Designing a Secure Mobile Agent System

Name

Course

Institution

Date

# **Executive Summary**

Security assurance and risk assessment are essential processes, which can help an organization to evaluate the effectiveness of information system security controls and improve overall security posture and risk profile. This paper examines security problems related to mobile client application systems and the potential solutions for secure fault tolerance using the Amazon web Service console mobile application as a case study. The overarching contribution is the development of a secure fault tolerant design solution adapted to the organizational needs and a business continuity and disaster recovery plan adapted to the unique security threats. An extensive risk analysis is conducted based on the NIST Cybersecurity Framework and the design solution described consistent with the ISO 31000:2009/2018 standard for risk management process.

Table of Contents

[**Executive Summary** 2](#_Toc76640986)

[**1.** **Introduction** 4](#_Toc76640987)

[**1.1** **Statement of the Problem** 4](#_Toc76640988)

[**1.2** **Organizational Requirements** 4](#_Toc76640989)

[**1.3** **Purpose of the Plan** 5](#_Toc76640990)

[**1.4** **Scope of the Plan** 5](#_Toc76640991)

[**1.5** **Rationale of the Plan** 6](#_Toc76640992)

[**1.6** **Conclusion** 6](#_Toc76640993)

[**2.** **Review of Related Literature** 6](#_Toc76640994)

[**2.1** **Security Problem** 6](#_Toc76640995)

[**2.2** **Current Security Solutions and their Limitations** 8](#_Toc76640996)

[**2.3** **Summary of the Research Outcomes** 9](#_Toc76640997)

[**3.** **Risk Analysis** 10](#_Toc76640998)

[**3.1** **Risk Analysis** 10](#_Toc76640999)

[**3.2** **Value of Assets** 10](#_Toc76641000)

[**3.3** **Potential Loss Per Threat** 10](#_Toc76641001)

[**3.4** **Threat Analysis** 11](#_Toc76641002)

[**3.5** **Overall Annual Loss Per Threat** 13](#_Toc76641003)

[**3.6** **Risk Mitigation Strategies** 13](#_Toc76641004)

[**4.** **Environmental Diagrams** 14](#_Toc76641005)

[**4.1** **System and/or Network Architecture Diagrams** 14](#_Toc76641006)

[**4.2** **Security and Business Requirement Mappings** 15](#_Toc76641007)

[**4.3** **Information or Data flow Diagrams** 15](#_Toc76641008)

[**4.4** **SDL Threat Modeling Diagrams** 16](#_Toc76641009)

[**4.5** **Risk Matrix** 17](#_Toc76641010)

[**4.6** **Process Overview** 18](#_Toc76641011)

[**4.7** **Shared Resource Matrix** 19](#_Toc76641012)

[**4.8 Attack and/or Malicious mappings** 20](#_Toc76641013)

# **Introduction**

## **Statement of the Problem**

Mobile agent technology has emerged as a promising technology that can make it easier to deploy distributed systems, including cloud-based and sensor networks. The key benefit of this technology is that it provides an infrastructure for executing autonomous agents and allows transfer or migration between computers. Although not all applications for distributed systems need mobile agents, the technology is effective in implementing other tasks. However, mobility comes with inherent security and privacy issues. A typical mobile agent platform consists of the mobile agents that define the behavior of software agents and runtime systems, which support the execution and migration of mobile agents. Protecting these components from their execution environments or agencies is a complex undertaking. Potential security threats include code manipulation, Denial of Service (DoS) attacks, and privacy breach. This work focuses on the security of the AWS console mobile application. The project entails an examination of the security-related problems, the possible security solutions, and the feasibility of a design solution that enhances the CIA-triad of confidentiality, integrity, and availability.

## **Organizational Requirements**

The AWS console mobile application allows users to view and manage resources. The application is optimized for iOS and Android mobile devices. Amazon has announced several features that are essential for computing, such as the ability to manage EC2 instance and performing basic operations like rebooting and terminating services. another crucial factor for the application is security (Amazon Web Services, Inc., 2016). Amazon provides important guidelines, best practices, and recommendations on how to secure the device with a password and using “Multi-Factor Authentication (MFA)”. Recently, Amazon created a new feature called multiple identities, which allows users to add multiple accounts and switch between them seamlessly. The key requirement for users to deploy this application is the iOS 12.0 and Android 8.0, and above (Amazon Web Services Inc., 2021). According to the company, security is a shared responsibility between the company and customers. The company is responsible for protecting the infrastructure that is supporting the cloud services. On the other hand, users have responsibility over the sensitivity of data and compliance with relevant laws and regulations.

