Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

# A Study on Threat Modeling in Smart Greenhouses

So-Hyeon Cho[1], Dong-Seok Kang[1], Min-Song Kang[1], Hyeon-Soo Kim[1], Jin-Woong Bae[1], Chung-Il Lee[1], Han-Byeol Ji[1], Yo-Han Won[1], Hyeon-Kyoung Hong[1], and Kyounggon Kim[2*]

[1] *Best of the Best, Korea Information Technology Research Institute, South Korea.*
[2] *Department of Forensic Sciences, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.*

*Received 10 Nov. 2020; Accepted 10 Dec. 2020; Available Online 20 Dec. 2020*

## Abstract

In the era of agriculture 4.0, cutting-edge technologies including Information and communication technology (ICT) is being introduced into traditional agriculture. As farm intelligence emerges as a key area of smart agriculture, the scope of agriculture has expanded from the seed industry to distribution and logistics, however the area that is still most directly connected to the physical agricultural environment is smart farming. Cybersecurity incidents or cybercrimes in smart farming can directly damage crops and harm human safety. Research on individual technical elements that constitute smart farming has been ongoing for a long time relatively, however it has not been long since the work of systematically identifying and classifying threats to smart agriculture as a whole. In this study, STRIDE threat modeling is used to identify cyber threats to greenhouse and make system design more robust. Through this work, we have derived 126 threats and have created 4 types of attack trees. It will be the basis to allow systematic threat classification more clearly in smart greenhouse.

## I. Introduction

The fourth industrial revolution affects agriculture. The era of agriculture 4.0, in which the labor force, knowledge, and experience, which are input elements of traditional agriculture, are accumulated as big data, and unmanned and intelligent agricultural work is realized has opened. In addition to the production stage of agriculture, smart agriculture has emerged in which various advanced technologies including ICT have been grafted throughout the expanded agricultural value chain. The reason why research and development for smart agriculture is being actively carried out is that in addition to the technological advancement of the times, smart agriculture is the key to solving various problems in the traditional agriculture.

Population growth requires more food and energy in the future, and the need to increase agricultural product productivity is increasing to prepare for the future food and energy crisis. Promoting food security was the reason it helped to not only solve the hunger problem, but also to improve the outlook for world peace. This shows that the need to strive for food security to ensure future food production is a global task and that agriculture occupies a very important area in human society.

The necessity of smart agriculture is ironically emphasized in the opposite case. Even in countries with slow population growth, smart agriculture can still play an important role. Although the population of the home country is decreasing, the import of agricultural products

**Keywords:** *Smart Agriculture, Smart Farming, Security; Cybercrime, Cyber-attack, Internet of Things, Threat Modeling.*

Production and hosting by NAUSS

* Corresponding Author: Kyounggon Kim
Email: KKim@nauss.edu.sa.

doi: 10.26735/KKJN1042

from abroad continues. In order to overcome this, production adjustment and market forecasting capabilities must be improved, and smart agriculture can perform this more easily than traditional agriculture.

ICT can meet the needs of food safety issues, livestock disease prediction, and distribution safety management beyond agricultural production. As such, smart agriculture is in the spotlight as the key to various problems, and the related market continues to grow. With the introduction of data-based farm intelligence into agriculture, the scope of smart agriculture has expanded beyond the production stage. Smart agriculture starts from the pre-production stage and is becoming a concept encompassing the production, distribution and consumption stage each.

If a security breach occurs in smart agriculture, the leakage of agricultural technology and obstruction of agricultural product production are fundamental. Distribution of productivity may be disrupted and the financial market and national security may be affected. Threat actors and attack vectors are very complex and diverse, as states can act as both targets and threat actors.

Smart farming has expanded, but looking at its practically commercialized form, the most widely introduced technology is in the direct production stage, smart farming. Since Internet of Things (IoT), cloud, and big data technologies, including TCP/IP-based wired networks and wireless networks such as Zigbee and Wireless LAN, are evenly used in smart farms, there is a possibility that existing cyber attacks against information and communication facilities will target these well known systems.

In this paper, STRIDE threat modeling technique is used to identify security threats of smart farms and derive possible attack scenarios. Our findings help direct designers when creating a smart agricultural system. Since the focus is on smart greenhouses in smart agriculture, our recommendatins can be introduced to governments and related industry planning to build smart greenhouses. In addition, this study can be similarly applied to the design of a vertical plant factory systems that will be the core of future smart-city, urban agriculture.

This paper is organized as follows. Section 2 examines research on cyber threats in smart agriculture, and Section 3 discusses the smart farm market and technology background. In Section 4, the research methodology we proposed is explained, and in Section 5, cyber threats are identified according to the threat modeling technique. Section 6 presents potential threat scenarios. Lastly, Section 7 summarizes the conclusion.

## II. Related Works

Advanced agricultural countries around the world are developing smart agriculture in a way that suits their environment in consideration of geographic, social, and economic characteristics. However, the terms and directions of technology development are slightly different per region.

The United States has been promoting R&D for smart agriculture-related technologies such as precision agriculture and big data for a long time, and has strengths in smartization and data library accumulation for field agriculture [1]. In the Netherlands, in order to increase productivity on a small area of land, it is growing by implementing a cutting-edge agricultural system centering on fields such as facility horticultural agriculture, fruit trees, and livestock, and seeking high added value through the pre-farming value chain [2]. In the EU, international cooperative research is being carried out in connection with farmers, experts, companies, NGOs, etc. for sustainable agriculture [3].

