GUIDELINES ON SECURITY BEST PRACTICES IN CLOUD OF THINGS (CoT)

Authored by

AISHWARYA SAVANUR

Project report

Submitted to the Faculty of Graduate Studies,

Concordia University of Edmonton

In Partial Fulfillment of the

Requirements for the Final

Research Project for the Degree

MASTER OF INFORMATION SYSTEMS ASSURANCE MANAGEMENT

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

December 3, 2020

GUIDELINES ON SECURITY BEST PRACTICES IN CLOUD OF THINGS (CoT)

Aishwarya Savanur

Approved:

Bobby Swar [Original Approval on File]

Bobby Swar Date: December 7, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci Date: December 14, 2020

Dean, Faculty of Graduate Studies

Abstract

Cloud of Things (CoT) is the amalgamation of Cloud Computing (CC) and Internet of Things (IoT) where these two diverse technologies support each other for high-performance smart applications such as smart cities. IoT systems generate an enormous amount of data via sensors/actuators with limited storage capacity, cloud computing with scalable and elasticity capabilities plays a pivotal role in enabling and meeting business needs. Although CoT systems have proven to be beneficial which is evident that the IoT Cloud platform market worth has been increasing and supporting the business to scale, this also raises many security and privacy challenges. Most of the attacks/risks which are common in cybersecurity space also apply in CoT systems such as Distributed Denial of Service (DDOS), Man in the middle attacks, data leakage, unauthorized access, but with greater attack surface area. The objective of this research is to educate learners about attacks associated with CoT deployment and identify best practices to aid the organizations to attenuate the security and privacy risks which is one of the gaps. To achieve the research objective, attacks associated with CoT are identified and mapped with NIST 800-53 R5 document. In addition, security best practices are reviewed and collated from security frameworks, standards, and guidelines documents to address each of the identified attacks.

Keywords: Cloud Computing (CC), Internet of things (IoT), Cloud of Things (CoT), CoT Security and Privacy Risks, CoT Security, and Privacy Controls.

Table of Contents

List of Figures

Figure

Introduction

Cloud of Things (CoT) is the integration of Cloud Computing (CC) and Internet of Things (IoT), where these two diverse technologies support each other for high-performance smart applications such as smart cities. In this modern era, CoT has drastically changed the way of the ubiquitous computing world. The change can be noticed as CoT emerged as a solution for several problems faced by Cloud Computing and IoT technology namely storage capacity, energy efficiency, computational capabilities. In addition to solving the problems of IoT and Cloud Computing, CoT has facilitated the users to experience fast, real-time access as well as dynamic monitoring (Ari et al., 2019). Some of the businesses have adopted CoT such as the telecommunication industry adopted smartphones, the healthcare industry integrated smart health applications as well as telemedicine capabilities, and others.

The integration of IoT devices and the cloud environment offers numerous benefits to the business (Atlam, 2017). One of the major advantages IoT achieves upon integration with cloud computing is massive storage capacity utilizing scalable resources in the cloud. Furthermore, cloud computing provides additional benefits of processing capabilities to the resource constrained IoT devices. Cloud computing also offers an efficient way of managing all the communication applications and portals. Cloud computing also enables the users to have fast, real-time access as well as dynamic monitoring on the applications in use.

CoT devices have experienced a data breach that exposed 4.1 billion records in the second quarter of 2019 (Risk Based Security, 2019). One of the major reasons for the data breach is that CoT has a greater attack surface that leads to exploiting the known

vulnerabilities in the cloud environment and IoT devices (Gruschka & Jensen, 2010; Hossain, Fotouhi, & Hasan, 2015). The exploitation of vulnerabilities poses the risk of financial, legal, and reputational loss to the business. As the utilization of CoT systems is increasing incrementally and businesses are steering towards adopting CoT systems needed for a guideline document that specifies security best practices to secure CoT systems. Therefore, the research objective is to propose a guideline document outlining security best practices that enhances CoT systems security for the organizations that have integrated their business with CoT systems or planning to adopt CoT. To achieve this objective a literature review is conducted in order to identify attacks and threats that are associated with CoT, further the identified attacks and threats are addressed and mapped with appropriate security and privacy control from NIST 800-53 R5. Standards, frameworks, and guidelines pertaining to Cloud and IoT have been reviewed to propose CoT security best practices and to address each of the attacks and threats.

The organization of this research paper is as follows: Firstly, a literature review was conducted to understand CoT architecture, several common attacks targeting CoT devices are identified and are mapped with security and privacy controls from NIST 800-53 R5. Standards, frameworks, and guidelines pertaining to Cloud and IoT have been reviewed to propose security best practices to secure CoT systems. Secondly, the methodology section can be found which includes research scope, research limitation, research questions, and research deliverable. Furthermore, analysis and discussion of the results section are included which focus on identifying security best practices of CoT devices based on standards, frameworks, guidelines of IoT, and cloud computing. In the last section result, conclusion, and recommendations for future work have been discussed

that entails how the security best practices of CoT devices can be beneficial for the organizations planning to use CoT systems.

Literature Review

This section encompasses scholarly articles about CoT architecture, CoT related attacks and threats and cloud computing and IoT related standards, guidelines, and frameworks.

CoT Architecture

The CoT architecture proposed by Cloud Customer Standard Council is the amalgamation of Cloud and of IoT components that contains user layer, edge tier, platform tier, and enterprise tier (Daly et al., 2017). The tiers of the architecture as mentioned in the Cloud Customer Standard Council (Daly et al., 2017) is described below. *Figure 1*. provides a more detailed view of components, subcomponents, and relationships for a cloud based IoT architecture.