* Overall, Amazon recommends the following requirements:
* MFA with each user account
* SSL/TLS for communications with AWS resources
* Using API and user activity logging with AWS CloudTrail
* Strong encryption and default security controls

## **Purpose of the Plan**

The purpose of this document is to develop an information security plan identifying the current security-related problems with the AWS Console Mobile Application. The project aims to achieve two goals. First, a comprehensive review of the security problem is described based on the technology used, people involved, business processes, and organizational context. Secondly, proper security solutions are reviewed together with their limitations using the principles of secure fault tolerance. Thirdly, a design is proposed using best practices for a secure fault tolerant solution. Lastly, a business continuity and disaster recovery plan is proposed for the final solution.

## **Scope of the Plan**

The scope of the plan includes a review of related literature, risk analysis, and design description.

## **Rationale of the Plan**

With the growing cybersecurity threats facing information systems, it is imperative for business leaders and managers of organizations to use security assurance and risk assessment as tools to improve the security and risk profile of their organizations. Various best practices, standards, and methods have been described for security and risk assessments, but there is no universally accepted framework for conducting security assessment assurance and risk assessments. Moreover, organizational contexts differ in terms of the technologies, people, and processes. Since mobile agent systems have unique security vulnerabilities and threats, security assessment assurance and risk assessment is essential to evaluate security components at the technical level.

## **Conclusion**

Although mobile agent technology is a promising a technology for distributed computing, security, privacy, and trust issues abound, which limits widespread application of these systems. Various security countermeasures and best practices have been described, but differences in organizational contexts means that some solutions may not work in certain contexts. A comprehensive approach to secure system design should involve risk assessment to evaluate potential security threats and determine the mitigation strategies.

# **Review of Related Literature**

## **Security Problem**

Security has been an issue since the usage of computational systems and the first computer networks. Even after about three decades of research and engineering design, mobile applications are still at risk. Address the security problem requires an understanding of the dynamic nature of security and the context in which an information system operates. Mobile agents provide a powerful paradigm for developing complex applications. These applications must process large amounts of distributed information. yet new security requirements appear, some of them inherent in the nature of agents and others due to the vulnerabilities associated with the mobility features and functions.

One of the classic approaches is to define the security of information systems is through the CIA-triad model, which covers three categories: confidentiality, integrity, and availability. Confidentiality refers to the protection of data and other computing resources from unauthorized access or use. Integrity refers to protection of data from unauthorized modification to ensure the data is correct and reliable. On the other hand, availability refers to the capability of legitimate users to access the system and computing resources whenever they need to perform a task.

The AWS mobile application platform has security issues related to the CIA-triad. In terms of the confidentiality, the key security problem is how to define who has the responsibility to define access control levels and monitor activities across the network (Zhou et al., 2019). In terms of integrity, there is also the issue of protecting the system in multi-tenant infrastructures, which impose higher risks of data breaches. Securing user application data and protecting privacy is important in creating customer trust (Aliyu et al., 2020). The problem with the current architecture of mobile computing is that raises issues over the security of users, the security for cloud data centers, and the security for mobile data. according to Hayes et al. (2020), protection of Personally Identifiable Information (PIA) is a challenge in mobile applications. Another challenge is complying with established standards and regulations. Currently, two global standards for multi-agent systems exist: the “Mobile Agent System Interoperability Facility (MASIF)” and the “Foundation for Intelligent Physical Agents (FIPA)”. MASIF provides interfaces between agent systems allowing migration across platforms and agents, while FIPA relates to remote communication services.

## **Current Security Solutions and their Limitations**

There are several solutions to specific security issues in mobile agent systems. Broadly the solutions can be categorized into three group: organizational approaches, which avoid the security problem and assume a closed environment, specific problems solutions, which claim to solve specific security problems, and holistic approaches, which aim to protect the system from any form of attack. Since organizational security approaches avoid the security problem, this paper addresses specific problem solutions and the holistic approaches.