Sina Sontowski et al. listed attacks that could occur in smart farm networks, demonstrated DoS attacks by building a test bed using Raspberry, and utilizing Wi-Fi deauthentication attacks [4]. Sebastian Lisner et al simulated attacks that may occur in wireless sensor networks based on two scenarios [5]. In addition, in research related to smart agriculture security, warnings about sensor and network security are often a prominent concearn.

As the definition and scope of smart agriculture expands, the connection with various industrial groups is strengthening. There are many new types of scenarios reflecting the expanded definition of smart agriculture. The Public-Private Analytic Exchange Program Report explained and introduced scenarios that can occur within the precision agricultural system in terms of confidentiality, integrity, and availability [6]. Molly M. Jahn et al described data contamination scenarios that can occur in smart agriculture and food systems [7].

Threat research on each of the components of a large system called smart agriculture has been systematically conducted. Idress S. Kocher et al introduced threat modeling study on WSN (Wireless Sensor Network). They intoduced DoS, sybil attacks, traffic analysis attacks, node replication attacks, and physical attacks then presented countermeasures for each layer [8]. Sebastian Lisner et al. conducted research on smart pharming vulnerability assessment while identifying network attacks that can occur in smart pharming [5]. Jason West introduced Precision Agriculture technology and a principles-based framework for assessing the vulnerability of the environment in which the technology is applied [9]. Kyoung-gon Kim et al. proposed STRIDE approach to identify cyber threat regarding Smart Home IoT [10],[11] and Smart TV [12]. However, this approach is not for the smart farm.

Although the terms threat assessment and framework were used in previous studies, studies using systematic threat classification methodologies were rare. Therefore, we identify threats and derive possible scenarios targeting smart greenhouses.

## III. Background

Precision agriculture is the area where security-related research has been focusing on among smart agriculture. Precision agriculture can greatly increase the production efficiency per area, and it also increases efficiency in varieties, irrigation, crop nutrition, fertilizer and pesticide.

There are three main categories of valuable resources in a smart farming business.

First, there is the production of growth like crops and livestock.

Second, data related to agricultural technology and sensing data management required for crop production, including quality information, can also be a business asset.

Third, resources include smart farming high value-added systems and technologies that have invested a lot from research and development to construction.

The main systems and technologies are as follows:

- Crop and Livestock Production
- Drilling and Seeding
- Fertigation
- Water Management
- Livestock Monitoring
- Livestock Tracking Wearables
- Crop Monitoring
- Aerial Monitoring and Spraying
- Farm Equipment
- Smart Agriculture Sensors
- Agriculture Machinery
- Food Distribution Vehicle Telemetry
- Supply Chain Monitoring
- Online portals for Commerce
- Supervisory control and data acquisition (SCADA)
- Heating, ventilation, and air conditioning (HVAC)
- Decision Support System (DSS)
- Farm Management Software
- Logistic Management Software
- Big Data Analytics and Machine Learning
- Location Technology
- Remote Sensing Technology

In smart agriculture, the forefront of the physical agricultural environment and ICT technology meeting can be seen as a greenhouse. According to Y.4466 (Framework of smart greenhouse service), finally published as the ITU-T standard, the smart greenhouse service enables precision farming with the help of IoT devices (such as sensors and actuators) installed in a smart greenhouse. A smart greenhouse is a facility that can control a greenhouse environment that minimizes human intervention by using IOT, and a group of smart greenhouses under the management of a manager is called a smart farm [13].

## IV. Methodology

In this study, a STRIDE threat modeling technique is used to identify the threat to smart greenhouses. Threat modeling is a proactive approach to secure resilience and to make the system robust

### *A.Identifying Architecture Layers*

We have focused on the structure of the smart farm greenhouse with international standards. Among the various assets of smart agriculture, it identifies the assets in the common denominator with the greenhouse. After that, we look at the structure of the greenhouse layer.

Smart farming using greenhouses relies on intelligent networks based on the Cyber Physical System (CPS). The CPS could monitor, interoperate, control, and integrate by computer and interactive systems while allowing interaction with the physical world using a set of network agents. Network agents include sensors, actuators, and control handlers.

Fig. 1 is a conceptual diagram of a greenhouse house suggested in the ITU-T recommendation, "Framework of smart greenhouse service". Sensors collect soil humidity, fertilizer, and weather change data and deliver it in real time via a wireless network, which simultaneously provides real-time access to analysis and information on land, crops, livestock, logistics and machinery. The actuator moves as pre-programmed [14].

After analyzing the greenhouse by hierarchy, the overall structure diagram is as depicted in Fig. 2. Through this analysis, it is possible to identify security threats more clearly by layer. Networks can be classified into five major layers.

*1) Physical Layer:*

The physical layer is composed of various sensor, MCU, router, switch, gateway, and actuator. This is the lowest layer that transmits the collected sensing data to the upper layer and receives control signals. One-way communication is performed when sensing data is transmitted to an upper layer, and two-way communication is performed when sensing and control data is exchanged with an upper layer.

*2) Link Layer:*

The link layer is composed of various communication technologies, and Wi-Fi, LTE, and GSM are deployed and used in this layer. ZigBee replaces long-distance communication, and Long Range (LoRa) and Bluetooth are often used for device-to-device communication, and facilities are built.