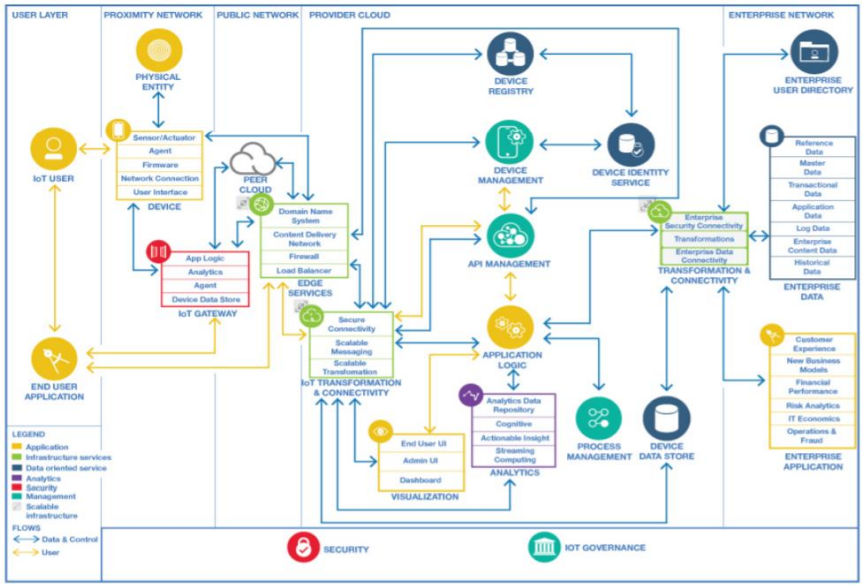

Figure 1. Cloud Architecture for IoT (Daly et al., 2017).

- The user layer is the first tier which is composed of IoT users utilizing the end-user applications such as smart health, logistic based application. All the end-user applications are domain-specific applications running on a variety of IoT devices. The data generated from the IoT devices hosting the applications are consumed by the edge.
- The edge-tier includes Proximity Networks and Public Networks where data is collected from end devices and transmitted to the platform tier. Proximity networks are one of the critical components of the CoT architecture that comprises physical entities such as sensors, firmware, network connectors, and user interface tier (Daly et al., 2017). Data collected from the user layer by physical entities flows through the IoT gateway. The IoT gateway is responsible for connecting end-user applications to the edge services. IoT gateways comprise application logic that filters and allows appropriate data to flow towards the respective endpoint. In addition, IoT gateways also contain analytics capabilities locally that aids in quantifying the data flow and enable to make decisions based on analytics results. Furthermore, IoT gateways are connected to a peer cloud that provides domain name services, firewalls, load balancers, and content delivery networks.
- The Platform tier is the next tier after the edge-tier which composes of the provider cloud that is responsible for receiving, processing, and analyzing data flows from the edge tier and connects to the enterprise tier (Daly et al., 2017). The provider cloud in the platform tier is composed of device registries that are a container of devices with shared properties. Registries are crucial in this

environment and must be created to connect IoT devices to the cloud environment. In addition to the registry which helps to connect, the provider cloud also contains the device management solution that oversees the devices but is not limited to configurations, settings, firmware upgrades. The device management is connected to the IoT transformations and connectivity center that ensures secure connections from IoT devices to the cloud environment and the device identity service. Furthermore, device management is connected to the API Management solution which consists of a set of tools to enable developers for building, analyzing, operating, and scaling APIs in the cloud environment. Another key component is virtualization that allows users to interact with enterprise applications. Lastly, the provider cloud also offers a data storage facility and managing the processes required by the business to operate.

- The last layer is the enterprise tier also known as enterprise network is composed of enterprise data, an enterprise user directory, and enterprise applications (Daly et al., 2017). The data flow in the enterprise network is controlled via transformation and connectivity components. The enterprise data holds all the data collected which is not limited to reference and historical data, monitor and log data, metadata, application, and enterprise content data, and so on. Furthermore, the enterprise applications are hosted in this tier comprising of some examples such as customer experience applications, new business models, financial performance and analytics, risk analytics and IT economics, operations, and fraud.

Common Attacks and Threats related to CoT

In this section, common attacks and threats related to CoT are identified through literature review leading to loss of availability, confidentiality, and integrity.

Distributed denial of service (DDoS). DDoS attacks have been hindering the regular business processes since internet services have been utilized. DDoS attacks are targeted to make IoT devices bot by taking complete control over devices (Ari et al., 2019). Attackers maliciously launch attacks and one of the common techniques is malicious code injection in the kernel of IoT devices to transform devices into a bot and once the IoT devices are controlled, simultaneous attacks are launched to bombard the connected cloud component to cripple the business. These attacks nearly halt the cloud platform to service legitimate IoT devices. These attacks are disastrous as in CoT a public cloud platform is mostly leveraged which is servicing multiple businesses. Therefore, the cloud platform which was supposed to be utilized for provisioning multiple businesses is incapacitated due to DDoS attacks.

Eavesdropping. Roman, Zhou & Lopez (2018) explains that the eavesdropping attacks can be launched by compromising the network of CoT. The concept of these attacks is to intercept traffic to gain sensitive knowledge about the architecture initially. Once the malicious actors have enough knowledge about the architecture other structured attacks can be launched. Therefore, eavesdropping is successful only when an attacker can gain control over communication channels and can perform exploitation.

Man-in-the-middle (MITM) attack. Ari et al., (2019) explains that MITM is one of the most common types of cyber-attacks that allow an attacker to eavesdrop on the communication between a legitimate sender and a legitimate receiver. Attacks secretly

relay the messages between communicating nodes and replace the packets with fraudulent packets. This mechanism fools the communicating nodes into believing that the falsely created packet is legitimate. MITM also leads to structured attacks such as session hijacking where the session is hijacked similarly.

Replay attack. A replay attack is a network layer attack that occurs when a malicious actor can eavesdrop on a network communication followed by intercepting it, for sending manipulated packets to fool the receiver into performing the activities not intended by the victim (Ari et al., 2019). This attack can be used to successfully gain unauthorized access to the network, steal sensitive data, and even causing system failures

Device capture. An unstructured attack where the node is compromised at the physical level either by an external attacker or a malicious insider. The adversary initiates the attack by capturing the nodes and using sniffers extracting sensitive information (Alaba et al., 2017). Also, this sensitive information is transmitted and securely stored in the attacker's system.

Side-channel attack. A side-channel attack aims to steal sensitive information about the system architecture and CoT architecture is exposed to attackers (Ari et al., 2019). Side-channel attacks pertain to cryptographic operations, computing cycle, resource allocation, and so on. The sensitive information is collected and used for developing lethal malware and spreading in the network.

Deployment of unauthorized device. Deployment of an unauthorized device occurs when a malicious device is connected to the network which could cause the exposure of sensitive information to adversaries (Ari et al., 2019). This aims to

maliciously connect the device to the network and gain information about the network, adjacent nodes, and other connectivity. This information can be used for reconnaissance and develop complex attacks to cause either system failure or data leakage.