Mobile agent systems must meet basic security requirements, such as authentication, confidentiality, availability, and non-repudiation. Authentication refers to the verification of the identity of an entity accessing a system. In mobile agent systems, the authentication process requires agents and platforms to be able to authenticate each other, which means that the agent should know the executing environment and *vice versa.* The decision on whether to grant a request is known as authorization, and it involves using password protection and digital signatures. A mobile agent system should also meet the principles of confidentiality, privacy, and anonymity. Confidentiality means that only authorized entities can access data. Various methods and techniques are used to ensure confidentiality, such as encryption. Another basic security requirement is accountability and non-repudiation. The system should record security related activities for auditing purposes. Moreover, a mobile agent platform should provide availability of data and services.

There are two broad security techniques for mobile applications explored in the literature: detection techniques and prevention techniques. Detection techniques aim to determine when an agent changes. Detection techniques vary depending on the scope of detection and whether they involve automatic detection or not (Jain & Saxena, 2016). These systems are broadly called intrusion detection systems (IDS), which can be categorized into two: “Network Intrusion Detection Systems (NIDS)” and “Host-based Intrusion detection Systems (HIDS) (Jain & Saxena, 2016). Further, IDS can be categorized into anomaly or misuse, depending on the network events detected. For instance, anomaly IDS identifies possible security breaches, logs the information, and triggers alerts. On the other hand, misuse-based IDS take specific action upon detecting a potential security threat. The idea is that using agent can improve the performance of IDS.

Prevention techniques aim to leverage the mobile agent security to safeguard against tempering attacks. This approach makes it difficult to access or modify the code without authorization. However, prevention techniques vary depending on the goal of prevention. For instance, the prevention may involve protecting the entire agent or part of it or trusting some functionalities. Some of the proposed solutions focus on creating trusted environments installed with temper-proof hardware computing at the hosting platform. Others use the concept of encrypted functions to prevent code tempering and data breach (Kamouri et al., 2020).

## **Summary of the Research Outcomes**

Overall, the literature review has established two general approaches to security involving mobile agent systems: detection approaches and prevention approaches. Detection approaches rely on IDS. On the other hand, prevention mechanisms use mobile agent security level, including trusted environments installed with temper-proof hardware computing at the hosting platform. Others use the concept of encrypted functions to prevent code tempering and data breach.

# **Risk Analysis**

## **Risk Analysis**

Security solutions that rely on detection approaches security risks. Firstly, IDS systems are prone to effects of noise, which limit the effectiveness of the security mechanism. These systems are prone to high false alarm rate due to software bugs creating incomplete packets, corrupt DNS data, and other packet data that is interpreted as malicious (Khraisat et al., 2019). Other security solutions based on the detection approach lack adequate accuracy and precision due to high false-negative rate. The false negative refers to a situation where the security system identifies an event as normal when the event is actually associated with an attack (Khraisat et al., 2019).

For systems that rely on preventive approaches, such as cryptographic traces, there is the inherent risk of using week cryptographic keys, which are easy to guess or break. While cryptographic keys ensure confidentiality and integrity, they do not provide non-repudiation and availability. similarly, security solutions based on trust do not provide confidentiality, integrity, nor availability.

## **Value of Assets**

The assets requiring protection are information assets, including data, code, and information systems. The value can be assessed in terms of the intrinsic value, the business value, and the performance value. In terms of the intrinsic value, the data is correct and complete. In terms of business value, the data contained in the system is useful for business purposes. Lastly, the asset is a key business driver.

## **Potential Loss Per Threat**

Potential loss in risk management refers to the possibility of loss, including financial loss. The following are the possible threats and the potential loss per threats.

Table 1. Potential loss per threat

|  |  |
| --- | --- |
| Threat | Potential Loss |
| Masquerading | Financial loss |
| DoS | Interruptions of business leading to loss of productivity |
| Eavesdropping | Loss of intellectual property rights (IPR) such as codes |
| Unauthorized access | Data and software loss and fines and penalties |

## **Threat Analysis**

According to the NIST Joint Task Force Transformation Initiative (2012) guidelines for risk assessment, the procedure should involve identifying threat events, vulnerabilities, and the likelihood that identified threats could be successful. Table 2 shows a threat matrix summarizing the threats and the vulnerabilities they can exploit.

