DEVELOPMENT AND VALIDATION OF A CLOUD FRAMEWORK FOR A LARGE SCALE ENTERPRISE IN DEFENSE INDUSTRY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

SALİH SAMET AKAR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

APRIL 2023

DEVELOPMENT AND VALIDATION OF A CLOUD FRAMWORK FOR A LARGE SCALE ENTERPRISE IN DEFENSE INDUSTRY

Submitted by SALİH SAMET AKAR in partial fulfillment of the requirements for the degree of **Master of Science in Information Systems Department, Middle East Technical University** by,

Prof. Dr. Banu Günel Kılıç
Dean, **Graduate School of Informatics** _____

Prof. Dr. Altan Koçyiğit
Head of Department, **Information Systems** _____

Prof. Dr. Sevgi Özkan Yıldırım
Supervisor, **Information Systems Dept., METU** _____

Examining Committee Members:

Asst. Prof. Dr. Özden Özcan Top
Information Systems Dept., METU _____

Prof. Dr. Sevgi Özkan Yıldırım
Information Systems Dept., METU _____

Asst. Prof. Dr. Tuna Hacaloğlu
Information Systems Engineering Dept., Atılım University _____

Date: **13.04.2023**

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Salih Samet AKAR

Signature : _____

ABSTRACT

DEVELOPMENT AND VALIDATION OF A CLOUD FRAMEWORK FOR A LARGE SCALE ENTERPRISE IN DEFENSE INDUSTRY

Akar, Salih Samet

MSc., Department of Information Systems

Supervisor: Prof. Dr. Sevgi Özkan Yıldırım

April 2023, 54 pages

Today, cloud computing has become actively used in the modernization processes of many industries. Within the scope of the thesis study, a case study was carried out, and a framework was developed that enables the use of cloud computing in the defense industry software development processes. During the development, the cloud class was chosen in accordance with the security and privacy constraints brought by the defense industry and the difficulties experienced in using cloud computing instead of existing technologies were expressed. The developed framework has been presented to defense industry employees. At the end of the study, the usage of the developed cloud framework with a questionnaire study was validated, the similarities and differences with the studies in the literature were discussed, and suggestions for future studies were presented. This study, which was carried out by complying with all restrictions and requirements in the defense industry software modernization process, is important for future studies with its pioneering structure.

Keywords: Defense Industry, Cloud Computing, Private Cloud, Security

ÖZ

SAVUNMA SANAYİ ALANINDA FAALİYET GÖSTEREN BÜYÜK ÖLÇEKTEKİ BİR İŞLETME İÇİN BULUT ÇERÇEVE GELİŞTİRMESİ VE DOĞRULANMASI

Akar, Salih Samet

Yüksek Lisans, Bilişim Sistemleri Bölümü

Tez Yöneticisi: Prof. Dr. Sevgi Özkan Yıldırım

Nisan 2023, 54 sayfa

Günümüzde bulut bilişim birçok endüstrinin modernleşme süreçlerinde aktif olarak kullanılır hale gelmiştir. Tez çalışması kapsamında bir durum çalışması yapılarak savunma sanayi endüstrisinin yazılım geliştirme süreçlerinde bulut bilişimin kullanımını sağlayan bir çerçeve geliştirilmiştir. Geliştirme esnasında savunma sanayinin getirdiği güvenlik ve gizlilik kısıtlarına uygun bulut sınıfı seçilmiş ve mevcut teknolojilerin yerine bulut bilişim kullanımında yaşanan zorluklar ifade edilmiştir. Geliştirilen çerçeve, savunma sanayi çalışanlarının kullanımına sunulmuştur. Çalışma sonunda bir anket çalışması ile geliştirilen çerçevenin kullanımı doğrulanmış, literatürdeki çalışmalarla benzerlik ve farklılıkları tartışılmış ve gelecek çalışmalar için öneriler sunulmuştur. Savunma sanayi yazılımlarının modernleşmesi sürecinde tüm kısıt ve gereksinimlere uyarak yapılan bu çalışma öncü yapısı ile gelecek çalışmalar için önem taşımaktadır.

Anahtar Sözcükler: Savunma Sanayi, Bulut Bilişim, Özel Bulut, Güvenlik

To my family and friends…

ACKNOWLEDGMENTS

First, I would like to express my gratitude to all the defense industry, that provided all kinds of opportunities and supported me during my graduate education and thesis process.

In addition, I would like to express my endless thanks to my dear supervisor Professor Sevgi ÖZKAN YILDIRIM, whose knowledge and experience I have benefited from throughout my work, whose moral values I have taken as an example, which I am honored to work with, and for the tolerance and patience he has shown throughout this process.

I would also like to express my endless thanks to my manager Hasan Hamdi KONYA, who helped me in every way while carrying out my thesis work, to my teammate Kürşat DURAK for his knowledge, experience, and moral support, and to my parents Hülya and Arif AKAR and to my brother Dr. Ünal Ahmet AKAR, who did not spare their moral support and stood by me in every difficulty.

Finally, I would like to express my endless thanks to my wife Melis AKAR who has always been by my side with her knowledge, skills, experience, and belief in me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IT	Information Technology
SAAS	Software as a Service
PAAS	Platform as a Service
IAAS	Infrastructure as a Service
DDOS	Denial of service
SSL	Secure Socket Layer
USA	United States of America
DNS	Domain Name System
CI	Continuous Integration
CD	Continuous Delivery/Deployment
EAL4+	Evaluation Assurance Level
NIST	National Institute for Standards and Technology
ARPANET	Advanced Research Projects Agency Network
SLA	Software License Agreement
QoS	Quality of Service
DoD	Department of Defense
SPI	Software, Platform, Infrastructure
UCI	Unified Cloud Interface
CCIF	Cloud Computing Interoperability Forum
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
UPS	Uninterruptible Power Supplies
SUS	System Usability Scale

CHAPTER 1

INTRODUCTION

Cloud computing is the general name of the service that provides access to applications and data in a specific location from different locations. It is a structure that enables computer resources to be used by different users over the internet without providing any infrastructure (Seyrek, 2011). Another definition for cloud computing by National Institute for Standards and Technology (NIST) is that cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST, 2011).

