chain is to identify attack components for responding to advanced attacks by attackers and establishing the organization's resilience while decreasing the probability of successful attacks by claiming legal liability on the attacker's ongoing activities [22].

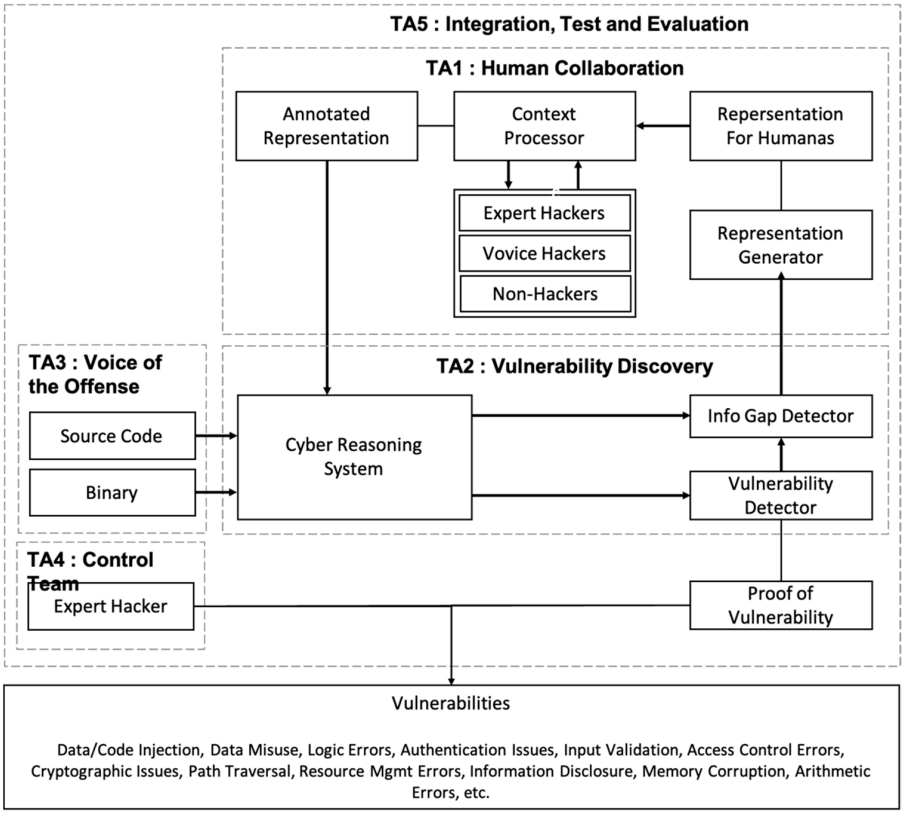

Figure 3. CHESS project's technical areas based concept diagram.

Common attack activities involve several stages, including reconnaissance, weaponization and delivery, exploitation and installation, command & control and exfiltration. Cyber Kill Chain is one of major models to analyze cyberattacks, and security companies prepare defense strategies in stages based on Kill Chain.

Figure 4 shows the concept of Cyber Kill Chain, including a description of each stage and defense strategies. However, security experts claim limitations in Cyber Kill Chain, and in fact, there are many problems that cannot be solved with Kill Chain alone. Moreover, it is vulnerable to an intruder's attack in that it assumes a firewall as a key defense means against an intruder in the existing external environment, so experts say that a strengthened defense is required for the internal of a firewall, and reconnaissance on the internal and effective recovery procedure on the weaponization stage are also required [23].

Reconnaissance	Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.
Weaponization	Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
Delivery	Intruder transmits weapon to target.
Exploitation	Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.
Installation	Malware weapon installs access point usable by intruder.
Command and Control	Malware enables intruder to have "hands on the keyboard" persistent access to target network.
Actions on Objective	Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.

Figure 4. Cyber Kill Chain defense strategies.

2.5. Analysis of Related Research Trend

Prediction of attacks minimizes damage to a system as the attack can be prevented, and a third party's intentional intrusion will be also prevented by blocking the attack in advance. Technology of predicting external attacks is researched on an ongoing basis and deep learning and machine learning based prediction is good examples.

Sagar said that the world spent approximately 44.5 billion dollars on the prevention of cyberattacks but heavily relies on threat intelligence related to Cyber Threat Intelligence (CTI), computer, network and information technology. He pointed that the existing CTI was corrective measure and emphasized the importance of preventive CTI by understanding the threats in hacker communities, suggesting a framework to detect advanced threats that can occur by hackers by collecting and analyzing a wide range of malignant hacker tools in the large-scale international hacker community through automated principal web, data and text mining [24].

Yong mentioned that the number of vulnerabilities discovered recently is sharply increasing, but those exploited were only a few. He emphasized a priority of vulnerabilities, suggesting an exploit prediction model named fastEmbed based on a combination of fastText and LightGBM algorisms. Compared to the existing text processing method, the model has improved the problem, by 6.283% on average, that the existing text processing method was not appropriate to identify relations between texts as it identified only static statistical characteristics [25].

Nektaria said that the development of AI led to a large number of innovations and spread of automated technologies, and under the circumstances, there were some cases that occurred where advanced attacks take place maliciously using AI. To solve this problem, he emphasized the need of security in a combination with AI, explored previous research on AI-based cyberattack, presented a cyber-threat framework using Cyber Kill Chain and introduced cases where the framework was applied [26].

3. Proposed Preemptive Prediction-Based Automated Cyberattack Framework

The preemptive prediction-based automated cyberattack framework proposed by this research aims to predict cyberattack methods depending on approaches to system vulnerabilities from the perspective of the attacker. Security mechanisms against common attacks consider the system administrator or the user and is oriented toward defense by analyzing system vulnerabilities rather than exploring the attacker's attack techniques. However, the attacker's intrusion into the system can be conducted from different perspectives of attackers according to their methodology. In order to predict intrusion from the attacker's viewpoint, this research collected attackers' strategic techniques through the analysis of open data (papers and patents), as well as closed data, created hacking scenarios using the collected techniques and provide the system administrator with a high probability among the created scenarios so as to ensure system integrity through security against the attack that can occur later. Figure 5 shows an overall conceptual diagram of the proposed framework.

The proposed preemptive prediction-based automated cyberattack framework consists of four modules. First is the structured/nonstructured data collection module that collects open structured data such as papers, reports and patents, as well as nonstructured data such as audio, image, video, social media, email and processes and refines the collected data to make it used as supportive materials for attack simulations. Second is the vulnerability-based knowledgebase module that collects information on attacks by third parties, including vulnerabilities, viruses and attack patterns and strategic techniques against attacks, and sorts out technologies that have occurred or may occur. The third is the attacker-oriented attack strategic simulation module, which analyzes the likelihood of a successful attack by attacking tools that can be used by attackers. Fourth is the attack prediction module that deduces the attack with information from the AI attack simulation and predicts the probability of attacks so as to prevent vulnerabilities through the attack

scenario. Figure 6 illustrates the methodologies applied to each stage of the proposed framework, based on its main modules.