Table 2. Threat analysis

|  |  |  |
| --- | --- | --- |
| Threats/ | Description of the Vulnerability | Vulnerabilities |
| Masquerading | An agent platform can masquerade as a legitimate platform an attempt to deceive the system | Unsecure Internet-based services |
| DoS | A malicious platform can issue massive requests and overload the system or consume excessive amounts of computing resources like memory | Application architecture |
| Unauthorized access | An agent can circumvent access controls or modify code and data | Physical security and insecure wireless networks |
| Eavesdropping | An agent can eavesdrop communications using Man-In-The-Middle attack or other methods | Internet-based services |

## **Overall Annual Loss Per Threat**

Table 3 gives a breakdown of the estimated annual loss assuming that the threats occur twice in a year and only affect the mobile client system.

Table 3. Overall annual loss per threat

|  |  |  |
| --- | --- | --- |
| Threat | Potential Loss | Annual Loss ($) |
| Masquerading | Financial loss | 4500 |
| DoS | Interruptions of business leading to loss of productivity | 12000 |
| Eavesdropping | Loss of intellectual property rights (IPR) such as codes | 6000 |
| Unauthorized access | Data and software loss and fines and penalties | 10,000 |
| Total Loss |  | 32500 |

## **Risk Mitigation Strategies**

The next step for the organization is to determine which vulnerabilities will be mitigated or accepted. There are strategies to risk mitigation: risk acceptance, avoidance, transfer, and reduction.

Table 4. Risk mitigation strategy

|  |  |  |  |
| --- | --- | --- | --- |
| Threat | Potential Loss | Mitigation Strategy | Measures/Actions |
| Masquerading | Financial loss | Risk reduction | Encryption and authentication |
| DoS | Interruptions of business leading to loss of productivity | Risk avoidance | Intrusion detection |
| Eavesdropping | Loss of intellectual property rights (IPR) such as codes | Risk reduction | Encryption and authentication |
| Unauthorized access | Data and software loss and fines and penalties | Risk avoidance | Antimalware |

# **Environmental Diagrams**

## **System and/or Network Architecture Diagrams**

The proposed solution focuses on protecting mobile agents from malicious platforms and other attacks to ensure overall integrity of the system. The system integrates two security mechanisms: cryptographic component and SOS agent (See Figure 1).

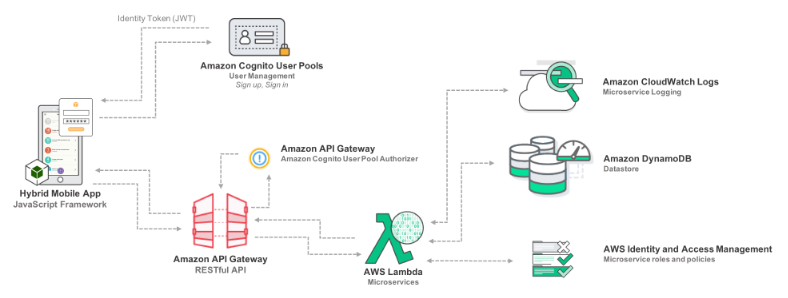


Figure 1. Proposed architecture of the mobile agent system

## **Security and Business Requirement Mappings**

The cryptographic method ensures effective security and data transmission by ensuring that it can trace the agent’s movements. Each host should have a private key (Ks) and a public key (Kp) used for encryption and decryption of messages, respectfully. The message consists of a code for execution.