Cloud computing provides many benefits to companies with its structure and features (Sethi, 2014). For this reason, the usage of cloud computing has become widespread among companies that are modernizing their software development processes (Odell et al., 2015). But the industry that each company serves imposes different requirements and constraints. The defense industry is also in the process of modernization and is an industry type where constraints and requirements are quite high. This research aims to overcome all challenges and to create a cloud framework in the defense industry and for including in software development processes. This chapter will introduce the study by first discussing the background and context, followed by the research questions and objectives, limitations, the significance and finally, the phases.

1.1. Overview of Cloud Computing

Although cloud computing is popular today, it was a concept in the 1950s where multiple users accessed a single resource through a terminal (Odell et al., 2015). In 1961, the foundations of the idea of cloud computing were laid by John McCarthy (Surbiryala & Rong, 2019). It was later matured by J.C.R. Licklider, who was influential in the development of the Advanced Research Projects Agency Network (ARPANET). He designed a global network system where everyone could access data globally (Timmermans et al., 2010). With the development of personal computers over time, the demand for central processing power decreased. However, with the development of computer technology in line with increasing needs, the benefits of cloud computing began to look attractive to companies. High-capacity networks, low-cost computers, virtualization and service-oriented architecture and efficient storage capabilities have led to increased investments in cloud computing. Major players in the industry such as Amazon, Google, Microsoft, Salesforce have led to evolution of cloud computing (Odell et al., 2015).

The cloud computing structure can be classified into three different service classes as platform as a service, infrastructure as a service, and software as a service and four deployment classes as public, private, community and hybrid (NIST, 2011).

1.1.1. Cloud Service Classes

According to characteristics, level of control granted to cloud consumer, and consumer activities cloud services are divided into three main services as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). These services are shown in Figure 1.

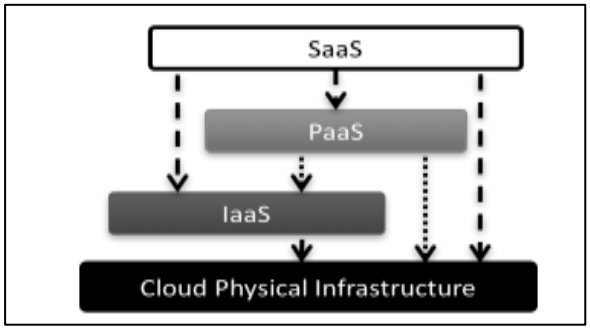

Figure 1. Cloud Service Model (Almorsy et al., 2016)

1.1.1.1. Software as a Service(SaaS)

SaaS provides only running a consumer application on cloud infrastructure. Many clients can access this application from various sources. Consumer does not have control over the cloud infrastructure sources except application specific configurations (Odell et al., 2015). Reducing application software licensing cost, removing need of infrastructure, secure socket layer (SSL) usability can be considered as the main advantages of SaaS (Bokhari et al., 2016).

1.1.1.2. Platform as a Service (PaaS)

Deploying an application that created by consumer with supported programming languages, service, libraries, and tools to cloud. The consumer does not manage cloud infrastructure, it has control over the deployed application and its configuration (Odell et al., 2015). The setup, administration, and maintenance time needed by developers is reduced by pre-configured development environments (Gibson et al., 2012).

1.1.1.3. Infrastructure as a Service (IaaS)

Consumer has capability for deploying and running a software on this type of service. IaaS provides all essential computational power like processing, storage, networks etc. to consumer. Therefore, it has control over the most of these sources (Odell et al., 2015). Virtualization of the infrastructure is the main concept in IaaS (Ashraf, 2014).

Figure 2 shows the SaaS, PaaS, and IaaS layers with users.

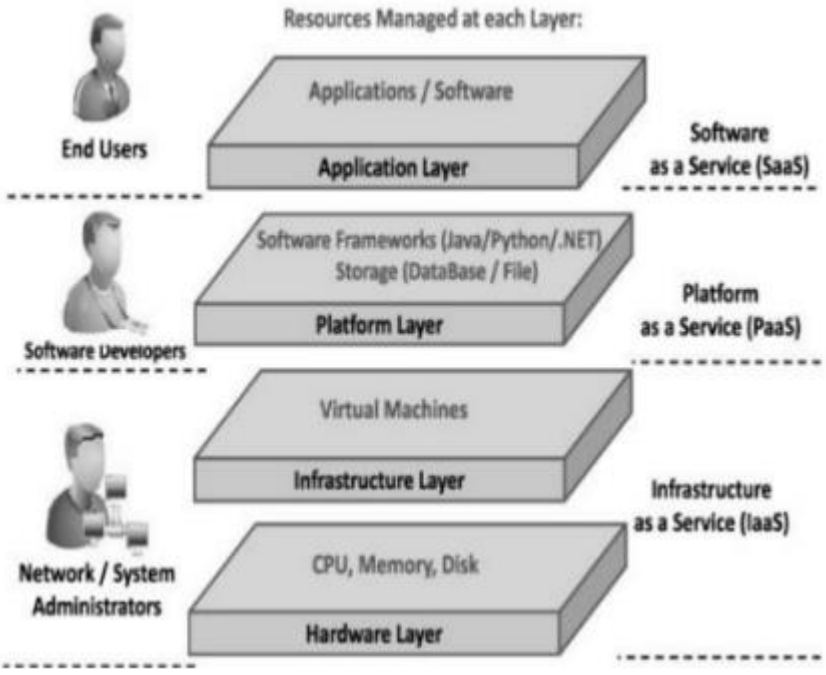

Figure 2. SaaS, PaaS, and IaaS layers (Odell et al., 2015)

1.1.2. Cloud Deployment Classes

In the field of cloud computing, according to distribution and physical location there are 4 different cloud structures: public, community, private and hybrid (Diaby & Rad, 2017). These structures have different properties from each other. Depending on the need, a choice is made between individuals and institutions.

1.1.2.1. Public Cloud

The public cloud structure is the service model used by large companies such as Google and Amazon and can be accessed by every user (Helvacioglu Kuyucu, 2011). However, that does not mean that client data visible to every user, only authorized and authenticated user can see the data (Diaby & Rad, 2017). Although it provides free access to end users, the number of endpoints affected by potential problems is high. Corporate places and companies that require high security do not prefer it because of such privacy problems. Large organizations that provide this type of service carry out many studies to minimize security problems (Helvacioglu Kuyucu, 2011). Therefore, public cloud is not suitable for organizations that have strict regulations and operating with sensitive data (Kumar Gupta, 2018).