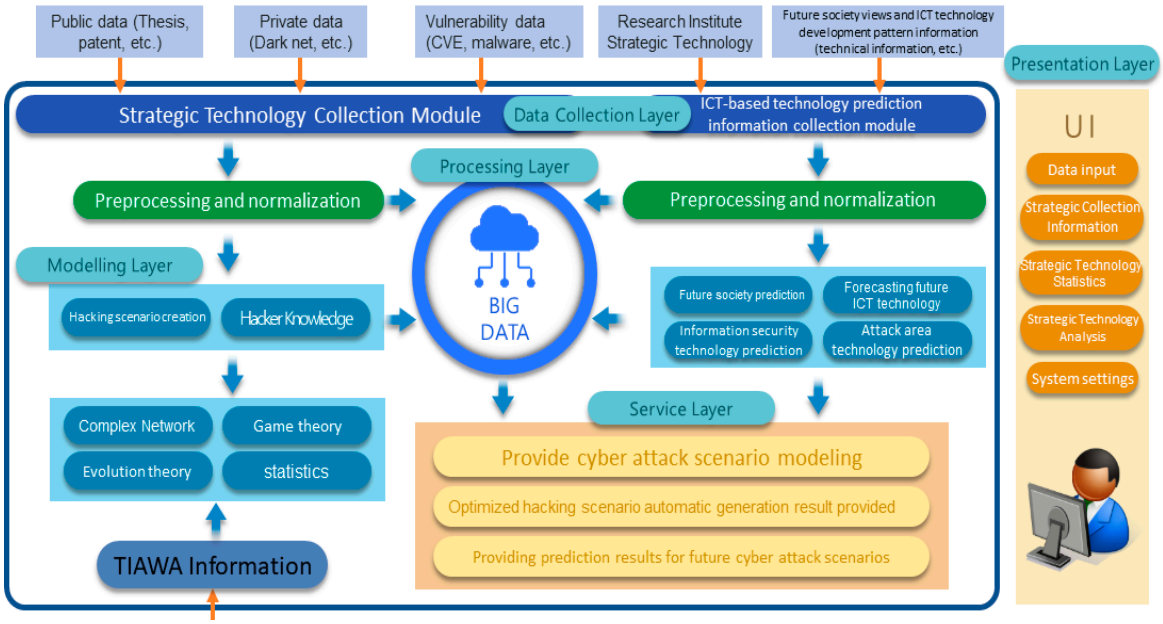

Figure 5. Conceptual diagram of the proposed preemptive prediction-based automated cyberattack framework.

Figure 7 shows the proposed framework based on Cyber Kill Chain.

Figure 8 shows the structure of the functional components of the proposed framework.

Figure 8 shows the overall flow of the proposed framework. Structured data such as papers, reports and patents, as well as nonstructured data, including social media, video, image and SNS (Social Networking Service), are collected with important keywords and materials, and then, they are converted into usable structured data by using TF-IDF, N-gram Exteaction and TextRank. This process is called a structured/nonstructured data collection module.

Keywords collected from various media and structured refer to vulnerabilities that can be attacked in the current system by using data in the vulnerability database that records associations between vulnerability information and keywords. These vulnerabilities are delivered to the attack prediction module through the vulnerability-based knowledgebase module. In this case, Naive Bayes Classifier is used for the vulnerability analysis based on the number of attacks occurring to the vulnerabilities with history, while SVM (Support Vector Machine) is used to analyze vulnerabilities that have yet to occur.

The attacker-oriented attack strategy simulation module uses attacking tools that can be used from the attacker's point of view and analyzes the probability of successful attacks with the attacking tool against the vulnerability by simulating the attacking tool in a virtual environment similar to the real environment.

The attack prediction module prioritizes the vulnerabilities collected through keywords according to the number of occurrences, forms several groups of attacks that can occur to vulnerabilities and predicts likelihood of attacks using history of occurrence.

Figure 9 shows a flow chart of the proposed framework.

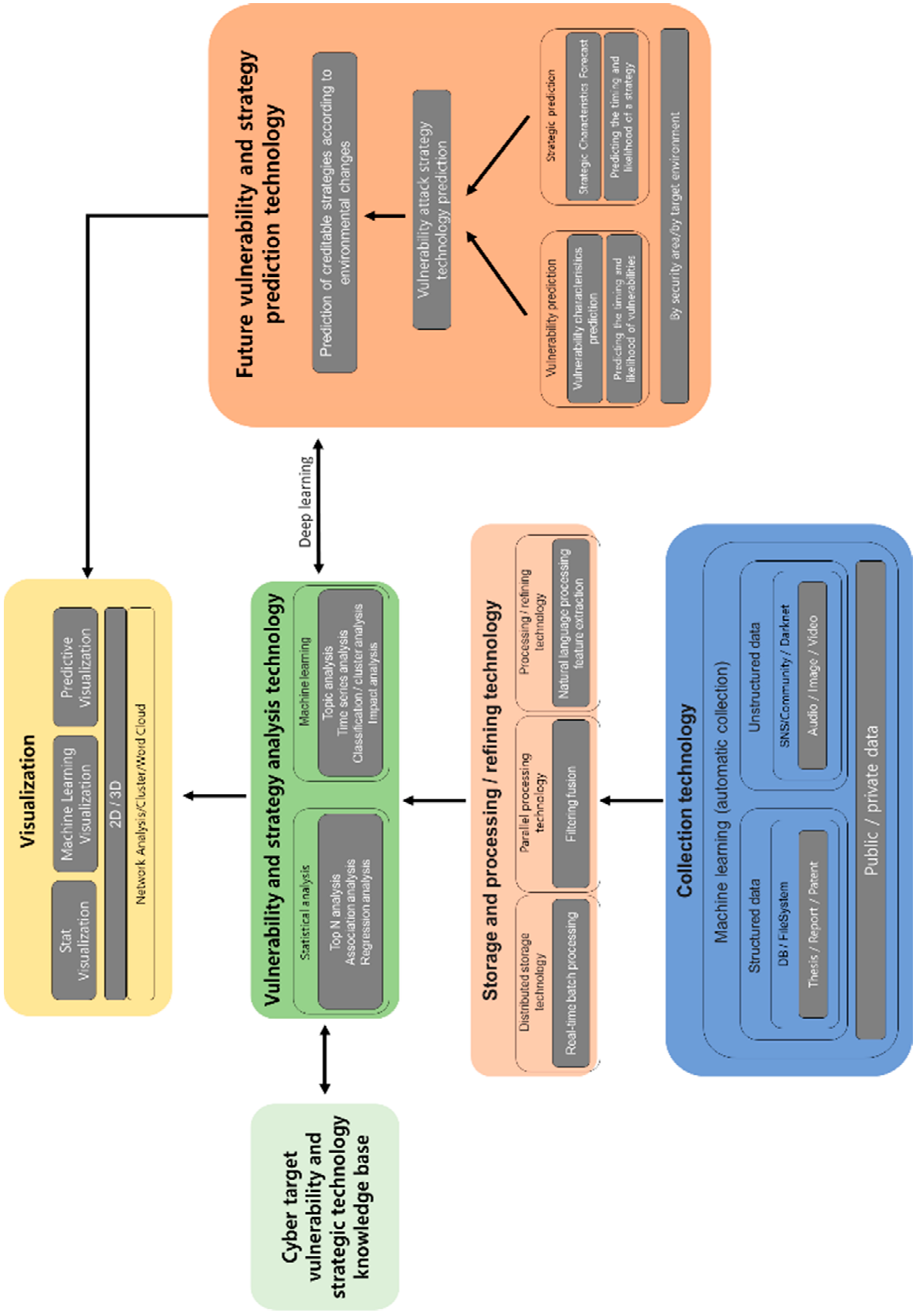

Figure 6. Proposed preemptive prediction-based automated cyberattack technology framework.