## **Information or Data flow Diagrams**

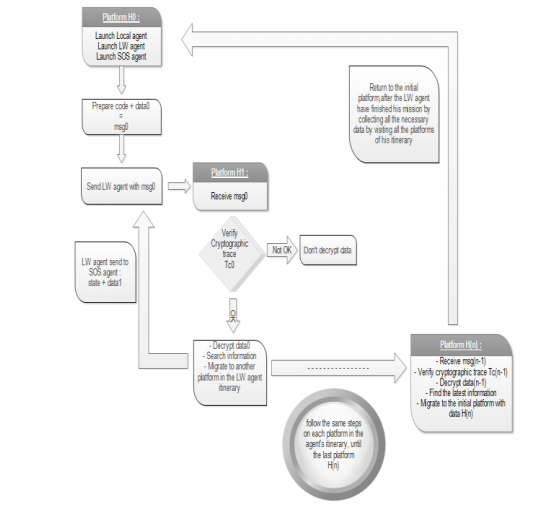


Figure 2. Illustration of the mobile agent data transmission process

## **SDL Threat Modeling Diagrams**

Threat modeling is a systematic process for identification of potential security threats and vulnerabilities and prioritization of mitigation measures to protect IT assets. The threat modeling process involves four distinct steps: decomposition of the application or infrastructure, determination of security threats, determination of countermeasures (mitigation), and ranking of the security threats. However, different threat modeling methodologies exist, such as the NIST model, OCTAVE, and STRIDE. The threat modeling envisaged in this work is based on the NIST model of threat modeling, which consists of four steps: characterization of the system and data, identification and selection of attack vectors, characterization of security controls, and analysis of the threat model (Souppaya & Scarfone, 2016). The NIST Cybersecurity Framework recommends five steps: identify, protect, detect, respond, and recover.

Figure 3. The NIST Cybersecurity Framework

## **Risk Matrix**

A risk matrix is a tool for determining the risk to information assets and identifying the potential impact of security threats based on the scale of severity.

Table 5. Risk-Level Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| Threat Likelihood | Impact | | |
| High (1.0) | Low  10 x 1.0 = 10 | Medium  50 x 1.0 = 50 | High  100 x 1.0 = 100 |
| Medium (0.5) | Low  10 x 0.5 = 5 | Medium  50 x 0.5 = 25 | Medium  100 x 0.5 = 50 |
| Low (0.1) | Low  10 x 0.1 = 1 | Medium  50 x 0.1 = 5 | 100 x 0.1 = 10 |

N.B. – High (> 50 to 100), Medium (>10 to 50); Low (1 to 10)

## **Process Overview**

The ISO 31000 (2009) Standard prescribes a process for risk management involving consulting, communicating, establishing the context, and identifying, analyzing, evaluating, treating, and monitoring and review of risks (See Figure 4):

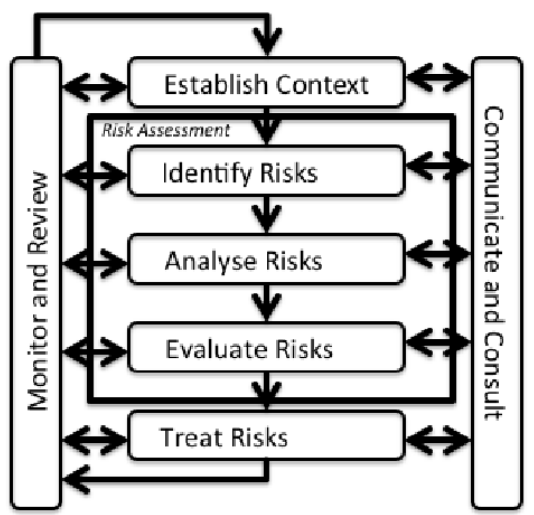


Figure 4. ISO 31000:2009 Risk Management Process (

The ISO 31000:2009 process has been replaced with the ISO 31000: 2018, which includes recording and reporting as part of the risk management process.

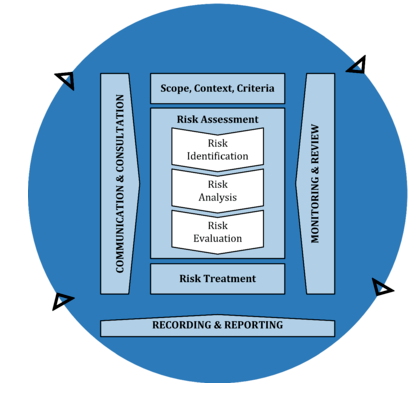


Figure 5. The updated risk management process according to ISO 31000:2018

The overall idea is that the risk management process is an integrated part of decisions making, with implications for organizational structure, operations, and processes.

## **Shared Resource Matrix**

The Shared resource matrix recognizes the importance of addressing the storage and timing requirements when performing a security analysis of a computer system (Kemmerer, 1983). The Table shows the application of the Shared Resource Matrix to the design of a secure mobile client system.