1.1.2.2. Private Cloud

Private cloud structure is used by a single organization. The result of a possible error affects a smaller community. The maintenance of this structure belongs to the organization using it. Maintenance and management can be done internally as well as

by third parties (Helvacioglu Kuyucu, 2011). The private cloud is known as the most secure cloud because data processes are controlled and managed by own organization (Diaby & Rad, 2017). Many medical offices, banking institutions, and other organizations that must meet federal and state guidelines for data controls use a private cloud. In case of private cloud, resources are not shared with others and therefore offer better performance compared to public cloud (Kumar Gupta, 2018).

1.1.2.3. Community Cloud

Many small organizations use the same service in the community cloud structure (Helvacioglu Kuyucu, 2011). In order to lower the operating expenses of IT, several institutions that share similar business objectives, initiatives, or resources require infrastructures like software and hardware (Diaby & Rad, 2017). An example of this is the collaboration of state institutions. In case of any failure, the impact is less than in the public cloud. Structures with the same degree of confidentiality can access each other's resources and share data. The workload is lower than the private cloud (Helvacioglu Kuyucu, 2011). The cloud infrastructure could be managed by a third-party organization or within one of the organizations in the community (Dillon et al., 2010).

1.1.2.4. Hybrid Cloud

The hybrid cloud structure has features that merge all models. Two or more organizations can serve together. Data management and application sharing can be done internally. It is scalable and has a higher fault tolerance. While any business can work in its own internal network, the public cloud structure feature comes into play in case of capacity increase and sudden load and provides an external network environment. The synchronization and transfer of large-scale data becomes difficult (Helvacioglu Kuyucu, 2011). Organizations maximize their efficiency and get better performance from the cloud infrastructure. Also, it is very convenient for the organization that needs to keep confidential data on the private cloud, and more general data on the public cloud (Kumar Gupta, 2018).

1.2. Research Question and Objective

Legacy applications used in the defense industry cannot satisfy today's needs and need modernization. The necessity of using web-based modern software for modernization has been stated by the defense industry. However, this requirement has presented many challenges. Web-based software that is planned to be used primarily requires data packet transfer over the internet. However, it is stated as a limitation that the software should not be connected to any external network. In addition, establishing a framework that can be accessed by every authorized user within the internal network of each version of the software is stated as another requirement. In addition, the infrastructure expected to be created should include scalability, high availability, reliability, and fault tolerance properties. For these reasons, it is aimed to develop a framework that can enable web-based software development in the defense industry that meets all these

requirements and constraints. In line with the purpose, answers to the following research questions were sought.

RQ1: What are the current challenges in the defense sector organization to use cloud infrastructure?

RQ2: What could be the structure in a cloud framework showing security and privacy?

RQ3: How valid is the developed framework for use in defense sector organization?

1.3. Research Significance

This study will contribute to the industry for defense sector companies that are considering modernizing their legacy applications with web-based software and transferring their technology infrastructure to cloud computing. It will be a pioneer in the sector with the ability of web-based applications to work in the internal network without being connected to any external network. In addition, it will contribute to the academy as it is one of the rare studies in the field of software development through cloud computing in the defense industry.

1.4. Research Limitations

Cloud computing can be used for different purposes in many different areas today. In this study, a framework infrastructure that enables cloud computing to develop software in the defense industry has been created and its use by software developers has been investigated. During the development, all difficulties were revealed by considering the constraints and requirements of the defense industry.

The major constraint imposed by the defense industry is the external network connection. The framework must not be connected to the external network in any way.

During the research, a case study was conducted by looking at the studies in the literature. Questionnaire method was used to validate the case study.

Research was conducted in collaboration with the IT department to comply with constraints and requirements. Necessary hardware and software were obtained from the IT department.

1.5. Research Phases

In the first stage of the research, the needs for the creation of the cloud service and deployment class were determined. At the same time, possible security problems that may be encountered while creating the cloud framework were determined by considering the constraints determined by the organizations in the defense industry.

In the second stage, a literature review was conducted on the use of cloud computing. Due to the priority of data security, it has been investigated how similar studies are provided in the literature.

In the third stage, the cloud framework was created with the information gathered and the constraints in the defense industry. It has been made available to the software department.

In the last stage, a questionnaire study was conducted to verify the use of the created framework and the results were stated in the thesis study.

Figure 3 shows the progression of this study.

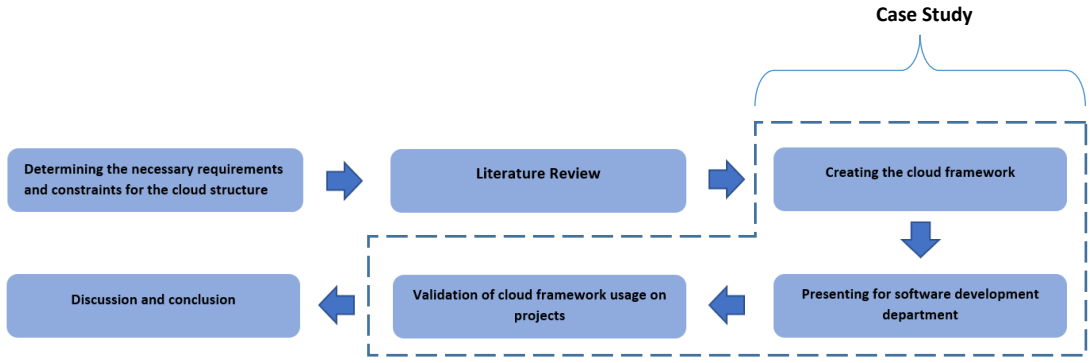

Figure 3. The progression of the study

CHAPTER 2

LITERATURE REVIEW

In this chapter, studies on cloud computing in the literature are mentioned. Previous studies in defense industry are examined in section 2.1. Studies about the security in cloud computing are presented in section 2.2. In addition, the difficulties that encountered in the transition to cloud computing are mentioned in section 2.3. Finally, review results are analyzed in section 2.4.

2.1. Previous Studies in Defense Industry

With the rapid development of cloud computing technology, many sectors have started to use cloud computing in their technology infrastructure for reasons such as speed, cost, scalability, and high availability. One of these sectors is the defense industry. However, unlike other sectors, the defense industry has some strict rules about software development and data storage.