*3) Middleware Layer:*

IoT-based middleware performs device management, interoperability, platform portability, as well as interoperability and security related tasks. Various types of middleware perform context-aware functions, and the architecture is implemented to protect security and user privacy.

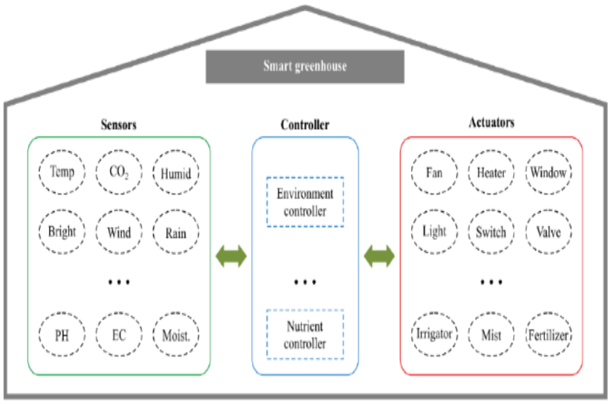

Fig. 1. Conceptual diagram of smart greenhouse [13]

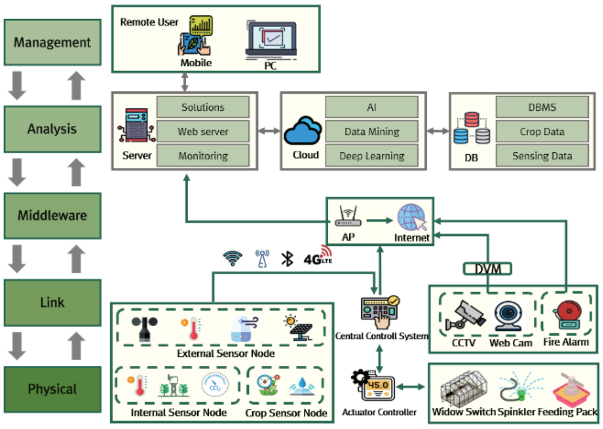

Fig. 2. Layered Architecture of smart greenhouse

*4) Analysis Layer*:

In the analysis layer, the equipment in the plant cultivation system is automatically controlled by comprehensively analyzing crops, external weather, and sensing data. The system can collect and analyze temperature data obtained from the atmosphere and perform systematic analysis of various conditions that can affect plant growth.

*5) Management Layer:*

The management layer uses web sites or mobile applications for system remote control and sensing network monitoring. A person with access authority can receive plant growth information stored in the database server in the analysis layer and use it for decision-making and can reflect requirements in real time through a user-friendly web-based control panel.

### *B. Threat Modeling Classes*

We have adopted the concept of threat modeling to analyze information security threats. Microsoft STRIDE and MITER CAPEC [15] models are representative threat modeling.

STRIDE is an abbreviation of most common six threats categories spoofing, tampering, repudiation, information disclosure, denial of services, and Escalation of privileges. Loren ohnfelder and Praerit Garg are the inventors of STRIDE threat modeling [16]. This framework and mnemonic were designed to help people developing software to identify the types of attacks that software tends to experience [17]. The classification of STRIDE simplifies threat categories and allows avails detailed studies. STRIDE has the advantage of being systematic and conceptual, thus it is very clear when it comes to the principle of threats and covering most of the known threats, STRIDE also has the tools that could inspect any system in the graphical interface and easy to use. From another point of view, STRIDE has issues with a sequence of threats and difficulties to categorize each real-life threat into the six categories of STRIDE.

STRIDE can be summarized into the following main items [18]:

1. Creating an architecture overview: during these steps, identify what the application does, create an architecture diagram, and identify the technologies used.
2. Creating a system model which help in analyzing and decomposing a system from most of its components.
3. Creating a Data Flow Diagram (DFD) showing the trust boundaries, data flow, entry points, and privileged code.
4. Creating attack library with STRIDE: One of the strongest attack libraries to be used as a source of attack library is CAPEC and ATT&CK frameworks from MITRE.

## V. Study Threat Modeling

### A. Architecture Overview

During these steps, identify what the application does, create an architecture diagram, and identify the technologies used.

Fig. 3 is a functional flow chart of the smart greenhouse. The standard configuration of the smart greenhouse consists of a smart greenhouse detection function connected to sensors, a smart greenhouse operation function connected to an actuator, a smart greenhouse control function that integrates and controls these two functions, a smart greenhouse operation function, and an integrated smart greenhouse management function

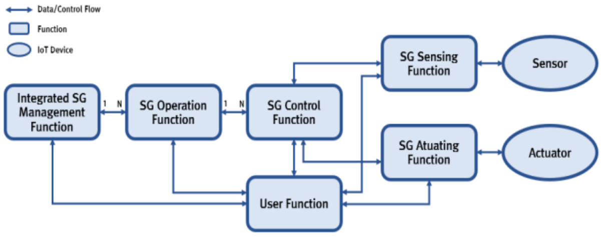

Fig. 3. Conceptual diagram of smart greenhouse [13]