Table 6. Shared Resource Matrix

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Resource Attribute/Primitive | | Write File | Read File | Lock File | Unlock File | Open File | Close File | File Locked | File Opened |
| Process | ID |  |  |  |  |  |  |  |  |
| Access rights |  |  | R |  | R |  | R | R |
| Buffer | R | M |  |  |  |  |  |  |
| Files | ID |  |  |  |  |  |  |  |  |
|  | Security classes |  |  | R |  | R |  | R | R |
| Locked by | R |  | M | R |  |  |  |  |
| Locked | R |  | R,M | R, M | R |  | R |  |
| In-Use Set |  | R | R |  | R,M | R, M |  |  |
|  | Value | M | R |  |  |  |  |  |  |
| Current Process | R | R | R | R | R | R | R |  |  |

N.B. R = operation reference, M = operation modifies the attribute under certain circumstance

## **4.8 Attack and/or Malicious mappings**

A potential malicious event is a Distributed Denial of Service (DDoS), which occurs when an attacker exploits security vulnerabilities to control devices and use the compromised devices as botnets to send malicious service requests and render the system unavailable to legitimate users. The diagram below describes the encrypted message flow between the agents. The Local Agent 9LW) migrates to another platform (H1) to execute a task while the SOS Agent awaits the message using a Time (T). The receiving agent receives the message from the sender and recalculates the timer before waiting for its message. Alternatively, if the timer elapses and the sending agent has not send the message, the receiving agent sends an alert to trigger deployment of a new sending agent.

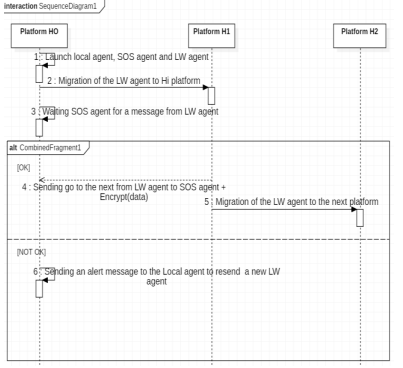


Figure 7. Encrypted message flow between the agents

References

Aliyu, A. Abdullah, A. H., Kaiwartya, O., Madni, S. H., Joda, U. M., Ado, A., & Tayyab, M. (2020). Mobil cloud computing: Taxonomy and challenges. *Journal of Computer Networks and Communications,* 1-23. https://doi.org/10.1155/2020/2547921

Amazon Web Services, Inc. (2016, December 14). AWS Mobile App Backend. Retrieved from https://d0.awsstatic.com/aws-answers/aws-mobile-app-backend.pdf

Amazon Web Services, Inc. (2021). AWS Console Mobile Application – User Guide. Retrieved from https://docs.aws.amazon.com/consolemobileapp/latest/userguide/console-mobile-app-guide.pdf

Hayes, D., Cappa, F., & Khac, N. A. L. (2020). An effective approach to mobile device management: Security and privacy issues associated with mobile applications. *Digital Business, 1*(1). https://doi.org/10.1016/j.digbus.2020.100001

ISO 31000:2009 Risk Management – Principles and Guidelines. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

ISO 31000:2018 Risk Management – Principles and Guidelines. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Jain, C. & Saxena, A. (2016). General Study of Mobile Agent Based Intrusion Detection System (IDS). *Journal of Computer and Communications,* 4, 93-98. doi: 10.4236/jcc.2016.44008.

Joint Task Force Transformation Initiative (2012). Guide for conducting risk assessments. NIST SP 800-30. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Kamouri, S. A., Moukafih, N., Orhanou, G., & Elhajji, S. (2020). Mobile agent security based on cryptographic trace and SOS agent mechanisms. *Journal of Communications, 15*(3), 221-230.

Kemmerer, R. A. (1983). Shared resource matrix methodology: An approach to identifying storage and timing channels. *1*(3), 256-277. https://doi.org/10.1145/357369.357374

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniues, datasets, and challenges. *Cybersecurity,* 2(10), 1-22. https://doi.org/10.1186/s42400-019-0038-7

Souppaya, M., & Scarfone, K. (2016). Guide to data-centric system threat modeling. NIST Special Publication 800-154. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800\_154\_draft.pdf

Zhou, W., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal, 6*(2), 1606-1616. https://doi.org/10.1109/JIOT.2018.2847733