Although the history of cloud computing dates back to the 1960s, cloud computing studies in the defense industry have been delayed due to strict rules. Governance and culture changes, information assurance, resiliency, cybersecurity, data migration, management and interoperability are considered challenges moving to a cloud computing environment (Department of Defense United States of America, 2012).

According to the 22 defense industry and military application studies given in Table 1, cloud computing studies could be carried out in the defense industry and military areas where data security and privacy are critical. The common view in the studies is that data should be kept within the organization by using a private cloud structure in areas where data security and privacy are critical. In this way, the security risk was minimized, and the benefits of cloud computing could be utilized. In addition, another view in the use of cloud computing is to reduce IT expenses and increase efficiency. The IT structure in organizations and the comparison table related to cloud computing are shown in Figure 4.

Table 1. Defense industry studies about cloud computing

Number	Study	Scope
1	(Zaerens, 2011)	Cloud computing usage areas in the defense industry
2	(Tibenszky-Forika, 2012)	
3	(Department of Defense United States of America, 2012)	
4	(Powell, 2013)	
5	(Jedynak, 2013)	
6	(Li & Mehnen, 2013)	
7	(Ragland et al., 2013)	
8	(Lele & Sharma, 2014)	
9	(Sethi, 2014)	
10	(Perkins, 2014)	
11	(ŢIGĂNUŞ, 2015)	
12	(Odell et al., 2015)	
13	(Dudash, 2016)	
14	(Ďulík, 2016)	

Table 1 (continued).

15	(Smith et al., 2017)	
16	(Kumar Gupta, 2018)	
17	(Deparment of the Environment and Energy Australian Government, 2019)	
18	(Tevaseu, 2020)	
19	(Odedra, 2021)	
20	(Choi & Kim, 2021)	
21	(Cho et al., 2021)	
22	(Cheng, 2022)	

If we look at the benefits of cloud computing, a Microsoft study mentioned that cloud computing is cheaper, faster, and environmentally friendly. In the study, it is mentioned that cost savings can be made with the pay as you go approach, it is six times faster than isolated data centers, and how environmentally friendly it is by reducing electricity consumption (Sethi, 2014). For the defense industry, the government in the Obama era also considered cloud computing efforts as potentially cheaper and more efficient way of providing IT services to government employees while improving access and security (Tibenszky-Forika, 2012).

Also in the current on-premise IT structure(intranet) used, scalability, service reliability, high availability, cost effectiveness, high responsive fault tolerance and high performance with security provided by cloud computing cannot be provided (Alambo Tona & Prasad Sharma, 2020).

The United States DoD (Department of Defense) released a cloud computing strategy in July 2012. It needed some innovations about legacy applications, data centers, data deliveries etc. (Odell et al., 2015). Also, the Department of Defense Chief Information Officer claims that there are issues with the too complicated IT networks that have been created over time to give immediate, specialized capabilities but have resulted in decreased security, inadequate information exchange across services and agencies, and

unnecessary money. The need for the enterprise to improve operational efficiency and thereby increase cyber security, improve the effectiveness of both garrison and tactical networks in the enterprise, reduce overall costs, and maintain the flexibility to use future emerging technologies was recognized by military leaders (Powell, 2013). The main goal is that implement cloud computing as the means to deliver the most innovative, efficient, and secure information and IT services in support of the Department's mission, anywhere, anytime, on any authorized device (Department of Defense United States of America, 2012). For all these, an infrastructure was created and improved in time. While creating the infrastructure, security and privacy, the most important issues, was considered with several ways. Data is classified as impact level. Thus, unclassified to most critical data transferred to different clouds. For the unclassified data, public cloud, for the critical data, private cloud was preferred (Odell et al., 2015). Thus, a hybrid cloud is used as cloud deployment class. In addition, IaaS is used as cloud service class, because of that management of the infrastructure belonged to department of defense (Powell, 2013). Because of the security and privacy regulations, no external network was permitted to private cloud. In addition, cloud computing was preferred because it is less costly than an on-premises IT structure, (Figure 4) (Odell et al., 2015) and fiscally constrained environment (Powell, 2013).

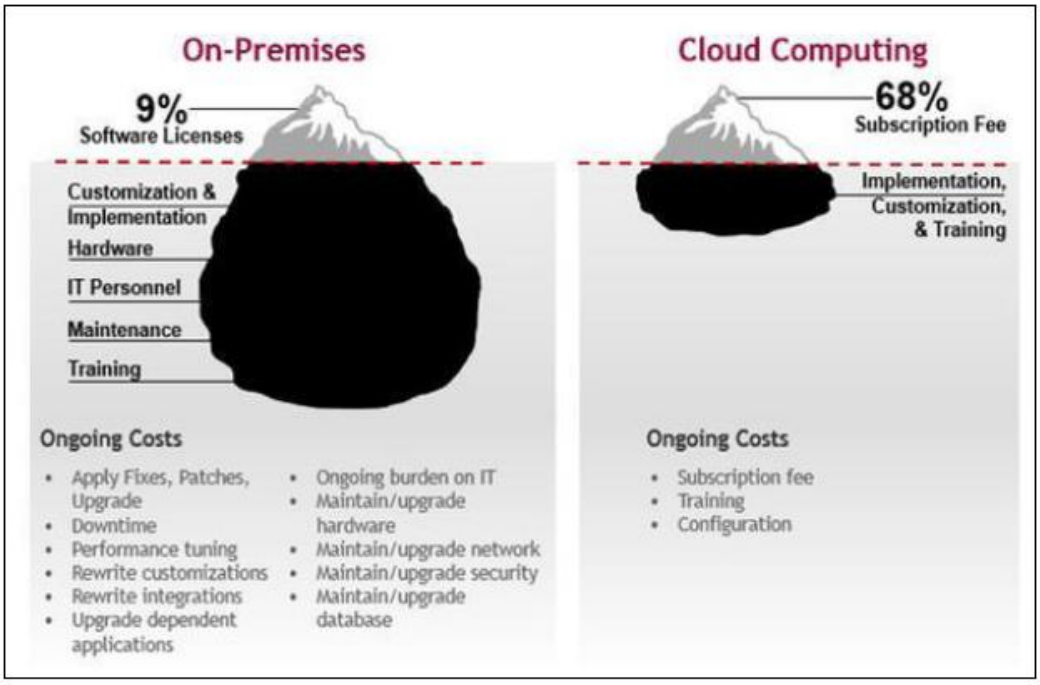

Figure 4. Comparison of on-premises and cloud computing infrastructures (Odell et al., 2015)

The Chinese government is keeping a close eye on cloud computing. In 2010, chip design, hardware, network etc. they have put into use a cloud project that serves in many civilian areas (Lele & Sharma, 2014). In addition, they have also developed cloud systems for the military, which are integrated into systems that provide information sharing and command automation of soldiers (Ragland et al., 2013).