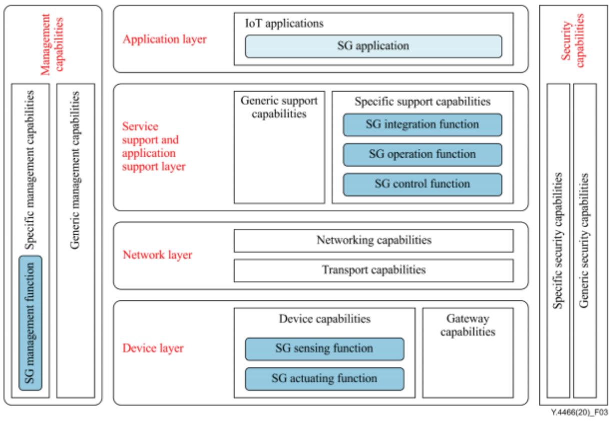

Fig. 4. Smart Greenhouse reference model in accordance with the IoT reference model [13]

### B. System Model

The next step is creating a system model which helps in analyzing and decomposing a system from most of its components. The IoT reference model consists of application layer, service support and application support layer, network layer and device layer, and capabilities of management and security. The reference model of smart greenhouse introduced in ITU-T standard document is shown in Fig. 4. Among those layers and capabilities of the IoT reference model, the SG service reference model defines six more functions specific to a SG service. In this regard, the following functions are defined as components of the SG service reference model:

- SG sensing function.
- SG actuating function.

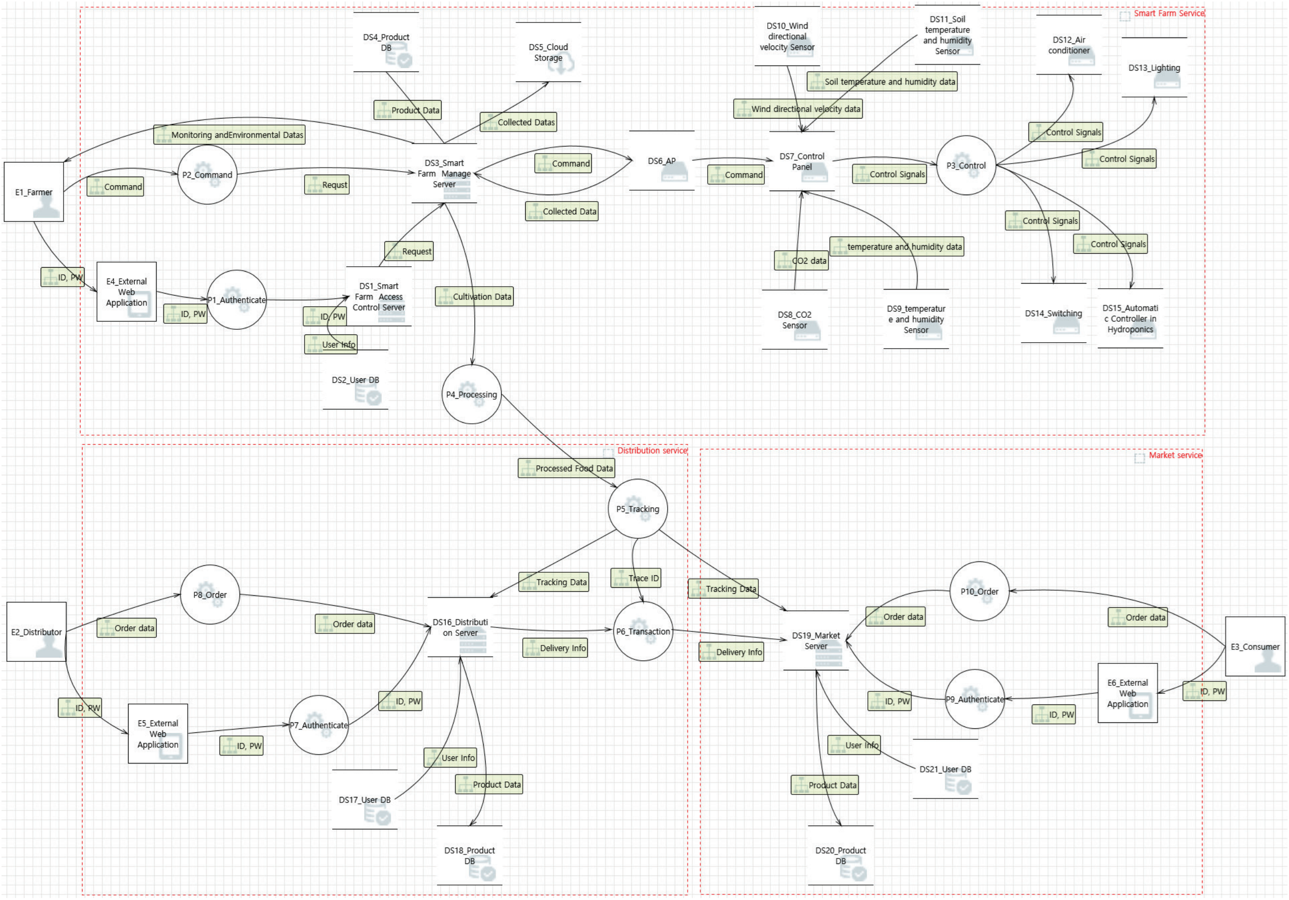

Fig. 5. Data flow diagram of smart greenhouse and related market

- SG control function; Rec. ITU-T Y.4466
- SG operation function.
- SG integration function.
- SG management function.

### C. Data Flow Diagram

We have created Level 2 DFD of smart farms, and through this, we identified threats of smart farms. The tool automates the full process of threat modeling.