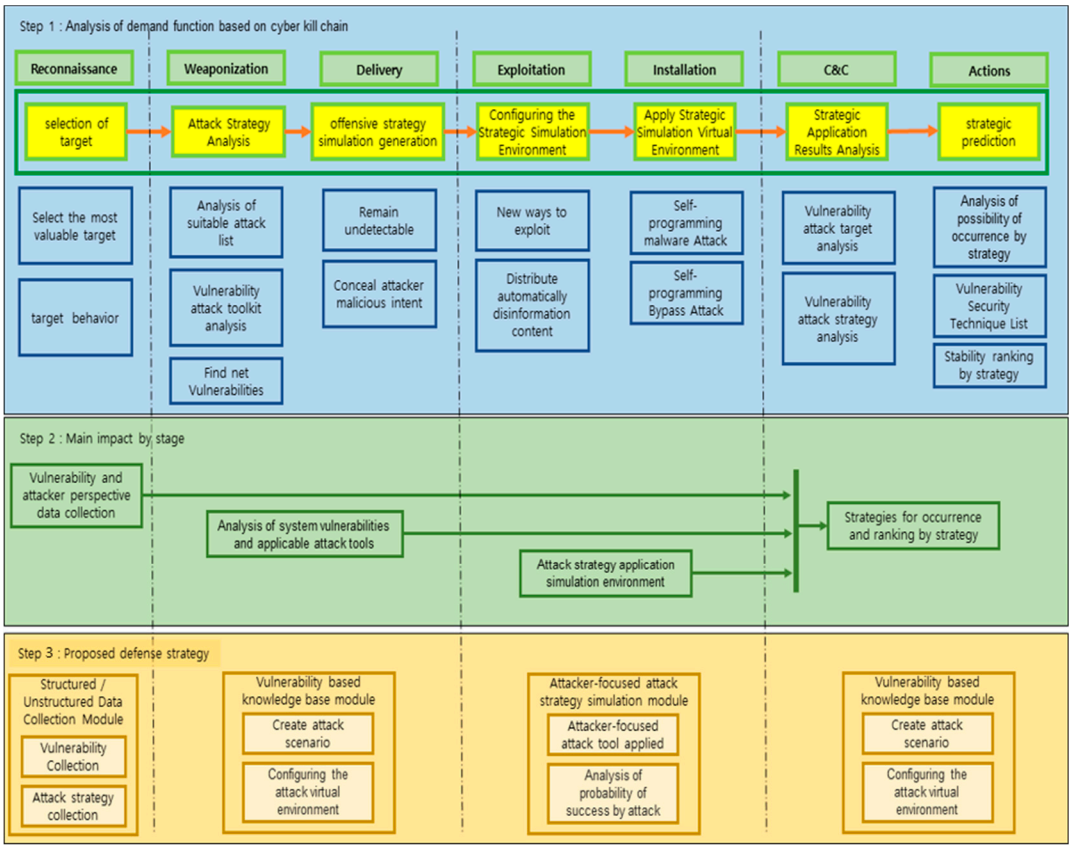

Figure 7. Steps of the proposed preemptive prediction-based automated cyberattack framework.

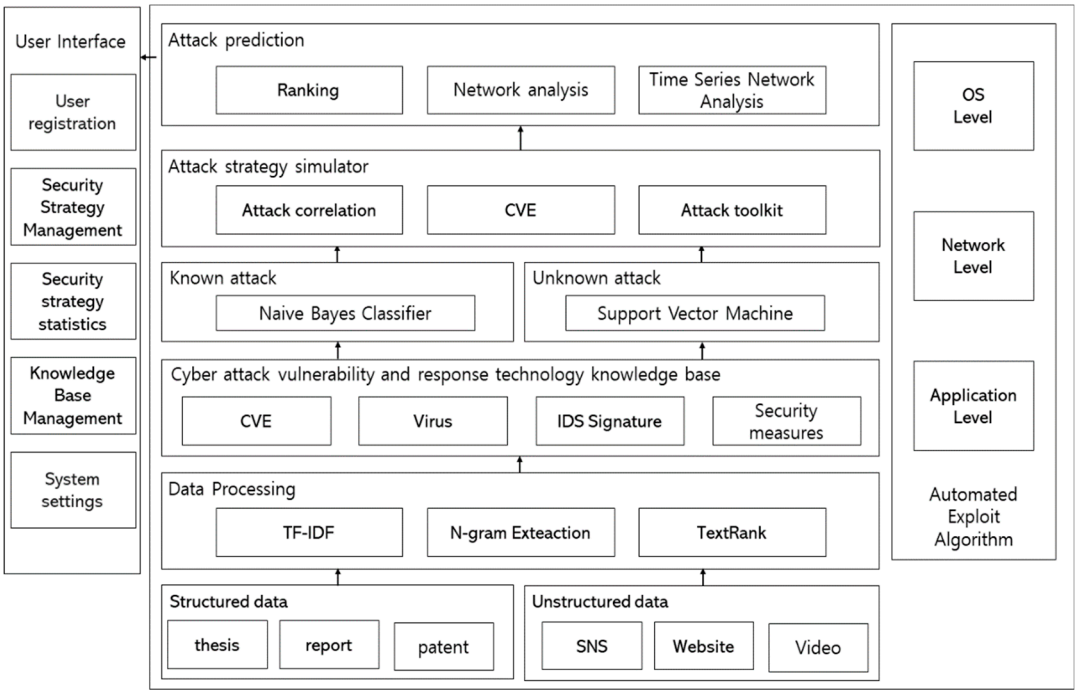

Figure 8. Structure of the functional components of the proposed preemptive prediction-based automated cyberattack framework.

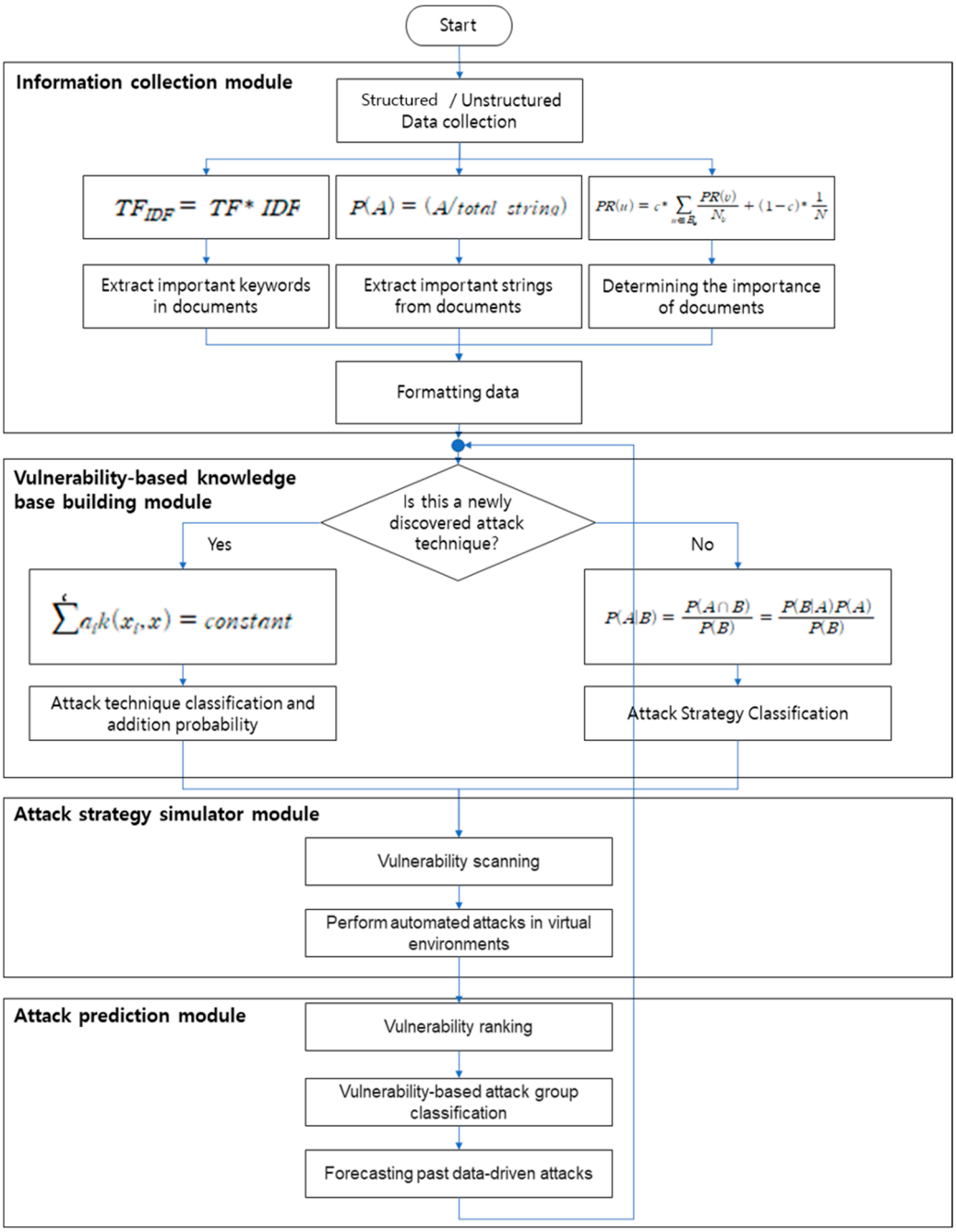

Figure 9. Flowchart of the proposed preemptive prediction-based framework.