Military analysts supported the use of cloud computing in the military (Lele & Sharma, 2014). Leader cloud computing companies such as Alibaba use the public cloud and implement up-to-date security practices by global cloud computing supporters against potential vulnerabilities. Due to these vulnerabilities and the preferential regulatory and legal policies of the government, the use of private cloud is emphasized instead of public (Ragland et al., 2013).

Indian Defense Department has also built an encrypted cloud infrastructure for its forces. It was presented by Defense Minister Manohar Parrikar and Army General Dalbir on November 9, 2015. It had used for storing personnel and operational data. Data center and its replication located in Delhi and controlled by Indian Army. For data security private cloud structure was preferred and suggested for the noncommercial data in future clouds (Dudash, 2016). In addition, the use of private cloud has been deemed appropriate for government applications such as e-government involving confidentiality (Lele & Sharma, 2014). Providing a secure and cost-effective service environment, an army's own private cloud will form the basis for creating a best-in-class IT environment (Sethi, 2014).

The United Kingdom Ministry of Defense that common with the the United Kingdom Government, announced that implementing the cloud first approach in all sectors in 2013. It was planned to transfer the IT infrastructure in the public sector to the cloud (Maude, 2013). The cloud-first strategy is to leverage the full benefits of the cloud computing approach to modernize the IT structure, reduce cost, and increase security, productivity, and agility (Sugumaran & Al-Mutawha, 2017). Also, privacy of data is emphasized in cloud first document deeply (United Kingdom Ministry of Defence, 2013).

The Australian Department of Defense has allocated a budget of approximately 5 billion dollars for related IT services in order to adapt to cloud computing. It is planned to use the virtualization feature of the private cloud by reducing the number of computer rooms in the department. However, in 2014, cloud computing did not take place in the military sector as it was found to be insufficient in terms of security (Lele & Sharma, 2014). By 2022, efforts have begun to integrate the cloud structure that will serve as IaaS to the defense industry (Hendry, 2022).

The current IT infrastructure management of organizations in Turkey belongs to the organizations. This situation increases the cost and causes inefficiency. For this reason, it is aimed to create a cost-effective cloud infrastructure that can provide higher quality service. In line with the purpose, a strategy report has been prepared that will both facilitate the transition process and meet the requirements of issues such as cyber security. The strategy is expected to be completed in the first half of 2023.

2.2. Security for Cloud Computing

Cloud computing security is a developing area of computer security, network security, and information security more generally (Wikipedia, n.d.-d). Although cloud

computing is a developing new technology, there are some security problems. Privacy, data protection, ownership, location, and lack of reliable audit standard to data security procedure can be seen security concerns. Security issues may vary depending on the cloud deployment model used (Ogigau-Neamtiu, 2012). Such as, public clouds are excellent for personal non-confidential information such as sharing images or videos with friends, but private or agency clouds are best for materials that need to be protected or classified information but are more expensive to manage (Onwubiko, 2010). The private clouds are designed to handle data security issues and provide more flexibility than a public cloud normally provides. Applications that demand total control and configuration of the infrastructure and security are best suited for this (Sen, 2014).

In Figure 5, the data is classified according to confidentiality, integrity, availability, privacy, and impact values and it is specified which cloud structure it will be suitable for.

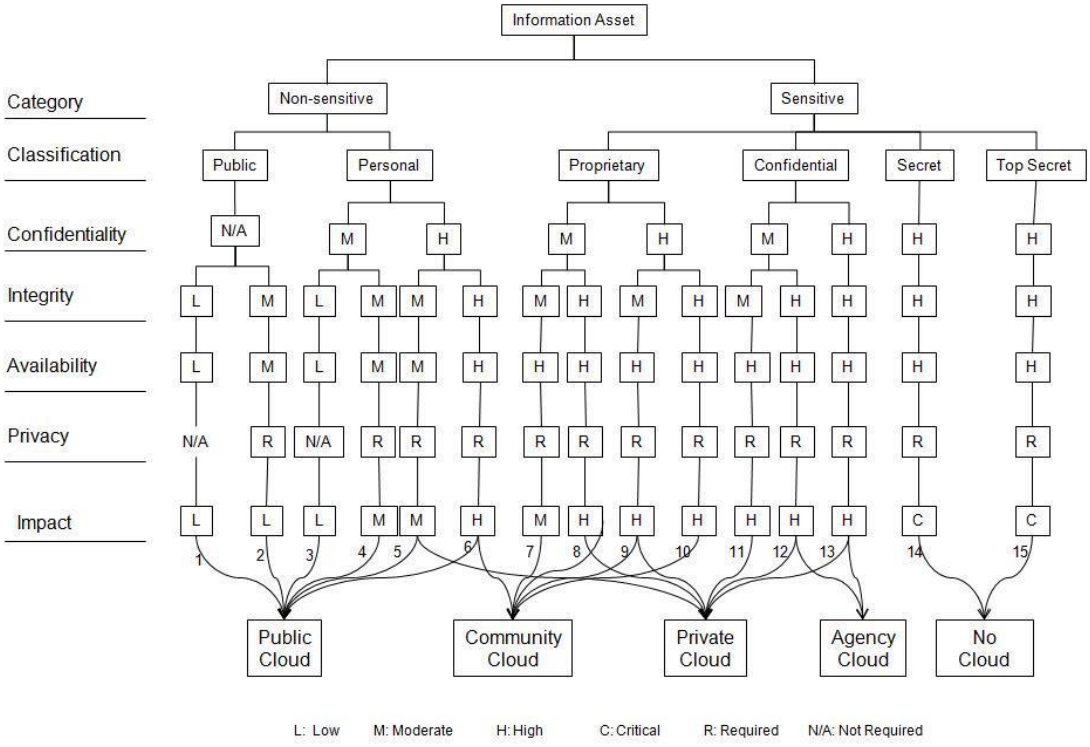

Figure 5. Information classification to cloud mapping (Onwubiko, 2010)

Because agency clouds are privately owned by the military or defense agencies, they are seen as being just as safe and dependable as private clouds. Defense agency clouds could need unique legal, governmental, and security compliance considerations that are not present in public clouds. Similar to information assets #12 and #13 can use private clouds or at least the agency cloud (Onwubiko, 2010).