Fig. 5 shows the data flow centering on the remotely controlled mobile application in the greenhouse. It is a visual representation of the data flow of smart farms, distribution, and markets, through which threats to processes can be identified. The components of each figure are as listed in Table I.

Through the components in Table I, threats can be derived according to the STRIDE element. According to report of the SANS Institute, the STRIDE element can be split into three different segments ST, ID, and RE as depicted in Fig. 6 [18].

ST: presents the attack surface or initial access points of the targeted system/zone of the threat modeling which is at level (N), initiated by threat actors and not due to misconfiguration or vulnerability of the system.

ID: presents the impact of the threats on the system, such as information disclosure or denial of service, and it could be any interaction around the targeted system (N-1) such as compromising credentials that enable the attacker to reach components in step (N).

RE: presents the post-exploitation activities such as lateral movement, escalation of privileges, and evasion techniques including denying the responsibility of performing the attack by clearing logging activities or evading the presence. In such case, the attacker either goes deeper to reach more critical zones of the primary target or moves to higher privileges systems/zones (N+1).

The number of derived threats is S:57, T:5, R:9, I:8,

Table I
DESCRIPTION OF SMART FARM DFD ELEMENTS

| Group | Component | Explanation |
|---|---|---|
| Entity | Farmer | Farmer |
| Entity | Distributor | Distributor |
| Entity | Consumer | Consumer |
| Entity | External Web Application | External Web Application |
| Process | Authenticate | Authenticate login info for Server |
| Process | Command | Smart Farm Control Command |
| Process | Control | Smart Farm Instrument Control |
| Process | Processing | Processing Food Products |
| Process | Tracking | Logistics Tracking |
| Process | Transaction | Commodity trading |
| Process | Order | Orders on farms, distribution, and markets |
| Data Store | User DB | store for farmer, distributor, consumer account information |
| Data Store | Smart Farm Manage Server | Smart Farm Management and Control Server |
| Data Store | Product DB | Store for product Info |
| Data Store | Cloud Storage | Store for the environment information of crops |
| Data Store | AP | Input Control Signal Transmission and Load Belling |
| Data Store | Control Panel | Input Control, Acquisition Data Signal Command and Acquisition |
| Data Store | Wind directional velocity sensor | Collect and transmit wind directional wind speed information |
| Data Store | Soil temperature and humidity sensor | Collect and transmit soil temperature and humidity information |
| Data Store | CO2 sensor | Collect and transmit CO2 concentration information |
| Data Store | Temperature and humidity sensor | Collect and transmit temperature and humidity information |
| Data Store | Airconditioner | Performing and transmitting temperature control signals |
| Data Store | Lighting | Performing lighting control |
| Data Store | Automatic Controller in Hydroponics | Perform Hydroponics control |
| Data Store | Switching | Performing opening and closing controls |
| Data Store | Distribution Server | Store and manage product distribution information |
| Data Store | Market Server | Store and manage product sales information |
| Data Flow | Command | Command from Farmer, Smart Farm Management Server, AP |
| Data Flow | ID, PW | ID and PW entered by the user |
| Data Flow | Monitoring and Environmental Datas | Monitoring data collected and environmental data |
| Data Flow | Request | Requests sent to the server |
| Data Flow | Product data | Product information in Product DB sent to Smart Farm Manage Server |
| Data Flow | Collected data | Environmental data collected by Smart Farm Manage Server |
| Data Flow | User Info | User Information in User DB |
| Data Flow | Wind directional velocity data | Wind directional velocity data |
| Data Flow | Soil temperature humidity data | Soil temperature and humidity data |
| Data Flow | CO2 data | CO2 concentration data |
| Data Flow | Temperature humidity data | Temperature and humidity data |
| Data Flow | Control Signal | control command signal |
| Data Flow | Cultivation data | Crop growth data from Smart Farm Manage Server |
| Data Flow | Processed Food Data | Data of processed crops data |
| Data Flow | Tracking Data | Logistics Tracking Data Sent to Distribution Server and Market Server |
| Data Flow | Trace ID | Tracking ID for logistic memory in the transaction process |
| Data Flow | Order data | Distributors and consumers, product order data used in the ordering process |
| Data Flow | Delivery data | Delivery data to be used when distributors deliver goods to the market |

Table II
STRID PER ELEMENTS FOR SMART FARM

| Component | No | Name | STRIDE | Description | Threat |
|---|---|---|---|---|---|
| Entity | E1 | Farmer | S | Attacker can spoof and this may lead to unauthorized access to .Command | T1 |
| | | | R | Farmer claims that it did not receive data from a process on .the other side of the trust boundary | T2 |
| Entity | E2 | Distributor | S | Attacker can spoof and this may lead to unauthorized access to .P9_order | T3 |
| Entity | E3 | Consumer | S | Consumer may be spoofed by an attacker and this may lead to .unauthorized access to Order | T4 |
| **Middle omission** | | | | | |
| Data Store | DS3 | Smart Farm Manage Server | S | Attacker can spoof and this may lead to data being written to .the attacker's target instead of smart farm manage server | T54 |
| | | | S | Attacker can spoof and this may lead to incorrect data deliv-.ered to cloud storage | T55 |
| | | | D | Cannot access smart farm manage server | T56 |
| | | | I | .Attacker can get information not intended for disclosure | T57 |
| **Middle omission** | | | | | |
| Process | P2 | Command | E | An attacker may pass data into command in order to change the flow of program execution within command to the attack-.er's choosing | T89 |
| | | | R | .Command repudiates that data was not received | T90 |
| | | | T | Data flowing across Command may be tampered with by an .attacker | T91 |
| **Middle omission** | | | | | |
| Data Flow | | ID, PW | D | Interrupt ID, PW flow so that it cannot be sent to the destination | T125 |
| Data Flow | | Monitoring and Environmental Data | D | Interrupt monitoring and environmental Data flow so that it cannot be sent to the destination | T126 |