3.1. Analysis of Security Requirements for Target System

This paper aims to present probabilities of attacks that can occur in the future through the collection and analysis of various structured/nonstructured data and learning of vulnerability information. Intentional attacks can take place in various layers, and the layers in which attacks occur, as well as security requirements for each layer, shall be analyzed so as to develop standards for responses to external attacks. The proposed framework analyzes the system security requirements to interpret vulnerabilities of the target system and creates attack scenarios.

In general, the Secure OS solution providing a security function requires to develop a security function of TCSEC (trusted computer system evaluation criteria) B1 Level that can protect systems from malicious attacks by blocking the illegal falsification and extortion of important files through the strict control of access in the level of operating system, as well

as obtaining of illegal root privileges, attacks against Daemon, hacking through system file falsification or an illegal execution file [27–30]. It can help in system development corresponding to the security function required by the TCSEC B1 Level, which is the US Department of Defense's evaluation criteria (multilevel security, mandatory access control, etc.). As Secure OS can remotely implement the security management of multiple servers, it is able to systematically conduct security management and block additional attacks following malicious intrusions by separating the web servers, web pages, application files and system files into different security areas [31–34]. Figure 10 shows TCSEC and its concept.

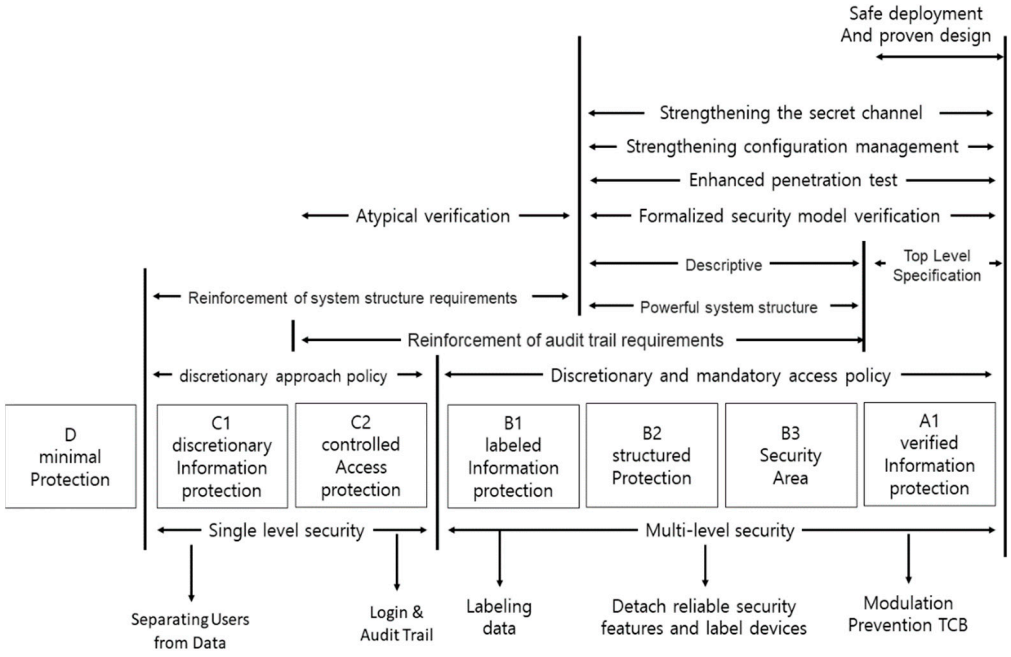

Figure 10. Trusted computer system evaluation criteria.

In general, Secure OS developed in compliance with TCSEC provides several characteristic functions that offer security that can be applied to the system. Table 1 lists the functions of Secure OS. The requirements for system security based on TCSEC B1 include user authentication, access control, authority management, confidentiality and integrity.

The security requirements for a target system are, roughly, user authentication, access control, authority management, confidentiality and integrity, and the details for each requirement are as follows:

If a subject to access the information object is not an authorized user, the system may be interfered with by the unauthorized user and substantially damaged. To prevent it, user authentication through electronic signature is required, and unauthorized access shall be notified to the administrator.

Access to the information object in the system can be managed according to system position of the user. An authorized user's access to the information object that is not permitted is unauthorized access, which requires access control by the security manager.

The roles and responsibilities of system administrators and system security managers shall be respectively allocated, and unauthorized access shall be prevented between each other.

Table 1. Secure OS security functions based on the TCSEC.

- User identification (user classification and authentication through electronic signature)
- Separation of authorities between the system administrator and the security manager
- Login management for authorized users
- Access control or denial of abnormal users
- Mandatory access control (MAC)
- ACL control (MLS & RBAC) of important information (file system, etc.)
- Mandatory control of user IP and use time, use-by date, use service, etc.
- System firewall (TCP/UDP/ICMP network In/Outbound control)
- Prevention of illegal forced closing of important service/process
- Self-Security Protection & setuid/setgid control, detection of active intrusion
- Detection of virus/worm's intrusion and blocking thereof (Host IPS)
- Automated blocking of attacks on obtaining system administrator authorities including BOF/Race Condition, etc.
- Automated blocking of unauthorized person and unauthorized work
- Automated notification via social media, email, console, etc. on illegal access
- User/group account management (create, delete, and manage: interworking same as OS)
- Audit log (detailed Real-Time Logging on accesses)
- System performance management (management of CPU/MEMORY, etc.)
- Tuning and security policy simulation to improve operating performance

In a system, an unauthorized user's access to information assets shall be prevented, which is not limited to users. By detecting and blocking not only unauthorized users to access the system but, also, abnormal work and malignant codes, the confidentiality of information assets shall be guaranteed.

The user's access to information assets shall be controlled according to the user's authority. The authorized user's unauthorized work can damage the integrity of the information assets, which indicates that the system integrity is not guaranteed. Table 2 shows the system security requirements.

Table 2. Analysis of the system security requirements.

Security Requirements	Description
User authentication	User classification and authentication through electronic signature Notification of illegal access to the administrator
Access control	ACL control of key information Mandatory access control according to sensitivity of resources in the system Mandatory control of user IP, available time, period, service
Authority management	Account management for authorized users Separation of roles and authorities between system administrators and security managers
Confidentiality	Detection and blocking of intrusion of malignant codes Blocking of unauthorized users and unauthorized works
Integrity	Blocking of attacks through the obtaining of the authority of a system administrator Prevention of unauthorized modification by an unauthorized user or work

3.2. Structured/Nonstructured Data Collection Module

The structured/nonstructured data collection module collects structured data with the database established, such as papers, reports and patents, as well as nonstructured data, which is prepared by individuals in an open network environment such as social media posts, audio, image, video and email. It filers the collected data and extracts key

texts. Figure 11 shows the data collected in the structured/nonstructured data collection module and applied techniques.

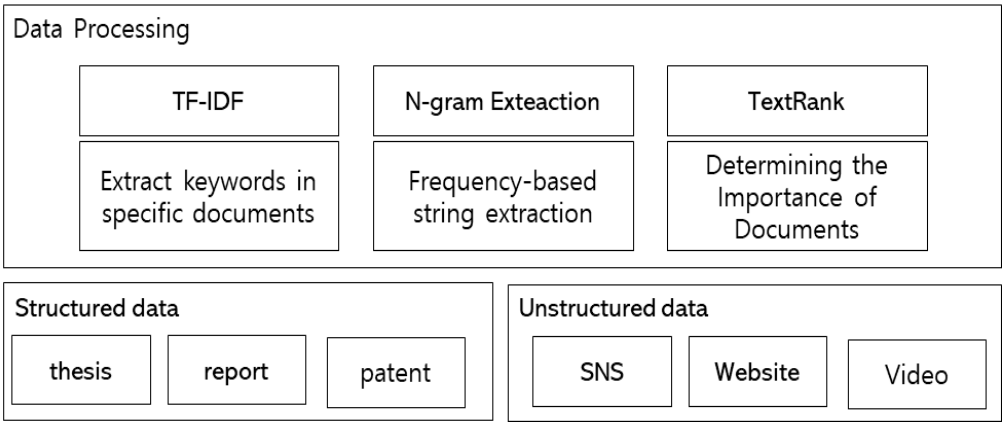

Figure 11. Structured/nonstructured data collection module.

The structured/nonstructured data collection module provides automated collection and data storage functions as key functions, and the automated collection process can be classified once again, depending on whether to use API. In the case of a common academic material platform, it collects data using API, and if API cannot be used, the data is collected using web scraping and web crawling.