6 areas that need to be considered in order to secure the cloud system are indicated in Figure 6 (Sen, 2014).

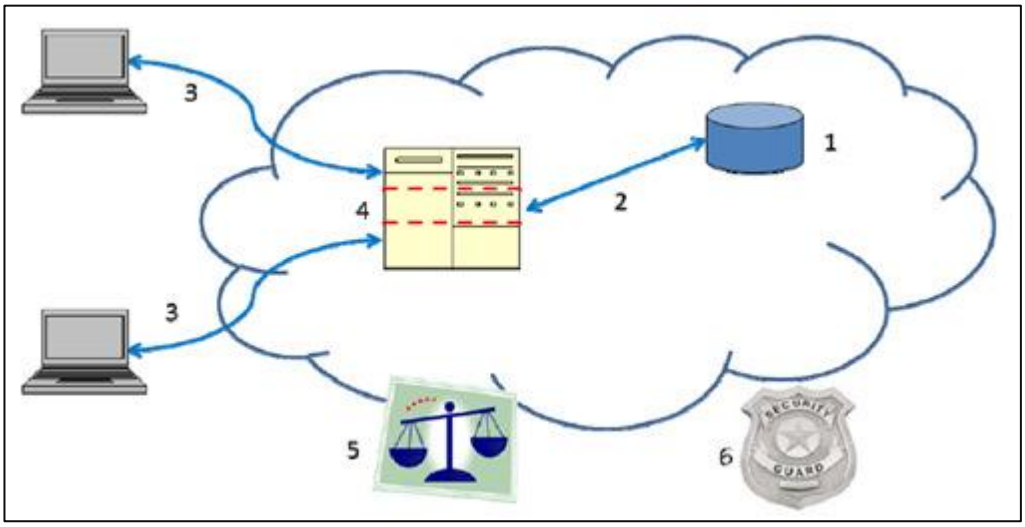

Figure 6. Areas for security concerns in cloud computing: (1) data at rest, (2) data in transit, (3) authentication, (4) separation between customers, (5) cloud legal and regulatory issues and (6) incident response (Sen, 2014)

Encryption is the best solution for data at rest and data in transit. The solution can be implemented using different encryption algorithms. Authentication and access control mechanism are the basic elements of security. It is decided to whom the data is accessible. Customers separation is used to prevent sensitive data from being opened to unauthorized users. Virtual machines are very useful for this job. In addition, there are some regulations and laws published by experts to make cloud systems safe. Compliance with these regulations and laws also plays a critical role in making the cloud system secure. Finally, specifying how the system will behave in the event of an incorrect or malicious behavior by the user is one of the security issues (Sen, 2014).

In terms of cloud computing service models, for SaaS, the service provider is responsible for all security in the infrastructure, as well as physical and environmental security capabilities. For PaaS, the security of the platform on which the application will be installed is the responsibility of the service provider, while the security of the application belongs to the customer. Finally, in the IaaS model, infrastructure security is the responsibility of the cloud provider, while all other security operations belong to the customer (Sahandi et al., 2012).

According to cloud computing service delivery models (SPI), detailed cloud computing security analysis and assessment method studies were carried out (Subashini & Kavitha, 2011) and an architecture in Figure 7 is created (Chen & Zhao, 2012).

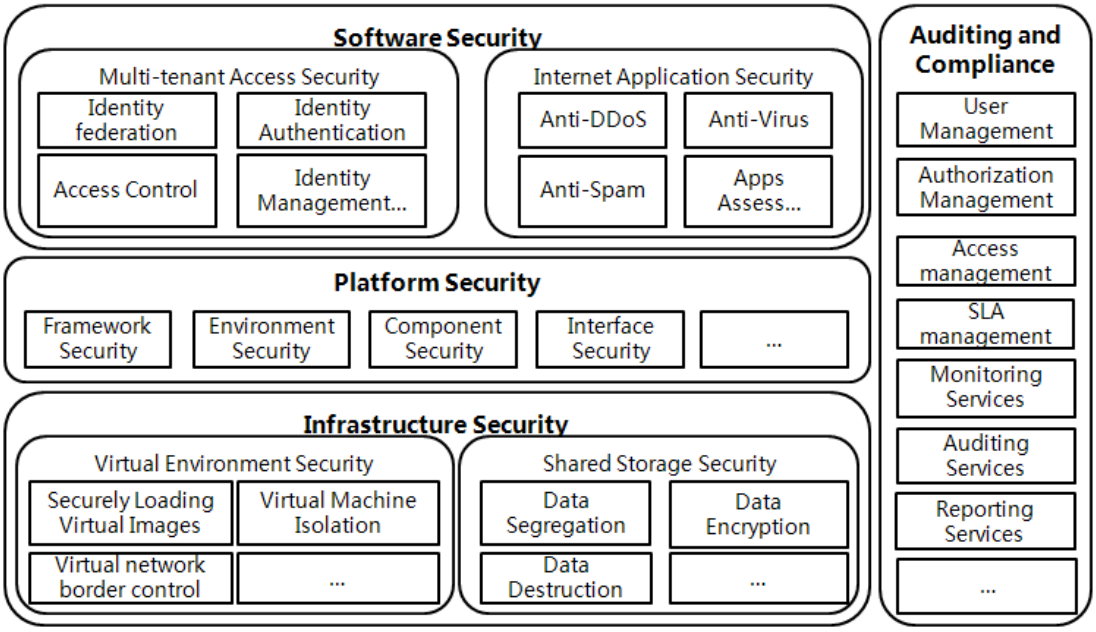

Figure 7. Cloud computing security architecture (Chen & Zhao, 2012)

The cloud requires appropriate control for the user's centralized access, where the user is constrained by the authorization information and identity of each user that needs to use any service provider. Authorization and authentication in the cloud include the procedures for authenticating qualified users and protecting their credentials. It is very important in cloud computing (Bokhari et al., 2016).