Key compromisation and the breakage of cryptographic protocols. Insecure key management and using weak encryption methods is a risk leading to data leakage of sensitive information. Sometimes developers use weak encryption keys or methods and tend to store the keys in the config file or codebase in plain text (Alaba et al., 2017). This can result in data leakage if exposed to malicious actors

Data loss and leakage. In CoT, systems data is hosted on the cloud platform where if not securely configured can result in data loss and breaches (Callegati et al., 2018). Few examples of poor configurations are access controls not following the principle of least privilege and role-based access controls leading to data loss by malicious insiders or attackers who have managed to take over a user account in the cloud platform, weak encryption algorithms, not prohibiting 0.0.0.0/0 on a network level, not isolating the resources and so on.

Spoofing attack. A spoofing attack is a network layer attack that targets to impersonate legitimate devices. In a Spoofing attack, a malicious attacker spoofs the identity of different devices on the network to launch attacks against network nodes. The spoofed target is malevolently utilized to target other network nodes for spreading malware and to launch DDoS attacks. Spoofing attacks are an attack that is used to first take control over multiple devices and then gain trust among other network nodes (Callegati et al., 2018). As the target is spoofed, other devices in the network trust the

compromised device, and some of the access controls are bypassed by the bad actors. This allows the attacker to compromise the whole network and launch much more catastrophic attacks.

Weak encryption keys. The developer is forced to incorporate weak cryptographic keys for data protection due to the limited resources of IoT devices. This leads to keys been compromised easily by the attackers by sophisticated deciphering mechanisms out of which one is chosen as the ciphertext attack (Zhang, Zheng, & Deng, 2018). In this attack, the cryptanalyst gathers information by obtaining the decryption keys from the chosen ciphertexts. This strategy leads to the adversary attempt to recover the hidden secret key used for decryption successfully.

Privileged access. Privileged Access is caused commonly when a privilege escalation attack is successful or trusted insiders decide to become rogue. A privilege escalation attack is also successful by taking advantage of programming errors and design flaws. These flaws are utilized to grant the attacker elevated access or unauthorized access to critical resources (Callegati et al., 2018).

Identity theft. Identity theft is carried out by the attacker from gaining personal information from a valid user (Modi, Patel, & Borisaniya, 2013). This information that is gained is used to get unauthorized access to restricted services and resources. The attacker performs malicious actions on behalf of the victim and the victim is held accountable for the attacker's actions.

Insecure APIs. This is one of the top threats in cloud architecture when integrated with IoT devices. The threat is caused as the cloud provider distributes a set of APIs that

helps consumers to retrieve data and get access to other services (Ari et al., 2019). Unfortunately, APIs are not securely developed and not protected to limit access to legitimate users. Therefore, it leads the attacker to exploit these unprotected APIs.

Malicious insider. An insider attack is a malicious attack on a system by an employee of the targeted environment. The insider has prior knowledge and insights about the environment which makes it easy to compromise sensitive systems (Ari et al., 2019).

Shared technology issues. There are many shared resources in a CoT system. These resources might be used via virtualization through multi-tenancy architecture (Alaba et al., 2017). This might allow access to the virtual machine (VM) of another user. This VM Monitor can have vulnerabilities and a malicious user could exploit to gain access to another user's VM.

Data breach due to vulnerabilities in web applications. Data breach is caused due to vulnerabilities in the application. One of the most common attacks is the zero-day attacks (Subashini, & Kavitha, 2011). In zero-day, attacks, novel vulnerabilities are exploited leading to zero-day attacks that take the organizations by surprise as the systems are unpatched. To protect from zero-day attacks, organizations must ensure regular patching procedures are implemented to prevent hackers from exploiting vulnerabilities and causing a massive data breach.

Unnoticed capture and unaware identification. CoT devices are deployed to collect data about users in an extremely discrete way from a small size camera or a small size sensor. This is a major privacy issue as data is captured without the consent of the

users (Callegati et al., 2018). As the users are unaware, this is a privacy issue that must be addressed.

Lack of transparency. The major issue is when the data collected from users are uploaded to the cloud (Zhang, Zheng, & Deng, 2018). Sometimes the user has no or limited control over data location and how data is being used. The ubiquitous sensing process which captures data makes it very difficult for the users to express their consent regarding data collection or what to do with such collected data while it is processed, analyzed, presented, and shared. Without granular controls, it is difficult to limit access to sensitive data to protect the privacy of users.

Unforeseen inference. An attacker is capable to access data from different sensors using the extensive computing power of the cloud. These privacy issues are a counter-use of cloud resources or invade the privacy of users. Furthermore, cybercriminals are not unfortunately the only ones that pose a privacy threat utilizing this strategy (Ari et al., 2019). It is more often the rival companies that use inference techniques to invade the privacy of other companies. The organization usually use this private information to target users appropriately.

Frameworks to Secure CoT

This section consists of several frameworks proposed to secure CoT architecture by different researchers:

Securing CoT using CUPS framework. Belguith, Kaaniche, and Russello (2019) proposed a CUPS, an Attribute-Based Encryption (ABE) framework for the opportunistic cloud of things applications. The goal is to protect the data during the decryption process

at edge nodes and decrease computation overhead on the user side. Besides, CUPS have the capability of providing the access policy update feature without involving a proxy server, without re-encrypting the enciphered data contents, and re-distributing the user's secret keys. *Figure 2* represents the CUPS model below:

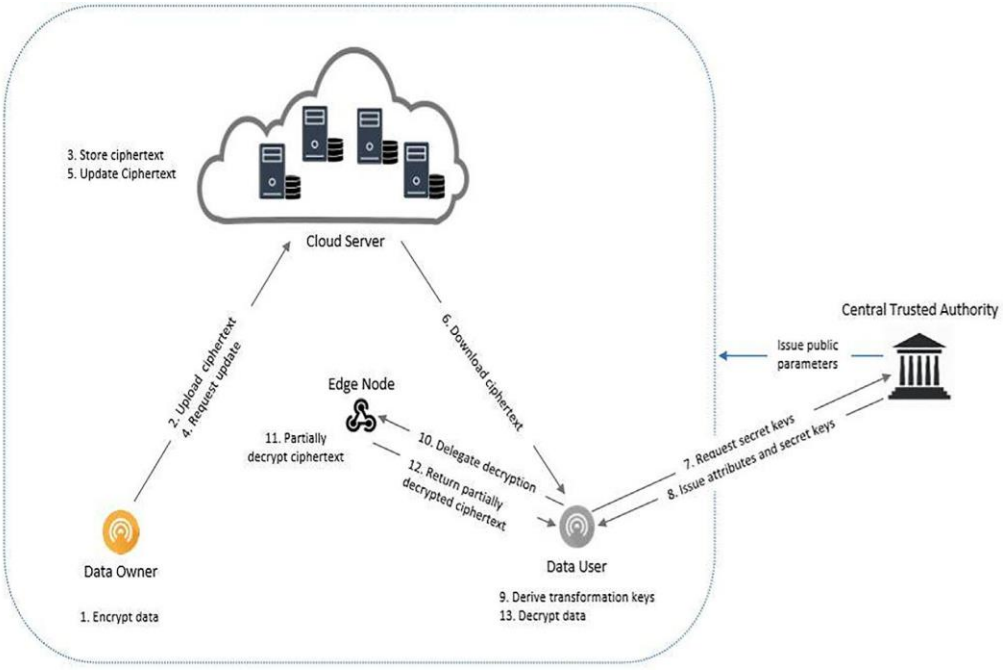

Figure 2. CUPS Architecture (Belguith, Kaaniche, and Russello, 2019)

CoT Secure Framework using the Three-Tier Model. Daneshgar, Sianaki, and Ilyas (2019) proposed a CoT framework based on a three-tier model. The framework proposed by the researchers provides a data security architecture for CoT systems that provides reliability, robustness, and security.

i) Tier 1 – This is also called smart gateways that are important for establishing a connection between the external network and fog. The proposed model aims to protect

from unauthorized sources that will drop packets entering from unreliable sources. This also plays a vital role in prioritizing the data and forming queues with higher to lower prioritization sequence.

ii) Tier 2 – Layered based security - Smart gateways that were placed to perform preliminary data examination by understanding the usage of resource and device consumption patterns (Daneshgar, Sianaki, and Ilyas, 2019). Furthermore, compared to past behaviors for anomaly detection. Furthermore, the behaviors were checked for priority tags of data and allowing in high priority order to move ahead. Encryption of data occurs at the second-tier using onion routing, DTLS services, and AES facilitated encryptions. *Figure* 3 represents the proposed layered architecture for CoT.

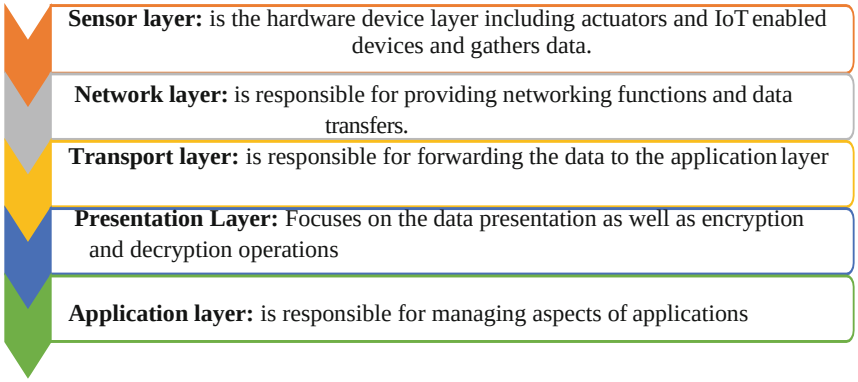

Figure 3. Proposed layered architecture for CoT (Daneshgar, Sianaki, and Ilyas, 2019)

iii) Tier 3 – In this tier, the data gets pre-processed storing the less priority data, while transferring high priority data. *Figure* 4 below represents the architecture of the proposed secure architectural framework for CoT that consists of a sensor layer, network layer, transport layer, presentation layer, and application layer.

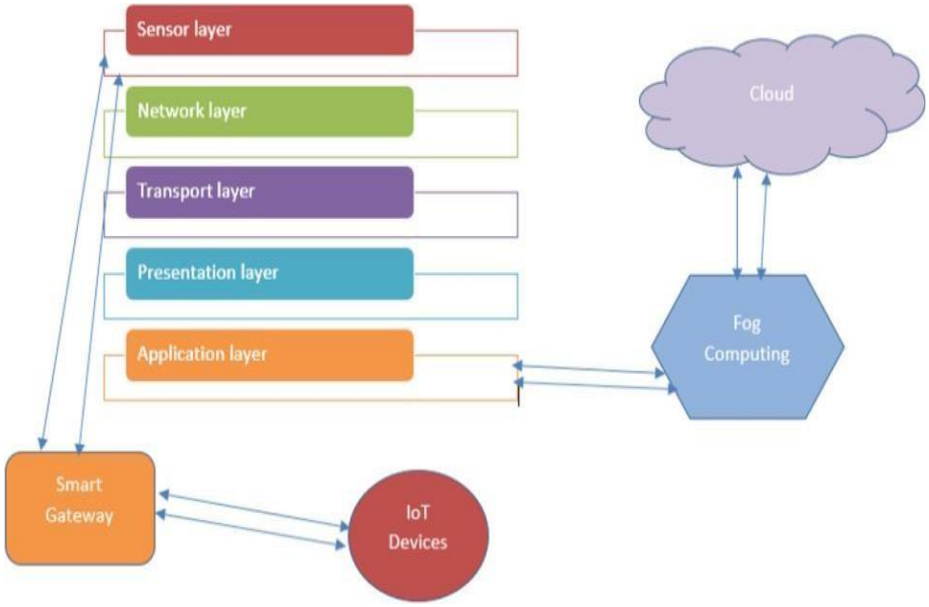

Figure 4. The architecture of the proposed secure architectural framework for CoT (Daneshgar, Sianaki, and Ilyas, 2019)

The proposed framework will help to overcome security challenges in CoT and concentrates on the architectural aspect of data security in CoT and includes several advantages like data prioritization, resource usage efficiency, and provides high-level data protection. However, the research has limitations like time-consuming, DTLS usage which is lightweight secure protocols are less secure than TCP protocols (Daneshgar, Sianaki, and Ilyas, 2019).