From the collected data, keywords for attack simulations are extracted through keyword extraction, and in the course of extraction, TF-IDF (term frequency-inverse document frequency), N-gram Extraction and TextRank are applied to summarize the data and prepare supportive materials for the simulation.

TF-IDF gives high scores to words that do not frequently appear in other documents than the document in a bid to extract keywords for the document. Formula (1) is used to find specific words frequently appearing in the document, and Formula (2) is used to find specific words frequently appearing in each document against all documents. Formula (3) is used to find keywords that frequently appear in that document and do not frequently appear in other documents and extract words with high importance in a specific document.

$$TF = (number\ of\ specific\ word\ entries)/total\ number\ ot\ words \tag{1}$$

$$IDF = log_e(total\ documents)/(number\ of\ documents\ with\ specific\ words) \tag{2}$$

$$TF - IDF = TF * IDF \tag{3}$$

TF-IDF allows extraction of key keywords regardless of the document's form by checking the percentage of words in the document, eliminating frequently used but less relevant characters such as prepositions and html codes.

TextRank is utilized to summarize the document and extract keywords by calculating the relative importance among documents or words. It adopts the concept of Google's PageRank algorithm for natural language processing, and Formula (4) is used, where c of the web page inflow is the inflow through a link while 1-c is the random inflow. Bu is the backlink start pointed towards node u, and N_v is the number of links of each node v. One node v divides its own ranking by N_v and delivers to page u, which is connected through the links. Nodes with backlinks from important nodes (high ranking) are ranked high [35].

$$PR(u) = c * \sum_{u \in B_u} \frac{PR(v)}{N_v} + (1 - c) * \frac{1}{N} \tag{4}$$

TextRank uses the set of words with a large amount of usage, organized in each document through TF-IDF, which was previously conducted, to check the word association

between documents. A set of documents with high correlations between words in each document can predict the relevance of recorded descriptions between each document.

N-gram Extraction is a language model calculating the weights of keywords by tokenizing strings in the unit of n consecutive characters based on the frequency of appearing in the document. This model designs a probabilistic process for a specific list of words, and therefore, contextual information can be obtained [36]. In general, as applying N-gram Extraction to every string in the document is ineffective, it is better to apply it to only specific categories to analyze the consecutive strings for important keywords. Formula (5) formulizes the process of totaling the relative frequency, obtaining how many times the word appears in the unit of string and measuring the importance based on the frequency of the string. The appearance probability of String A can be identified by dividing the number of appearances of String A by the sum of all strings.

$$P(A) = \left(\frac{A}{total\ string} \right) \tag{5}$$

Sentences extracted by applying N-gram Extraction are analyzed for the main keywords classified by the two techniques, TF-IDF and TextRank, which were previously processed and the words related to the keywords by analyzing the related sentences focusing on the keywords. Through this, it is possible to automatic collecting keywords related to technology. Figure 12 shows the process of collecting and processing data in the structured/nonstructured data collection module.

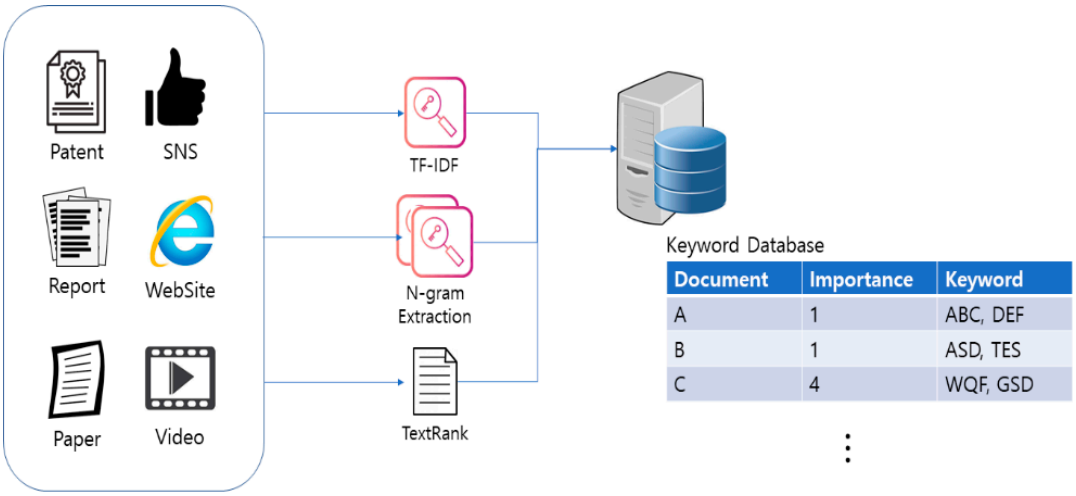

Figure 12. Data collection and processing process.

3.3. Vulnerability-Based Knowledgebase Module

The vulnerability-based knowledgebase module continuously analyzes vulnerabilities and attack strategies for the current system through statistical analysis and machine learning based on the data collected by the structured/nonstructured data collection module. It applies the analysis results to a virtual environment set similar to the real environment so as to estimate the probability of a successful attack and prepare attack strategy scenarios that can occur. Figure 13 shows the structure of a knowledgebase with information on the techniques and attack techniques applied in the vulnerability-based knowledge base module.

Keywords obtained through analysis in the structured/nonstructured data collection module can be utilized as an independent variable for attacks that can occur in the future, and each keyword is linked to related attack and keywords for new attacks are added to predict attacks on an ongoing basis.

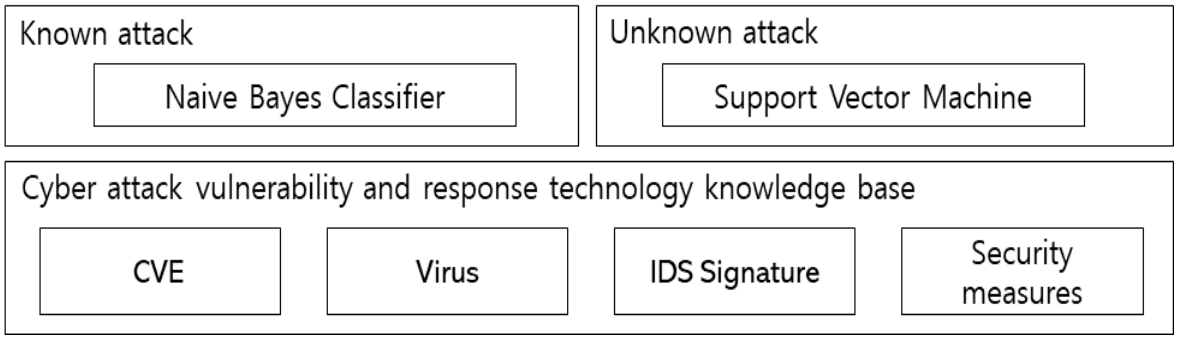

Figure 13. Vulnerability-based knowledgebase module.

In the structured/nonstructured data collection module, the Naive Bayes Classifier is used to classify specific attack strategies through keywords. When another attack with different strategies occurs, which category the new attack strategy belongs to will be identified using SVM.

The application of the Naive Bayes Classifier in this paper is to obtain the probability of known attacks and the process of calculating the probability of whether the keyword of the collected data is related to the attack using keywords recorded in the existing knowledgebase Proceed. Therefore, the Naive Bayes Classifier is applied to perform the process of finding the correlation between the collected data and the attack strategy in the comparative analysis with the keywords recorded in the knowledgebase.

To predict the probability of attack strategies in the existing knowledgebase, Naive Bayes Classifier is used, which is based on obtained probability. Based on the currently observed value, Naive Bayes Classifier calculates the probabilities of which category the strategy belongs to, with an algorithm in which, based on an assumption that the dataset characteristic sets are equal and independent, a classifier is created through the multiplication of conditional probability. Naive Bayes Classifier is an algorithm based on the Bayes' theorem and expressed as Formula (6).