The fact that cloud apps are not bound to particular users is one of its key features (Subashini & Kavitha, 2011). It's possible for multiple people to access the same program simultaneously. The vulnerabilities present in conventional Web apps and technologies are also present in cloud applications. The vulnerabilities in online applications in the cloud can prove to be much more damaging than those in regular Web apps, hence the usual security solutions are insufficient for the cloud computing environment (M. Ali et al., 2015).

In PaaS, the service provider supports resources for building programs or applications on top of the service platform, including the operating system platform, programming tools, and storage space. Although some controls are provided to the clients, there are still other security risks that need to be taken into account and controlled that are below the application level, such as network and host intrusion (RoyChowdhury, 2014). Also, developer must be educated for providing their own application security working on the platform. Also, applications should be upgraded frequently (Hashizume et al., 2013).

IaaS security concerns can only be resolved through physical security, and virtualization security. The private cloud appears to have less impact than the public cloud, where IaaS poses the biggest risk (Asma et al., 2012). The use of virtualization technology raises some security concerns for maintaining ownership of data,

independent of location (RoyChowdhury, 2014). The ability to build, clone, distribute, migrate, and roll back virtual machines using virtualization enables users to run a range of applications (Jasti et al., 2010). As long as the virtual machine monitor (low-level software that controls and monitors its virtual machines) is secure, cloud customers using IaaS have more control over security than those using alternative models (Hashizume et al., 2013).The cloud concept is only implemented over the Internet, thus whatever security problems and threats that exist online must also be taken into account while using cloud services (RoyChowdhury, 2014).

The Table 2 shows the definiton of the security parameters. Table 3 shows possible cloud computing threats and the security parameter it matches.

Table 2. Security parameter definitions (Abdulsalam & Hedabou, 2022)

Terminology	**Definition**
Authentication	Establishing the right identity of a user in a system
Integrity	Maintaining the completeness and accuracy of every part of information
Non-repudiation	Avoid the deniability of one's actions
Confidentiality	To ensure the accessibility of information to only authorised users.
Availability	Information is accessible to only authorized users.
Authorization	Access to resources is restricted to only authorized personnel

Table 3. Threat and security parameter matches (Abdulsalam & Hedabou, 2022)

Threat	**Matching Security Parameter**
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

- Immoral use and abuse of cloud computing: Cloud computing technology presents lots of features to users. But full control over this huge structure is hard. Therefore, hackers can use this weakness and attack the structure with some ways like DDoS, password cracking etc. (Abdulsalam & Hedabou, 2022).

- Malicious insider attackers: These attacks are executed from inside of the corporation. Attackers use own privilege access to get private data and not detected by security systems because of legal behaviors. Therefore, it is hard to detect this type of attacks (Ogigau-Neamtiu, 2012).

- Vulnerable programming interfaces: API (Application Programming Interface) is the interface that user interact with the cloud structure. These interfaces bring extra complexity and vulnerability to cloud computing (Abdulsalam & Hedabou, 2022).

- Data leakage and loss: Transfer data over unreliable paths, weak authentication, lack of disaster control are factors that can cause data leakage and loss (Kushwaha, 2021).

- Distributed technology vulnerabilities: Virtualization is presented by multi-tenant architecture that means many users with their access use single application with shared sources. However, a security vulnerability can be created in virtual machines by an inside user (Abdulsalam & Hedabou, 2022).

- Services and account hijacking: This type of attacks is used for the steal credentials for a user. Thus, it can be set a trap for other users with stolen account credentials (Abdulsalam & Hedabou, 2022).

- Anonymous profile threat: An advantage to use cloud computing is less maintenance and manage on the structure. However, it can cause a security issue in the structure. Lack of security in the structure can cause an anonymous profile to leak classified data. (Abdulsalam & Hedabou, 2022).

Table 4 shows the possible causes for each threat in the cloud structure, given the definitions above.

Table 4. Possible causes for each threat (Abdulsalam & Hedabou, 2022)

	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Immoral use and abuse of cloud computing		X	X	X	X	
Malicious insider attackers	X	X	X	X	X	X
Vulnerable programming interfaces		X		X		X
Data leakage and loss		X	X	X	X	
Distributed technology vulnerabilities	X	X				X
Services and account hijacking	X	X	X	X	X	X
Anonymous profile threat		X	X	X	X	

Each cloud, based on deployment class can have different types of threats that presented in Table 5. It shows that when accessability increased internal to external network, vulnerabilities increase in the same rate.

Table 5. Threats for each cloud deployment class (Abdulsalam & Hedabou, 2022)

	Private Cloud	Community Cloud	Public Cloud	Hybrid Cloud
Spoofing		X	X	X
Tampering			X	X
Repudiation			X	
Information Disclosure			X	X
Denial of Service	X	X	X	X
Elevation of Privilege	X	X	X	X

There are some defense mechanisms determined to maximize security and to prevent possible problems against the specified threats (Sen, 2014). Table 6 specifies the

threats and possible defense mechanisms. In addition, defense mechanisms definitions are showed in Table 7.

Table 6. Threats and possible defense mechanisms (Sen, 2014)

Threat	**Possible defense mechanisms**
Spoofing	Authentication Protect secrets Don't store secrets
Tampering	Authorization Hashes Message authentication codes Digital signatures Tamper-resistant protocols
Repudiation	Digital signatures Timestamps Audit trails
Information Disclosure	Authorization Privacy-enhanced protocols Encryption Protect secrets Don't store secrets
Denial of Service	Authentication Authorization Filtering Throttling Quality of service (QoS)
Elevation of Privilege	Run with least privilege

Table 7. Definitions of threat defense mechanisms

Defense Mechanism	**Definition**
Authentication	Act of proving identity of the user (Wikipedia, n.d.-a)
Authorization	Function of specifying access and control rights/privileges to resources (Wikipedia, n.d.-b)

Table 7 (continued).