Securing CoT using Knowledge-based Cognitive "CAPTCHA" Technique. Ogiela et al., (2018) proposed the use of A Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) in the CoT environment to address security and privacy issues. In this research, the authors have presented an idea to use cognitive CAPTCHAs for a challenge-response test. This technique will protect the limited resource devices and cloud environment from bots as well as software-based

Artificial Intelligence (AI). The research consists of several techniques that have been incorporated recently in the form of visual captcha designs. The techniques prevent bots or unauthorized users by presenting along with image fragments and symbol recognition. *Figure 5* shows the proposed scheme is depicted below:

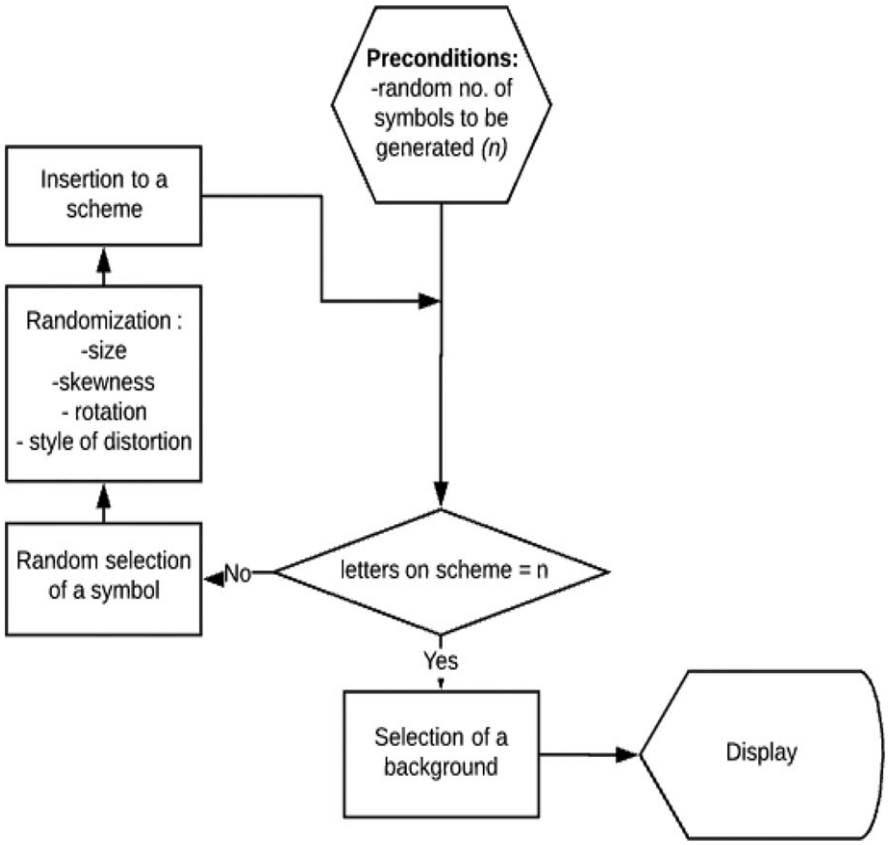

Figure 5. The scheme of the proposed CAPTCHA algorithm (Ogiela et al., 2018)

Secured CoT Frameworks. Bhattasali, Chaki, and Nabendu (2013) present an insight into the security challenges in the environment of CoT with a focus on security and trust. The authors proposed the concept of secure trusted things as a service that aims at reducing the number of privacy and security issues in CoT. The scheme proposed by Bhattasali, Chaki, and Nabendu (2013) includes an encryption mechanism that enables less overhead. Furthermore, a trust model that enables real-time decision

making is the focus of the proposal as demonstrated in *Figure 6.*

Secure and Trusted CoT (SCoT). CoT provides a distributed heterogeneous data storage domain to enhance scalability and flexibility with reduced cost. Several challenges need to be considered to realize the concept of CoT. The main concerns are security and trust. The framework of SCoT mainly focuses on the security and trust in the cloud environment where the number of IoT devices are interconnected. Figure 6 represents the Trust as a Service in SCoT Framework below:

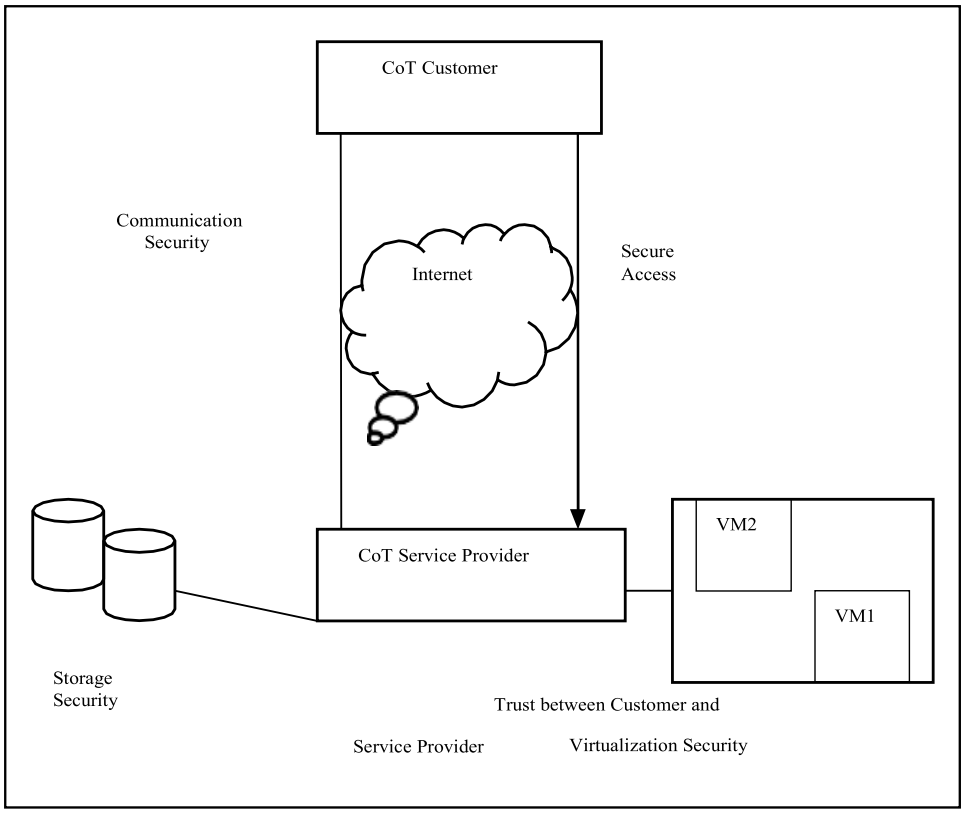

Figure 6. Trust as a Service in SCoT Framework (Bhattasali, Chaki, and Nabendu, 2013)