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(B|A)P(A)}{P(B)} \tag{6}$$

In Formula (6), *P(A)* is Prior Probability, which means probability from an event that the observer has known. *P(B | A)* is Likelihood Probability, referring to the probability that other events occur in the assumption that a known event has occurred. *P(A | B)* is Posterior Probability, which is a conditional probability obtained through Prior Probability and Likelihood Probability. *P(B)* is the probability that event B occurs (Normalizing Constant). Using this, relevant attack strategies can be classified based on the probability recorded in the knowledgebase.

Keyword classification through SVM is classified into three layers: the application layer, the transport layer and the internet layer among the four layers of TCP/IP. First, the internet layer including the network layer, and the other two layers are classified into two boundaries. After that, by classifying the application layer and the transport layer, a process of classifying an unknown attack group is performed based on the collected attacks based on keywords.

SVM develops a Hyperplane based on the data and classifies the data into two categories by obtaining the error with the Hyperplane. Unlike Naive Bayes Classifier, SVM implements nonprobable classification and can be used to determine the category to which new data belongs. SVM makes a Hyperplane by applying the kernel function to two-dimensional coordinates, and the vectors defined by the Hyperplane are selected to be combined with image vector parameters. Point x corresponding to the hyperplane is calculated by Formula (7). In Formula (7), if $k(x_j, y)$ becomes smaller as the distance between x

and y is longer, each sum indicates the proximity of data point x_j corresponding to x. As such, the proximity between data can be determined.

$$\sum a_i k(x_j . y) = constant \tag{7}$$

Figure 14 shows the overall flow of the vulnerability-based knowledge base module.

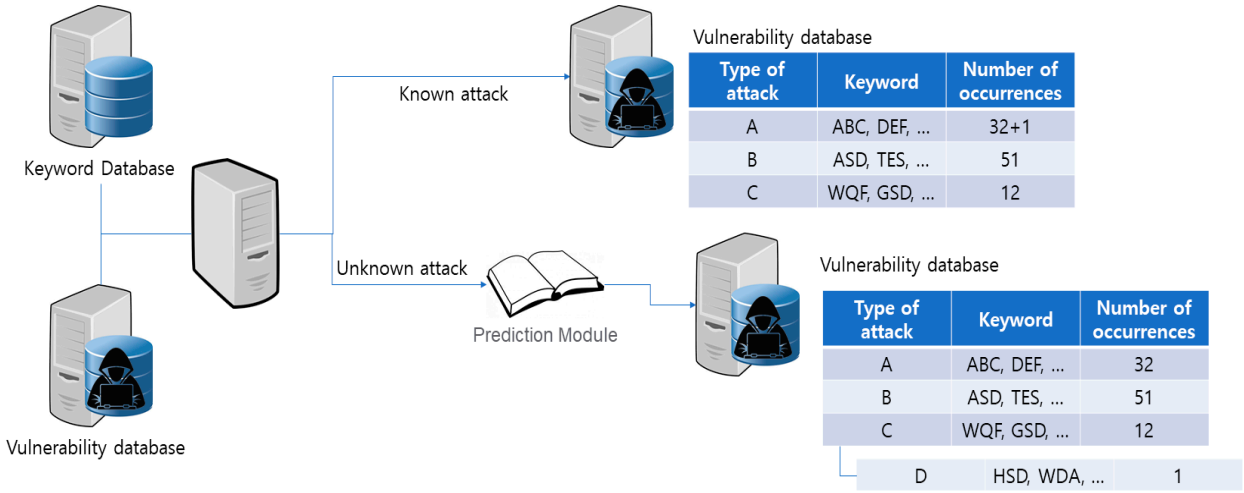

Figure 14. Attack classification process.

3.4. Attacker-Oriented Attack Strategy Simulation Module

The Attacker-oriented Attack Strategy Simulation Module performs an attack on a virtual environment by analyzing the correlation between the analyzed keywords, applicable attack strategies and system vulnerabilities from the attacker's perspective. The purpose of this module is to identify the probability of successful attacks by applying the vulnerabilities of the knowledgebase, correlation between keywords and attacks and attacking tools used by the attacker in the real environment. Figure 15 shows the structure of the attacker-oriented attack strategy simulation module.

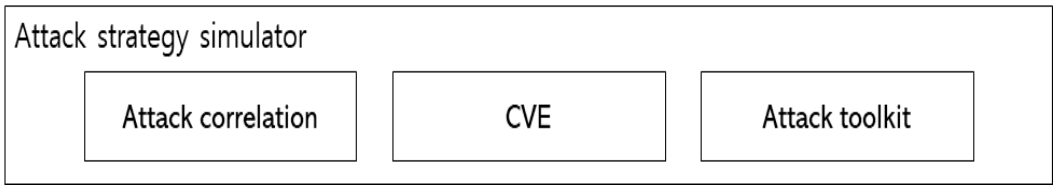

Figure 15. Attacker-oriented attack strategy simulation module.

Attackers may use a variety of attack strategies according to their propensity, as well as private toolkits. It is difficult to apply attack strategies by identifying all of the individual attack strategies. To solve this problem, this research analyzes the tools that can be used to attack [37–39].

3.5. Attack Prediction Module

The attack prediction module predicts attacks that can occur in the future, with materials collected through the vulnerability-based knowledgebase module. This module implements network analysis and time series network analysis to set a prediction scope. Here, network is a data structure composed of nodes and edges. Each entity is called node, and a link between nodes is called an edge. This structure is a structure in the context of

physics and, in the case of mathematics, network, node and edge, is called a graph, vertex and link.

A general network analysis can be conducted through similarities between connection patterns, and it is appropriate for analyzing interactions between large-scale data. There are various network analysis methods, and this research adopted the Ranking (Centrality) method to derive the ranking of data appropriate for the criteria and conditions, as well as the clustering method, to identify the circulation structure and common meaning between words.

The time series network analysis method enumerates the results of the data structure-based network analysis according to the lapse of time. It enumerates the association with the results of analysis of the existing network in a time series to analyze the trend of the association while analyzing the level of convergence of various subjects, as well as trend to derive implications. Figure 16 shows the technique applied in the Attack Prediction Module.

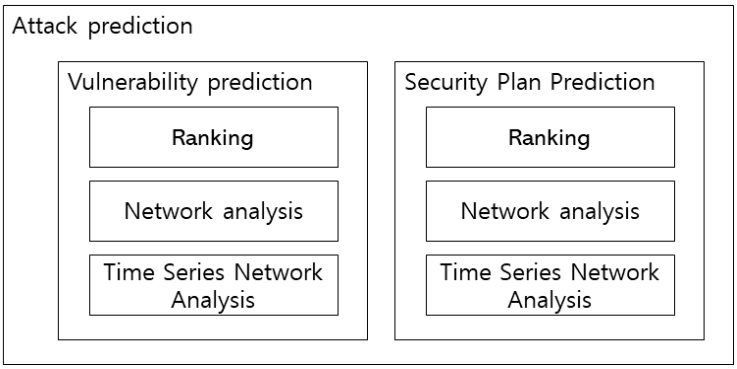

Figure 16. Conceptual diagram of the attack prediction module.

First, the Ranking method applied to network analysis derives rankings of data according to various criteria and conditions, and it is utilized for measuring relative importance. To measure the relative importance, the closeness, betweenness and degree can be used. Closeness is a measure of how a specific node is close to other node on average, and betweenness is a measure of how many paths passes a specific node when shortest path sets are obtained for all node pairs. Degree is a measure of how a specific node is connected to other nodes. With the three measures, the ranking of data is determined and relative importance is measured.

Next, the clustering method analyzes clustering among data and classifies or clusters large-scale data for the purpose of using the results for collecting response strategies or deduction. For clustering, the K-means algorithm groups datasets. The K-means algorithm divides input data into less-than n or k groups and relocates the center of gravity to the center point of each group and clusters data with high similarity. By applying the K-means algorithm, each keyword and weight are largely divided into three categories: application layer, transport layer and internet layer in the 4th layer of TCP/IP.