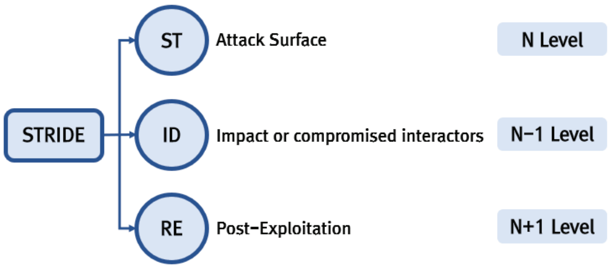

Fig. 6. STRIDE Threat diagram

D:28, E:20, showing a total of 126 threat lists. Some of them are as follows in Table II.

### *D. Attack Tree*

Attack Tree method assumes a security analyst thinks like an attacker and the first thing an attacker decides is the target and goals of an attack. Each goal has a separate attack tree. Each attack tree begins with a goal which represents a root node in the attack tree. Then a list of all possible scenarios to achieve goals will be defined as sub goals and thus a set of sub-nodes under the root node. Every sub-node can is evaluated for figuring out the possibility of success, cost of attack, and particular requirement. Using OR and AND as  conditional symbols OR used to represent alternative ways to achieve a node or sub-node, and AND describes different steps to achieve the same node or sub-node. An attack tree for a smart farm is as listed in Table III.

There could be some security requirements based on the attack tree. For example, spoofing attack make invalid access to command.  In this case, applying the security patch provided by Microsoft is recommended to avoid a system being abused as network traffic tampering server. In addition, network packets containing important data should be encrypted by SSL.

## VI. Potential Attack Scenarios

In this section, some possible attack scenarios will be presented. The smart greenhouse not only can be directly attacked, it also can perform as a security hole that threatens related industries such as smart logistic, traffic, and smart city. The following are hypothetical threat scenarios under the various confidentiality, integrity, and availability standards.

### *A. Confidentiality*

- Target identification

Location data used by GPS systems can be a key security factor. The GPS system can be used to target specific crops on a specific farm [19].

- Information leakage

IP is altered through DNS spoofing to illegally secure other countries' agricultural technology [20]. Agricultural technologies such as genetic engineering, modified seeds organic pesticide information, and fertilizers can be removed.

- Vulnerable authentication chain

As there are not any international standards for authentication interface in smart farming system yet, when using several smart farming control systems and platforms made by different vendors in a single farm, IoT devices delegations are often vulnerable due to exposing auth token or device ID. Vulnerable authentications can be exploited to gain unauthorized access to victim's devices and network.

### *B. Integrity*

- Pollution of livestock health monitoring data

If there is a problem with the wearable smart technology and monitoring system [21] for livestock, it becomes dangerous. Mishandled data can be left to cause livestock to go beyond defined areas [22] and, in the worst case, exploited as an undetected spread of animal disease [23].

- Food safety misinformation campaign

Mass production of 'fake news' can cause confusion in the information ecosystem, health problems of GMO foods, and the use of crops and weeds in US agriculture as issues in society and pose a business threat to companies and related businesses.

- Supply chain shared data pollution

The food system is closely related to commodity transactions and derivative financial products, and the financial market is closely related to the domestic market. Influencing the supply flow of primary commodities such as grain, coffee, and seafood can disrupt the financial system as well as other operations and resource flows. The pollution of important data interferes with the normal functioning of the state and society [24]-[26].

### *C. Availability*

- Control hijacking

By using the Evil Twin Access Point, the packet of the remotely controled system is stolen, and then the forgery packet is transmitted, it could result in an unintentional operation [27]. The entire account can be stolen through password cracking [28].

- System paralysis

DoS attacks on HVAC and SCADA systems or by infecting ransomware can disrupt production. ARP spoofing can be used for MITM or session hijacking, but it can cause DoS.

- Resource exhaustion

The network of smart farming is used as an access point for crypto jacking by infecting online IoT devices with botnets or to other networks for existing cyber operations for farmers' networks or third-party data collectors.

- Natural disaster

Due to the nature of smart agriculture, compared to other industries, it is inevitably affected by nature. Nature disasters can not only temporarily affect information and communication systems, but can also damage precision functions.