As CoT treats everything as service, the framework also treats things, security, and trust as service, which is considered as Secure Trusted Things (STeTaaS) as a Service

in the SCoT framework. Security as a Service is considered when there is a data transmission between two customers that is between the sender and the receiver through a third-party CoT service provider.

Secured-Trusted-Things-as-a-Service (STeTaaS). STeTaaS is a concept that includes Things as a service, Security as a service, and Trust as a service. Security and trust are two main concerns in the environment like CoT to provide reliable services to the end-users in a timely manner (Sethi, 2012). To provide uninterrupted services, heterogeneous things are also treated as services. Therefore, STeTaaS is the basic concept to build the base of the SCoT framework.

Trust as a Service. In the cloud environment, every user cannot become a service provider but are considered as a cloud customer. Trust between CoT customer and CoT service provider is provided as service in the SCoT framework to improve anonymous communication. A service level agreement (SLA) is formally defined between the customer and the service provider. This SLA is a trust that is established between the customer and the service provider and includes general information about services, priorities, responsibilities, guarantees, warranties, and so on.

There are various levels of agreement between the customer and the service provider. Trust as a Service mainly focuses on secure data storage, secure data transmission, secure virtualization. This paper described the Secure Trusted Things as a service concept in the proposed SCoT framework. Initially, trust needs to be established between communicating parties. The proposed model motivates organizations for utilizing all benefits of cloud services and reducing their expenditures.

CoT Related Standards and Frameworks

In this section, some of the security frameworks, standards, and guidelines pertaining to cloud computing and IoT systems are identified and reviewed. Since there are no existing frameworks, standards, and guidelines are directly related to CoT. Therefore, methodology was developed to gather appropriate security and privacy controls to reduce the risks relevant to CoT systems from the mentioned documents in this section.

The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0

Cloud Security Alliance promotes implementing best practices for providing security assurance within the domain of cloud computing and has delivered a practical, actionable roadmap for organizations seeking to adopt the cloud paradigm (Rich et al, 2017). CSA v4.0 version incorporates advances in cloud security and supporting technologies reflects on real-world cloud security practices and integrates the latest Cloud Security Alliance research projects and offers guidance for related technologies.

Baseline Security Recommendations

Baseline Security Recommendations (2017) was published by the European Union Agency for Cybersecurity (ENISA) for IoT that provides a set of recommendations that an IoT device must follow and a list of security features to adopt. Core Baseline guides with the best security practices for mitigating risks and provide security to IoT devices. Core Baseline Recommendation aims at providing security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks, and identifying potential good practices and security measures to apply to protect IoT systems. (BSR ENISA, 2017).

CIS Controls Cloud Companion Guide Version 7

CIS Cloud Companion Guide (2019) provides the best security practices available in CIS to any kind of Cloud Environment from both consumer and customer perceptive. The document consists of various considerations such as business requirements in Cloud environments, unique risks, and the importance of security requirements (CIS CCG, 2019).

CIS Controls Internet of Things Companion Guide

The CIS Controls have internationally recognized cybersecurity best practices for protection against common cybersecurity threats. CIS is commonly used in different sectors of industry sectors and throughout local, state, and federal governments. The CIS Controls companion guide focuses on security-related factors that should be analyzed before a purchase is made. These include the ability to manage authentication credentials (e.g., change a password, enable 2-factor authentication), encrypt network traffic, and receive software updates. A major factor of IoT is making sure devices are outfitted with all necessary security features before the purchase is made, as embedded devices do not get new functionality over time. CIS helps with an enormous number of security controls that are applicable for IoT and addresses several IoT security challenges and what are the important security consideration that must be taken care of to overcome IoT related security problems.

NIST SP 800-53 Revision 5

Security and Privacy Controls for Information Systems and Organizations was released on March 16. NIST SP 800-53 R5 presents a proactive and systemic approach to

develop comprehensive safeguarding measures for all types of computing platforms, including general-purpose computing systems, cyber-physical systems, cloud, and mobile systems, industrial/process control systems, and Internet of Things (IoT) devices (NIST SP 800-53 Rev. 5, 2020).

Research Methodology

The research project has concentrated on developing security best practices document that can be referenced by the businesses while adopting CoT. This document serves as a reference guide to understand what are the different types of attacks and threats that are associated with CoT usage and further highlights the way to address the challenges. The end-users of this document will be presented with security best practices based on current standards, frameworks, guidelines such as NIST 800-53 R5, CSA, etc., that can help in reducing the risk of cyber-attacks posed to the organizations that have integrated their business with CoT systems or planning to adopt CoT.

The scope of this research is to list common attacks and threats related to CoT for identifying best practices and reviewing standards, frameworks, and guidelines pertaining to cloud computing and IoT which can be used by organizations to secure CoT infrastructure and its applications.

This research focuses on providing the solution for the following research questions:

- What are the common attacks and threats in CoT that organizations must be aware of while planning to deploy CoT systems in their environment?

- What are the appropriate controls which must be implemented to maintain the security and privacy of the CoT environment?
- What are the best security practices organizations must follow while adopting CoT architecture?

The compilation of the research deliverables was based on the steps outlined below:

1. In the first step, common attacks and threats in CoT systems have been identified by conducting a literature review.

2. In the second step, based on the identified attacks and threats in step 1, relevant security, and privacy controls from NIST 800-53 R5 publications have been identified and mapped to address the attacks and threats.

3. In the third step, standards, frameworks, and guidelines pertaining to Cloud systems as well as IoT systems have been reviewed and a guideline document is proposed outlining security best practices to reduce the risk of cyber-attacks posed to the organizations that have integrated their business with CoT systems or planning to adopt CoT.