Formula (8) is to find the closest cluster by calculating the distance between each data and the cluster. Formula (8) is used to differentiate groups of attacks by resetting the center of mass for grouping data based on the result of Formula (9), and Formula (9) is used to differentiate groups of attacks.

$$S_i^{(t)} = x_p : \left| x_p - u_i^{(t)} \right|_2 \leq \left| x_p - u_j^{(t)} \right|_2 \forall j,\ 1 \leq j \leq k \tag{8}$$

$$u_i^{(t+1)} = \frac{1}{\left| S_i^{(t)} \right|} \sum_{x_j \in S_j^{(t)}} x_j \tag{9}$$

The Euclidean distance value of the keyword calculated by the two equations is used as a means to check the relevance of each keyword to the attack. Keywords form a certain cluster for each attack, and attack techniques that can proceed according to the keywords collected through the cluster can be selected.

While the network analysis method is used to identify complicated relations of security technology domains by understanding the relationship of similarity between data, the time series network analysis method is applied to analyze the trend of links through time series enumeration. The time series analysis models include Autocorrelation (AR), Moving Average (MA), Autoregressive Moving Average (ARMA) and Autoregressive Integrated Moving Average (ARIMA) models. When, among data with a tendency of maintaining average, a previous value affects a following value, AR is applied. When the average is moving for time series data, for example, when the average of variables continuously tends to increase or decrease, MA is applied. A mix of the AR and MA models is the ARMA model. The ARIMA model reflects the momentum of the past data.

The ARIMA model can be applied to variables with relatively instable time series characteristics compared to the ARMA model. ARIMA is divided into AR (Autoregression), I (Integrated) and MA (Moving average). The ARIMA model can predict the value that can occur at the point t by summing the past values for the value of e_t, which is the error value, and y_t, which is the value at point t, which is finally desired to be measured.

In the AR model, prediction is based on patterns in the past, while the time series observed value y_t is predicted by the past observed values ($y_{t-1}, y_{t-2}, \ldots, y_{t-p}$). In the MA model, when the error of the observed value at time point t can be explained by $e_{t-1}, e_{t-2}, \ldots e_{t-q}$, it is assumed to follow the MA(q) model [40–42].

$$y'_t = I + \left(a_1 y'_{t-1} + a_2 y'_{t-2} + \cdots + a_p y'_{t-p}\right) - \left(e_t + \theta_1 e_{t-1} + \theta_2 e_{t-2} + \cdots + \theta_q e_{t-q}\right) \quad (10)$$

In the ARIMA model, when finding y_t with delayed data weight p for autoregression, along with delayed error q for the moving average, it is the ARIMA (p,d,q) model and expressed as Formula (10). Formula (10) analyzes the data grouped by Formula (9) as a time series, allowing you to infer the most likely attacks in the end.

Figure 17 shows the process of processing the data collected in the attack prediction process and shows the flow of the Attack Prediction Module. The vulnerabilities and keywords are analyzed based on data that has been previously processed and transmitted to rank vulnerabilities, and the attack methods that can be deducted from vulnerabilities are classified by group. After that, the ARIMA model is applied to predict the probable attacks based on the previous data of the deducted attacks.

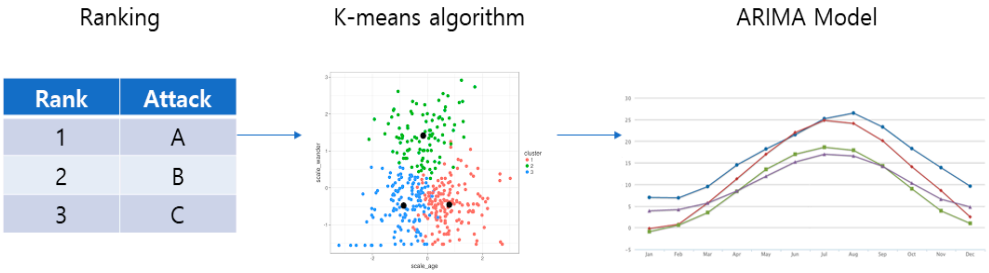

Figure 17. Attack prediction process.

4. Comparative Analysis of Cyberattack Strategy Frameworks Using the Cyber Kill Chain Method

The framework proposed in this research detects attacker-oriented attacks on vulnerabilities and predicts attacks, their success rate and level of threat to minimize damage. In general, vulnerabilities to a system or a network can be classified by vulnerability analysis through vulnerability scanning, along with actual attack methods through penetration

testing. In particular, penetration testing has the same function as the proposed framework in that an actual attack can be carried out on the vulnerabilities that can be attacked, but the proposed framework not only carries out attacks but also predicts the probability of vulnerability occurrence and delivers the results to the administrator. Table 3 shows comparative analysis among vulnerability scanning, penetration testing and proposed framework [43–45].

Table 3. Comparative analysis of the existing methodologies and the proposed framework.

	Vulnerability Scanning	**Penetration Testing**	**Proposed Framework**
Scope	Identify all potential vulnerabilities	Identity attackable vulnerabilities	Identity attackable vulnerabilities
Vulnerabilities	Classify vulnerabilities based on standardized theoretical information	Check vulnerabilities to specific network resources	Check vulnerabilities to specific network resources
Usefulness of checking results	Identify and provide vulnerabilities that cannot be false-positive or exploited	Identify and attack vulnerabilities that actually threaten	Identify and attack vulnerabilities that actually threaten
Network connection check	No connections revealed among network components	Exploit a trust relationship among network components	Check a trust relationship between network components
Improvement support	Provide lists of vulnerabilities	Evaluate potential risk of a specific vulnerability that can be exploited, and prioritize vulnerabilities that require caution and immediate processing	Predict specific vulnerabilities with high probability of occurrence
Inspection on security investment	Does not provide virtual attacks	Carry out actual attacks to check if it normally operates	Carry out actual attacks to assess probability and level of threat
Security risk evaluation	Identify patches that are not applied only. Actual security risk cannot be evaluated.	Assess risk based on actual threats through imitating hackers or worms' acts	Assess risk based on substantial threats using attackers' attack strategies

5. Conclusions and Future Plans

As cyberattacks become diverse and sophisticated, researchers in that field are studying not only defense strategies but, also, the prediction of cyberattacks, and the Science of Security is being also increasingly studied, in which assumptions on physical security, managerial security and information security and their verifications are conducted and new knowledge are created. In addition, various research and projects approaching cyberattacks from different perspectives are underway [46].

One of the good examples is the CHESS project owned by the US Department of Defense and BAS, which is in the commercialization phase. The CHESS project, which analyzes vulnerabilities from the attacker's point of view, studies methods to find vulnerabilities from the attacker's point of view, analyzes technologies and systems to find vulnerabilities and develops and applies concept verification codes for vulnerabilities. BAS conducts a simulation of attack scenarios in an automated way, and various attack scenarios are simulated for vulnerabilities in the existing environment so that a more precise vulnerability analysis can be conducted.

As such, various studies on attack simulation are in progress, and countermeasures for attack strategies must be prepared at any time. In response to an attack, an analysis of the vulnerability used in the attack or a security measure based on an attack technique can be applied. However, it is difficult to analyze information about all attacks and to suggest solutions. Therefore, an automated means to strengthen security against ever-increasing attacks is required, and this paper proposed an attack prediction framework based on structured/unstructured data.

A prediction-based cyberattack framework was proposed. In the framework, structured and nonstructured data was collected to analyze attacking tools and attack strategies, and the attacks were simulated in a virtual environment to predict attacks that may occur in the future, and then, they were prioritized, and finally, the prediction results and scenarios were delivered to the administrator.