Table III

ATTACK TREE FOR SMART FARM

| **Attack Tree** | | | | **Threats** |
|---|---|---|---|---|
| **1** | | **Application** | | |
| OR | 1.1 | Bypass Authentication | | |
| | OR | 1.1.1 | SQL Injection | T5, T6, T8, T9, T12, T17, T33, T34, T35, T37, T38, T59, T66, T67, T68, T105, T106, T110, |
| | OR | 1.1.2 | Brute Force | T79, T80, T82 |
| | OR | 1.1.3 | XSS | T21, T22, T23, T24, T25, T27, T28, T32, T33, T34 |
| OR | 1.2 | Control the Smart Farm | | |
| | OR | 1.2.1 | CSRF | T21, T22, T23, T24, T25, T27, T28, T32, T33, T34 |
| | OR | 1.2.2 | Bypass Business Logic | T52, T53, T59, T66, T67, T68, T71, T74, T114, T115, |
| OR | 1.3 | Get Secrets of the Company | | |
| | OR | 1.3.1 | SQL injection | T15, T29, T39, T48, T57, T64, T94, |
| | OR | 1.3.2 | SSRF | T94, T101, T120, |
| **2** | | **Network** | | |
| OR | 2.1 | Network Sniffing | | |
| | OR | 2.1.1 | ARP Spoofing | T1, T3, T4, T5, T6, T8, T9, T12, T17, T18, T21, T22, T23, T24, T25, T27, T28, T32,, T66, T67, T68, T71, T74, T76, T78, T79, T80, T82, T85, T86, T87, T95, T96, T97= |
| | OR | 2.1.2 | ICMP Redirect | T1, T3, T4, T5, T6, T8, T9, T12, T17, T18, T21, T22, T23, T24, T25, T27, T28, T32, T33, T34, T35, T37, T38, T41, T42, T45, T46, |
| OR | 2.2 | Packet Manipulation | | |
| | OR | 2.2.1 | ARP Spoofing | T1, T3, T4, T5, T6, T8, T9, T12, T17, T18, T21, T22, T23, T24, T25, T27, T28, T32,, T66, T67, T68, T71, T74, T76, T78, T79, T80, T82, T85, T86, T87, T95, T96, T97= |
| | OR | 2.2.2 | MITM | T1, T3, T4, T5, T6, T8, T9, T12, T17, T18, T21, T22, T23, T24, T25, T27, T28, T32, T33, T34, T35, T37, T38, T41, T42, T45, T46, T49, T51, T52, T53, T54, T55, T59 |
| OR | 2.3 | Denial of Service | | |
| | OR | 2.3.1 | SYN/UDP Flooding | T7, T10, T92, T102, T104, T107, T108, T113, T117, T125, T126 |
| | OR | 2.3.2 | Smurf Attack | T14, T16, T30, T31, T44, T50, T56, T58, T60, T62, T104, T107, T108, T113, T121, T122 |
| **3** | | **System** | | |
| OR | 3.1 | Arbitrary Code Execution | | |
| | OR | 3.1.1 | Buffer Over Flow | T11, T13, T36, T40, T43, T61 |
| OR | 3.2 | Remote Code Execution | | |
| | OR | 3.2.1 | Memory Corruption | T20, T26, T61, T84, T103, T109 |
| **4** | | **Hardware** | | |
| OR | 4.1 | Firmware Debugging | | |
| | OR | 4.1.1 | JTAG | T65, T69, T70, T83 |
| | OR | 4.1.2 | UART | T65, T69, T70, T83 |
| | OR | 4.1.3 | RS232 Port | T65, T69, T70, T83 |

## VII. Conclusion

We have schematically illustrated the data flow of a smart farm, and classified threats based on STRIDE. We also analyzed threats that could occur in the smart farm by creating an attack tree. Through this threat modeling process, the security requirements were finally derived.

This study was conducted similarly to the analysis of major threats that may exist in the existing information and communication infrastructure. To establish a customized security system for smart farms, a new paradigm must be presented based on big pictures including related industries, infrastructure, and stakeholders.

In addition, a comprehensive model and a security framework linked to various stages of smart agriculture and related industries are needed.

## Acknowledgment

All authors thanks to Korean Information Technology Research Institute (KITRI) and Best of the Best (BoB) 9th.

## References

[1] N. Zhang, M. Wang and N. Wang, “Precision agriculture – a worldwide overview,” in *Comput. Electron. Agric*., vol. 36, no. 2-3, pp. 113-132, Nov. 2002, doi: 10.1016/S0168-1699(02)00096-0.

[2] P. Reidsma, et al., “Sustainable agricultural development in a rural area in the Netherlands? Assessing impacts of climate and socio-economic change at farm and landscape level,” in *Agric. Syst.,* vol. 141, pp. 160-173, Dec. 2015, doi: 10.1016/j.agsy.2015.10.009.

[3] M. Kernecker, A. Knierim, A. Wurbs, T. Karus and F. Borges, “Experience versus expectation: farmer’s perceptions of smart faming technologies for cropping systems across Europe,” in *Precis. Agric.,* vol. 21, no. 1, pp. 34-50, Apr. 2020, doi: 10.1007/s11119-019-09651-z.

[4] S. Sontowski, et al., “Cyber Attacks on Smart Farming Infrastructure,” in *Proc. 6th IEEE Int. Conf. Collab. Internet Comput. (IEEE CIC 2020),* Oct. 2020.

[5] S. Linsner, R. Varma and C. Reuter, “Vulnerability Assessment in the Smart Farming Infrastructure through Cyberattacks,” in *38th GIL-Jahrestagung in Wien: Digitalisierung für landwirtschaftliche Betriebe in kleinstrukturierten Regionen - ein Widerspruch in sich,* Wein, Austria, Feb. 18-19, 2019. pp. 119-124.

[6] A. Boghossian, et al., “Threat to Precision Agriculture,” 2018 Analytic Exchange Program, USA, 2018.