Results

For the identified threats and attacks from the literature review related security controls from NIST 800-53 R5 have been identified and listed in table 1. Table 1 shows the common attacks and threats identified through the literature review. The first column in the table represents an attack and threats column and followed by attacks and threats description and scenarios in the CoT environment. Further columns consist of control and its description relating to CoT systems.

Table 1. CoT Related Attacks and Threats with Relevant Security Controls

S.No	Attacks and Threats	Description and Scenario	Controls (NIST 800-53 R5)	Description (NIST 800-53 R5)
1	**Distributed Denial of Service (DDoS)**	Description: DDoS attack is a common attack targeting the availability aspect of the CIA triad. Scenario: In a scenario where multiple IoT devices are connected to a cloud environment using a secure connection and all the provisioning/device management is handled using a cloud console. The IoT devices in the architecture/business model are acting as sensors collecting for example weather information which is processed in the cloud using big data analytics to predict the weather. The attackers can take control over the IoT devices to disrupt the services by making them a Bot. For example, installing malware by the malicious actor on all IoT devices and taking control over the IoT device to make them a botnet for sending a huge amount of data to cloud-hosted servers for the sole purpose of disrupting the services.	SC-6 SC-7	**RESOURCE AVAILABILITY:** This control prevents delays or interference of low-priority processes in the service system to higher-priority processes and causes users and processes to use only available resources. This control does not apply in cases where system components have only one user or role. **BOUNDARY PROTECTION:** One of the things that can be done to restrict or prevent the activity of interfaces in the CoT is to restrict external web traffic to servers designated in managed interfaces and to prevent the flow of external traffic that forges internal addresses.

Refer to the link below for the complete result of CoT Related Attacks and Threats with Relevant Security Controls:

https://drive.google.com/file/d/1K0BrzXCvDyXvXi370ffwHLPhXkiiR9A_/view?usp=sharing

For the identified threats and attacks, the security best practices for the CoT environment have been collated and listed below in Table 2.

Table 2. Security Best Practices CoT

Serial No	Attacks and Threats	Security Best Practices for CoT
1	Distributed Denial of Service (DDoS)	• Protect the network by maintaining network-based URL filters. In this approach, the filters are enforced to limit the systems/host ability to connect to the website not approved by the organization (CIS). • Use of Domain Name System (DNS) filtering service to be implemented at the network level that would help the organization to block access from known malicious domains. In addition, enabling DNS query logging for detecting hostname lookups for malicious domains (CIS). • It is observed that numerous DDOS attacks were successful by sending malicious emails and attachments in the email. Therefore to counteract such attacks CIS has mentioned certain controls such as Domain-based Message Authentication (DMARC) for reducing the possibilities of spoofed or altered emails from valid domains to further reduce the possibilities of DDOS attack Sender Policy Framework (SPF) must be implemented/ enabled for receiver-side verification. CIS further suggests blocking all unnecessary email attachments and to sandbox the received files, attachments for further analysis (CIS). • Since DDOS attacks primarily target the network to cause unavailability of authenticated systems it is suggested that ingress and egress filtering rules must be implemented based on business needs. In addition, it is recommended by CIS to perform a regular automated port scan to detect anomalous activities (CIS). • Firewalls are an integral solution that an organization must be implemented for detecting and protecting from DDOS attacks. Therefore, it is recommended to institution host-based firewalls and application layer firewalls (CIS). • DDOS attacks can prevail by exploiting a diverse set of vectors. Therefore, it is important to initially detect DDoS attacks based on know patterns. For detection and further protection, it is recommended to implement a Network-based Intrusion Detection System (NIDS) for identifying unusual attack mechanisms and deploying Network-based Intrusion Prevention Systems (NIPS) to block malicious traffic at the perimeter level (CIS).

		• Using secure hypervisors and implement a patch management process to keep the systems up to date (CSA). • To ensure the secure configuration of IoT devices, it is recommended to protect from vulnerabilities that could be caused by misconfigurations leading to DDoS attacks (CIS). • IoT devices must be configured in a restrictive approach as opposed to a permissive approach that ensuring secure and trusted communication. In addition, IoT devices should not be reachable via default inbound collections (ENISA).

Refer to the link below for the complete result of Security Best Practices CoT:

https://drive.google.com/file/d/15czLYw1Op-5ChMBjvzq6b_dLYJBX74FJ/view?usp=sharing

Analysis and discussion of Results

In this document, several common attacks and threats associated with CoT have been identified such as DDOS, Eavesdropping, etc, which have been explained in the literature review previously. The attacks and threats are described briefly with respect to CoT devices along with attack scenarios. In addition, these are further mapped with security and privacy controls derived from NIST 800-53 R5.

The first output consists of the following section (a) Attacks and threats that are associated with CoT systems; (b) Description and Scenario that briefly defines the attack and threats and relates them to CoT scenarios; (c) Security and Privacy control from NIST 800-53 R5; (d) Description of controls that aligns with the CoT systems. This output helps the organization to get familiar with several common attacks and threats faced by CoT systems and suggests the organization that should follow a set of security and privacy controls to address the identified attacks and threats associated with CoT systems.

Security Best Practices for CoT

The study conducted on several existing standards, frameworks, and guidelines pertaining to Cloud and IoT is analyzed and reviewed to check which of the identified standards, frameworks, and guidelines best fits in securing CoT systems. The applicable standards, guidelines, and frameworks are used to list the security best practices for CoT. The proposed security best practices provide a guideline that an organization should follow to overcome the threats and attacks that are associated with CoT systems which were identified in the earlier stage of research. Several attacks and threats have been combined that have common best practices. The security best practices are mapped from the following standards, guidelines, and frameworks, namely (a) The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 BY CSA, (b) Baseline Security Recommendations for IoT by ENISA, (c) CIS Controls Cloud Companion Guide Version 7 (d) CIS Controls Internet of Things Companion Guide. The proposed guidelines cover major security best practices, the organization should follow to secure the CoT system against threats and attacks.