Author Contributions: Conceptualization, methodology, investigation, writing—original draft preparation and project administration, J.K.; validation and formal analysis, S.R.; data curation, Y.S. and writing—review and editing and supervision N.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) and funded by the Ministry of Education (NRF-2019R1I1A3A01062789).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yasasin, E.; Prester, J.; Wagner, G.; Schryen, G. Forecasting IT security vulnerabilities—An empirical analysis. *Comput. Secur.* **2020**, *88*. [CrossRef]
2. Caporale, G.M.; Kang, W.-Y.; Spagnolo, F.; Spagnolo, N. Non-linearities cyber attacks and cryptocurrencies. *Financ. Res. Lett.* **2020**, *32*. [CrossRef]
3. Park, N.; Lee, D. Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment. *Pers. Ubiquitous Comput.* **2018**, *22*, 3–10. [CrossRef]
4. Kim, J.; Park, N. Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing. *Pers. Ubiquitous Comput.* **2019**, 1–9. [CrossRef]
5. Kiwia, D.; Dehghantanha, A.; Cho, K.K.R.; Slaughter, J. A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. *Comput. Sci.* **2018**, *27*, 394–409. [CrossRef]
6. Noor, U.; Anwar, Z.; Amjad, T.; Cho, K.K.R. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Gener. Comput. Syst.* **2019**, *96*, 227–242. [CrossRef]
7. Science of Security. Available online: https://www.nsa.gov/What-We-Do/Research/Science-of-Security/ (accessed on 20 April 2021).
8. Smith, C.L.; Brooks, D.J. *Security Science: The Theory and Practice of Security*; Elsevier: Amsterdam, The Netherlands, 2013.
9. Lee, J.; Moon, D.S.; Kim, I.K. Technological trends in cyber attack simulations. *Electron. Telecommun. Trends* **2020**, *35*, 34–48.
10. Lee, D.; Park, N. Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. *Multimed. Tools Appl.* **2020**, 1–18. [CrossRef]
11. Khan, P.W.; Bryun, Y.-C.; Park, N. A Data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electronics* **2020**, *9*, 484. [CrossRef]
12. Yadav, T.; Rao, A.M. Technical aspects of cyber kill chain. *Commun. Comput. Inf. Sci.* **2015**, *536*, 438–452.
13. Fox, D.B.; Arnoth, E.I.; Skorupka, C.W.; McCollum, C.D.; Bodeaou, D.J. *Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions*; The Homeland Security Systems Engineering and Development Institute: McLean, VA, USA, 2018.
14. Lee, D.; Park, N.; Kim, G.; Jin, S. De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment. *Peer-Peer Netw. Appl.* **2018**, *11*, 1299–1308. [CrossRef]
15. Hassanzadeh, A.; Burkett, R. SAMIIT: Spiral attack model in IIoT mapping security alerts to attack life cycle phases. In Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research 2018 (ICS-CSR 2018), Hamburg, Germany, 29–30 August 2018.
16. Computers and Humans Exploring Software Security. Available online: https://www.darpa.mil/program/computers-and-humans-exploring-software-security (accessed on 28 April 2021).
17. Kim, J.; Park, N.; Kim, G.; Jin, S. CCTV video processing metadata security scheme using character order preserving-transformation in the emerging multimedia. *Electronics* **2019**, *8*, 412. [CrossRef]
18. Park, N.; Sung, Y.; Jeong, Y.; Shin, S.-B.; Kim, C. The analysis of the appropriateness of information education curriculum standard model for elementary school in Korea. *Int. Conf. Comput. Inf. Sci.* **2018**, 1–15. [CrossRef]
19. Hahn, A.; Thomas, R.K.; Lozano, I.; Cardenas, A. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *11*, 39–50. [CrossRef]
20. Yadav, T.; Rao, A.M. Technical aspects of cyber kill chain. In *International Symposium on Security in Computing and Communication. Security in Computing and Communications*; Springer: Cham, Switzerland, 2015; pp. 438–452.

21. Lee, D.; Park, N. Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance. *Supercomputing* **2017**, *73*. [CrossRef]
22. Kim, J.; Park, N. Role-based Access Control Video Surveillance Mechanism Modeling in Smart Contract Environment. In *Transactions on Emerging Telecommunications Technologies*; John Wiley & Sons, Inc.: New York, NY, USA, 2021. [CrossRef]
23. Park, N.; Kang, N. Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. *J. Sens.* **2015**, *16*, 1–16. [CrossRef]
24. Samtani, S.; Chinn, R.; Chen, H.; Nunamaker, J.F., Jr. Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *J. Manag. Inf. Syst.* **2017**, *34*, 1023–1053. [CrossRef]
25. Fang, Y.; Liu, Y.; Huang, C.; Liu, L. FastEmbed: Predicting vulnerability exploitation possibility based on ensemble machine learning algorithm. *PLoS ONE* **2020**, *15*, e0228439. [CrossRef] [PubMed]
26. Kaloudi, N.; Li, J. The AI-based cyber threat landscape: A survey. *ACM Comput. Surv.* **2020**, *53*, 1–34. [CrossRef]
27. Paul, K. Multi-level security requirements for hypervisors. In Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, AZ, USA, 5–9 December 2005.
28. Park, N.; Kwak, J.; Kim, S.; Won, D.; Kim, H. WIPI mobile platform with secure service for mobile RFID network environment. *J. Adv. Web Netw. Technol. Appl.* **2006**, 741–748. [CrossRef]
29. Xu, M.; Jiang, X.; Sandhu, R.; Zhang, X. Towards a VMM-based usage control framework for OS kernel integrity protection. In Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, Sophia Antipolis, France, 20–22 June 2007; pp. 71–80.
30. Kim, J.; Lee, D.; Park, N. CCTV-RFID enabled multifactor authentication model for secure differential level video access control. *Multimed. Tools Appl.* **2020**, *79*, 23461–23481. [CrossRef]
31. Park, N.; Kim, M. Implementation of load management application system using smart grid privacy policy in energy management service environment. *Clust. Comput.* **2014**, *17*, 653–664. [CrossRef]
32. Park, N.; Bang, H.C. Mobile middleware platform for secure vessel traffic system in IoT service environment. *Secur. Commun. Netw.* **2016**, *9*, 500–512. [CrossRef]
33. Park, N.; Hu, H.; Jin, Q. Security and privacy mechanisms for sensor middleware and application in internet of things (IoT). *J. Distrib. Sens. Netw.* **2016**, *12*. [CrossRef]
34. Keyword Eextraction and Key Sentence Extraction using TextRank (Implementation and Experiment). Available online: https://lovit.github.io/nlp/2019/04/30/textrank/ (accessed on 28 April 2021).
35. Figueiredo, L.N.L.; de Assis, G.T.; Ferreira, A.A. DERIN: A data extraction method based on rendering information and n-gram. *Inf. Process. Manag.* **2017**, *53*, 1120–1138. [CrossRef]
36. Park, N.; Kim, B.G.; Kim, J. A Mechanism of masking identification information regarding moving objects recorded on visual surveillance systems by differentially implementing access permission. *Electronics* **2019**, *8*, 735. [CrossRef]
37. Kim, J.; Park, N. Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments. *Appl. Sci.* **2020**, *10*. [CrossRef]
38. Park, N.; Park, J.; Kim, H. Inter-Authentication and Session Key Sharing Procedure for Secure M2M/IoT Environment. *Int. Inf. Inst. (Tokyo) Inf.* **2015**, *18*, 261–266.
39. Kotu, V.; Deshpande, B. Autoregressive integrated moving average. *Data Sci.* **2019**. [CrossRef]
40. Park, J.; Kim, J.; Gupta, B.B.; Park, N. Network Log-Based SSH Brute-Force Attack Detection Model. *CMC-COMPUTERS MATERIALS & CONTINUA* **2021**, *68*, 887–901. [CrossRef]
41. Kim, J.; Park, N. A Face Image Virtualization Mechanism for Privacy Intrusion Prevention in Healthcare Video Surveillance Systems. *Symmetry* **2020**, *12*. [CrossRef]
42. Park, N. The implementation of open embedded S/W platform for secure mobile RFID reader. *J. Korean Inst. Commun. Inf. Sci.* **2010**, *35*, 785–793.
43. Park, N. Secure data access control scheme using type-based re-encryption in cloud environment. In *International Conference on Hybrid Information Technology*; Springer: Berlin/Heidelberg, Germany, 2011.
44. Park, N. Secure UHF/HF dual-band RFID: strategic framework approaches and application solutions. In *International Conference on Computational Collective Intelligence*; Springer: Berlin/Heidelberg, Germany, 2011.
45. Park, N.; Song, Y. Secure RFID application data management using all-or-nothing transform encryption. In *International Conference on Wireless Algorithms, Systems, and Applications*; Springer: Berlin/Heidelberg, Germany, 2010.
46. Park, N.; Kim, S.; Won, D.; Kim, H. Security analysis and implementation leveraging globally networked RFIDs. In *IFIP International Conference on Personal Wireless Communications*; Springer: Berlin/Heidelberg, Germany, 2006.