[7] M. M. Jahn el at., “ Cyber Risk and Security Implications in Smart Agriculture and Food Systems,” Jan. 2019. [Online]. Available: https://jahnresearchgroup.webhosting.cals.wisc.edu/wp-content/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf (accessed Nov. 14, 2019).

[8] I. S. Kocher, C.-O. Chow, H. Ishii and T. A. Zia, “Threat Models and Security Issues in Wireless Sensor Networks,” in *Int. J. Comput. Theory Eng.,* vol. 5, no. 5, pp. 830-835, Oct. 2013, doi: 10.7763/IJCTE.2013.V5.806.

[9] J. West, “A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies,” in *J. Agric. Food Inf.,* vol. 19, no. 4, pp. 307-330, Feb. 20, 2018, doi: 10.1080/10496505.2017.1417859.

[10] K. Kim, el at., “What’s your protocol: Vulnerabilities and security threats related Z-Wave protocol,” in *Pervasive Mob. Comput.,* vol. 66. July 2020, doi: 10.1016/j.pmcj.2020.101211.

[11] K. K. Gon and K. S. Hoon, “Using Threat Modeling for Risk Analysis of SmartHome,” in *Proc. Symp. Korean Inst. Commun. Inf. Sci.,* 2015, pp. 378-379.

[12] I.-K. Oh, et al. “Derivation of Security Requirements of Smart TV Based on STRIDE Threat Modeling,” in *J. Korea Inst. Inf. Secur. Cryptol.,* vol. 30, no. 2, pp. 213-230, 2020, doi: 10.13089/JKIISC.2020.30.2.213.

[13] *Framework of smart greenhouse service*, Rec. ITU-T Y.4466, International Telecommunication Union, Geneva, Switzerland, Jan. 2020. [Online]. Available: http://handle.itu.int/11.1002/1000/14169

[14] M. S. Farooq, S. Riaz, A. Abid, K. Abid and M. A. Naeem, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," in *IEEE Access,* vol. 7, pp. 156237-156271, 2019, doi: 10.1109/ACCESS.2019.2949703.

[15] B. E. Storm, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington and C. B. Thomas, “MITRE ATT&CKTM: DESING AND PHILOSOPHY,” MITRE Corp., McLean, VA, USA, Tech. Rep. July 2018.

[16] L. Kohnfelder and P. Garg, “The threats to our products,” Apr. 1, 1999. [Online]. Available: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx

[17] A. Shostack, *Threat Modeling: Designing for Security,* Indianapolis, IN, USA: Wiley, 2014.

[18] M. Kamal, “ICS Layered Threat Modeling,” SANS Institute Reading Room, Jan. 22, 2019. [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/ics-layered-threat-modeling-38770

[19] A. S. Elmaghraby and M. M. Losavio, “Cyber security challenges in Smart Cities: Safety, security and privacy,” in *J. Adv. Res.,* vol.

5, no. 4, pp. 491-497, July 2014, doi: 10.1016/j.jare.2014.02.006.

[20] M. A. Hussain, H. Jin, Z. A. Hussien, Z. A. Abduljabbar, S. H. Abbdal and A. Ibrahim, "DNS Protection against Spoofing and Poisoning Attacks," *2016 3rd Int. Conf. Inf. Sci. Control Eng. (ICISCE),* Beijing, 2016, pp. 1308-1312, doi: 10.1109/ICISCE.2016.279.

[21] S. Neethirajan, "Recent advances in wearable sensors for animal health management," in *Sens. Bio-Sens. Res.*, vol. 12, pp. 15-29, Feb. 2017, doi: 10.1016/j.sbsr.2016.11.004.

[22] State-Federal Animal Disease Traceability Working Group, "Animal Disease Traceability," Animal and Plant Health Inspection Service, USA, Apr. 2018. [Online]. Available: https://www.aphis.usda.gov/publications/animal_health/adt-summary-program-review.pdf

[23] Activeherd, "Livestock Tracking System," NFC Group, 2018. [Online]. Available: https://www.tracks360.com/asset-tracking-solutions/assettracking-applications/livestock-tracking-system/

[24] "World Trade Statistical Review," World Trade Organization, 2017. [Online]. Available: https://www.wto.org/english/res_e/statis_e/wts2017_e/wts2017_e.pdf

[25] N. Kshetri, "The simple economics of cybercrimes," in *IEEE Secur. Priv.,* vol. 4, no. 1, pp. 33-39, Jan.-Feb. 2006, doi: 10.1109/MSP.2006.27.

[26] J. A. López, H. Navarro, F. Soto, N. Pavón, J. Suardíaz and R. Torres, "GAIA2: A multifunctional wireless device for enhancing crop management," in *Agric. Water Manag.,* vol. 151, pp. 75-86, Mar. 31, 2015, doi: 10.1016/j.agwat.2014.10.023.

[27] A. Kumar and P. Paul, "Security analysis and implementation of a simple method for prevention and detection against Evil Twin attack in IEEE 802.11 wireless LAN," *2016 Int. Conf. Comput. Tech. Inf. Commun. Technol. (ICCTICT),* New Delhi, 2016, pp. 176-181, doi: 10.1109/ICCTICT.2016.7514574.

[28] N. Pimple, T. Salunke, U. Pawar and J. Sangoi, "Wireless Security — An Approach Towards Secured Wi-Fi Connectivity," *2020 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS),* Coimbatore, India, 2020, pp. 872-876, doi: 10.1109/ICACCS48705.2020.9074350.