Conclusion

As CoT system is used worldwide by a large number of people that depict a huge benefit to the future internet. CoT technology is used every day ranging from a smartwatch to smart industries providing immense advantages to a business. The advancements in CoT systems do offer benefits but can be targeted by attackers. Therefore, consideration of privacy and security best practices of CoT is critical. In this document with the intent to provide an additional level of security in CoT systems, control mapping of NIST 800-53 R5 has been performed with common attacks targeting CoT devices. In addition to this, security best practices have been proposed that are derived from relatable standards,

frameworks, and guidelines that can potentially help the organization to secure the CoT applications.

The limitation of this research is that identified controls and proposed best security practices are not tested in the real environment. In future, research can be extended to address novel attacks pertaining to CoT systems as the threat landscape changes by finding the security best practices. Research could also be extended to include other relevant standards, guidelines, and frameworks. Future study can be enhanced to understand which best practices align to SaaS v/s PaaS v/s IaaS deployment.

References

Alaba, F. A., Othman, M., Hashem, I. A., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28. doi:10.1016/j.jnca.2017.04.002

Ari, A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., & Gueroui, A. M. (2019). Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. Applied Computing and Informatics. doi:10.1016/j.aci.2019.11.005

Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). Integration of Cloud Computing with the Internet of Things: Challenges and Open Issues. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). doi:10.1109/ithings-greencom-cpscom-smartdata.2017.105

Baseline Security Recommendations for IoT. (2018, April 20). Retrieved from https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Belguith, S., Kaaniche, N., & Russello, G. (2019). CUPS: Secure opportunistic cloud of things framework based on attribute-based encryption scheme supporting access policy update. Security and Privacy. doi:10.1002/spy2.85

Bhattasali, T., Chaki, R., & Chaki, N. (2013). Secure and trusted cloud of things. 2013 Annual IEEE India Conference (INDICON) doi:10.1109/indcon.2013.6725878

Callegati, F., Giallorenzo, S., Melis, A., & Prandini, M. (2018). Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective. Computers & Security, 74, 277-295. doi:10.1016/j.cose.2017.10.006

CIS Controls™ Companion Guides. (2019). Retrieved from https://www.cisecurity.org/controls/cis-controls-companion-guides/

Cloud ControlsMatrix (CCM) (2019). [Online]. Available: https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Connected Consumer Products - IoT Security Foundation. (2016). Retrieved from https://www.iotsecurityfoundation.org/wp-content/uploads/2016/12/Connected-Consumer-Products.pdf

CSA Security Guidance. (2019). [Online]. Available: https://cloudsecurityalliance.org/research/guidance

Daly, G., Edwards, M., Indurkya, G., Kreger, H., Libow, E., Marcus, B... Tumashow, A. (2016). Deliverable. Retrieved from https://www.omg.org/cloud/deliverables/cloud-customer-architecture-for-iot.htm

Daneshgar, F., Sianaki, O. A., & Ilyas, A. (2019). Overcoming Data Security Challenges of Cloud of Things: An Architectural Perspective. Advances in Intelligent Systems

and Computing Complex, Intelligent, and Software Intensive Systems, 646-659. doi:10.1007/978-3-030-22354-0_58

Force, J. (2020, March 16). Security and Privacy Controls for Information Systems and Organizations. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5

Future-proofing the Connected World - Cloud Security Alliance. (2016). [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Gruschka, & Jensen, M. (2010). Attack Surfaces: A Taxonomy for Attacks on Cloud Services. 2010 IEEE 3rd International Conference on Cloud Computing. doi:10.1109/cloud.2010.23

Gupta, S. (2020, April). IoT Cloud Platform Market., from https://www.marketsandmarkets.com/PressReleases/iot-cloud-platform.asp

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems on the Internet of Things. 2015 IEEE World Congress on Services. doi:10.1109/services.2015.12

IoT Security Compliance Framework. (2016). [Online]. Available: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf

IoT Security Guidelines Overview Document. (2020). [Online]. Available: https://www.gsma.com/iot/iot-security-guidelines-overview-document/

ISO/IEC 27001 - Information security management. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27007:2020. (2020, January 21). [Online]. Available: https://www.iso.org/standard/77802.html

ISO/IEC 27017:2015. (2015, November 30). [Online]. Available: https://www.iso.org/standard/43757.html

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2012). A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing, 63(2), 561-592. doi:10.1007/s11227-012-0831-5

Noor, T. H., & Sheng, Q. Z. (2011). Trust as a Service: A Framework for Trust Management in Cloud Environments. Lecture Notes in Computer Science Web Information System Engineering – WISE 2011, 314-321. doi:10.1007/978-3-642-24434-6_27

Ogiela, M. R., Krzyworzeka, N., & Ogiela, L. (2018). Application of knowledge-based cognitive CAPTCHA in Cloud of Things security. Concurrency and Computation: Practice and Experience, 30(21). doi:10.1002/cpe.4769

Pacheco, L., Alchieri, E., & Solis, P. (2017). Architecture for Privacy in Cloud of Things. Proceedings of the 19th International Conference on Enterprise Information Systems, 2, 978-989-758-248-6, 487-494. doi:10.5220/0006357504870494

Peer-Reviewed Document - Cloud Security Alliance. (2015). Retrieved from https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

Rich, M., Francoise, G., Adrian, L., David, M., Gunnar, P., & Mike, R. (2017). CSA Security Guidance. [Online]. Available: https://cloudsecurityalliance.org/research/guidance

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279. DOI:10.1016/j.comnet.2012.12.018

Security, R. (2019, August). Request the 2019 Q1 Data Breach QuickView Report. Retrieved from https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

Sethi, M. (2012). Nordsecmob.aalto.fi. [Online]. Available: http://nordsecmob.aalto.fi/en/publications/theses_2012/sethi-mohit_thesis.pdf

Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty Security Considerations for Cloud-Supported Internet of Things. IEEE Internet of Things Journal, 3(3), 269-284. doi:10.1109/jiot.2015.2460333

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11. doi:10.1016/j.jnca.2010.07.006

Tschofenig, H., & Fossati, T. (2016). Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things. [Online]. Available: https://tools.ietf.org/html/rfc7925

Wayne, J., & Timothy, G. (2011). Guidelines on security and privacy in the public cloud ... - NIST. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Y. Zhang, D. Zheng and R. H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2130-2145, June 2018, doi: 10.1109/JIOT.2018.2825289.