Hashes	Transforming any given key or a string of characters into another fixed length value (Zola, 2021)
Message authentication codes	To confirm that the message came from the stated sender and has not been changed (Wikipedia, n.d.-e)
Digital signatures	Mathematical technique used to validate the authenticity and integrity of a digital document, message or software. (Gillis et al., n.d.)
Tamper-resistant protocols	Tampering is an intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data (NIST, n.d.).
Audit trails	It is a date and time-stamped, sequential record of the history and details around a financial transaction, work event, product development phase, or financial ledger entry (Auditboard, 2021).
Throttling	Intentional limitation of the communication speed (Wikipedia, n.d.-c)
Quality of service (QoS)	Refers to any technology that manages data traffic to reduce packet loss, latency, and jitter on a network. QoS controls and manages network resources by setting priorities for specific types of data on the network (Lutkevich & Finnell, 2021).
Run with least privilege	Limits users' access rights to only what are strictly required to do their jobs (Rosencrance, n.d.).

2.3. Challenges adopting to cloud computing

2.3.1. Security and Privacy

Security is the highest level of concern in cloud computing, as there are uncertainties about how to fully ensure security at all levels (network, host, application, data, etc.) (Avram, 2014). A survey conducted by International Data Corporation (IDC) revealed that security is one of the biggest problems in cloud computing (Sajid & Raza, 2013).

Data is stored and processed by the cloud provider. This situation can cause problems in terms of data security and confidentiality (Alshomrani & Qamar, 2013). Users may worry about their personal data being stored in this way, because protection of personal data is a human right (Kh. E. Ali et al., 2018). These concerns can be addressed with proper authentication and authorization mechanism (Jadeja & Modi, 2012). In addition, each country's own laws are specified in each country's own laws, which and how much of their data can be stored and processed (Bashari Rad et al., 2017).

Private cloud model used in the defense industry attract the attention of malicious people due to the sensitive data they contain, and the damage to be incurred in a possible attack can be much greater than non-cloud systems. For this reason, all security policies and procedures must be followed in implementation of cloud (Bolin, 2010).

Security is the major element that an organization should take the necessary precautions before making the transition to cloud computing (Bashari Rad et al., 2017).

2.3.2. Reliability/Performance

Critical applications that require 24/7 support can also run in the cloud. The consequences of a failure in the cloud system can be catastrophic for the application. For this reason, failure scenarios should be tested, and necessary precautions should be taken. Although the testing process is extra costly in terms of business, it will prevent a disaster (Avram, 2014). For example, interruption of government operations could be catastrophic. The public and private sectors may be affected. It also reduces trust in the system (Mudawi et al., 2020). Another example is Apple's MobileMe cloud service, which allows multiple devices to sync. When the service was put into use, it worked very slowly due to network problems and made its user unhappy. Therefore, other technology companies have developed the application in such a way as to run the application in the users' locale environment, to provide service to the user even if there is no network connection. Video calling, online games, etc. reliability still poses a challenge to the cloud (Brohi & Bamiah, 2011).

2.3.3. Interoperability

It is the ability of two or more systems to work together by exchanging data (Brohi & Bamiah, 2011). It can be considered as the collaboration of different clouds or the collaboration of an organization and a cloud (Dillon et al., 2010). Many cloud systems

are not designed to interact with each other. This situation creates difficulties for organizations to combine IT systems with cloud systems (Brohi & Bamiah, 2011). To prevent this situation, some standards have been established (Sajid & Raza, 2013). For example, Unified Cloud Interface (UCI) Project proposed by the Cloud Computing Interoperability Forum (CCIF) is a standart for cloud system interfaces (Dillon et al., 2010).

2.3.4. Costs

Obviously, the adopting IT infrastructure to cloud computing will not be without cost. On the contrary, existing IT costs will be replaced by cloud computing costs (Wyld, 2009). While the costs in the existing IT infrastructure are reduced, new costs such as data communication, data migration and virtual machine unit are added (Dillon et al., 2010). There are also some optional cloud computing features that will cost extra. For example, support, disaster recovery, application modification and data loss insurance major benefits of cloud computing (Avram, 2014). Considering all the costs, an organization's strategy for adopting to cloud computing should not be all or nothing. Instead, a portfolio should be prepared by combining the public, private and hybrid options of cloud computing with the existing IT infrastructure of the organization. For example, in an organization where a completely private cloud infrastructure is used, the costs of the cloud may be high as well as security because the burden of the cloud is placed on the organization. Therefore, it has to compromise between cost and safety (Wyld, 2009).

2.3.5. Changes in the IT infrastructure and workforce

In the studies carried out, it has been observed that the IT teams do not want to give up the existing servers easily and they resisted the transition to the cloud model for a while. However, considering the expense of traditional IT infrastructure, the transition to the cloud model is inevitable (Wyld, 2009). Also, IT employees need to keep up with this change. In addition to their existing skills, they should also receive training and develop themselves in cloud computing (Diaby & Rad, 2017). Otherwise, it would be in favor of the organization to retire the employees and replace them with staff with cloud computing capabilities (Wyld, 2009). In addition, some IT workers can lose their jobs as their role is fulfilled by cloud computing (Diaby & Rad, 2017).

2.3.6. Political Issues

For cloud service providers, it is costly and difficult to serve all states on globally. Each state has its own laws. In fact, every institution within the state has its own rules. For this reason, it is difficult to provide a safe service that can comply with all regulations (Wyld, 2009). Especially in the case of sensitive data, governments are more sensitive. For example, the Canadian government requested that the computer working within the US borders should not be used because you are worried about the privacy of Canadian data (Mather et al., 2009). In addition, governments may request that sensitive data be stored where they specify within their boundaries. However, it cannot be guaranteed for the place where cloud service providers are stored (Avram,

2014). Politics affects the development of the cloud-based global economy due to the regulations it constitutes (Parrilli, 2010). Also, cloud customers make an agreement that the provider will guarantee issues such as reliability, performance, and high availability before receiving service from the service provider. This agreement between the provider and the customer is called Service Level Agreement (SLA). Apart from this agreement, the service provider has the right to reject the requests This can create an obstacle for the customer. For this reason, the agreement constantly may need to be customized according to users' feedback (Dillon et al., 2010).

2.4. Critical Analysis of Literature Review

First, the results obtained as a result of the literature review were divided into headings according to the search criteria. Since cloud computing is a very wide issue, research is limited to previous studies in defense industry, security for cloud computing and challenges adopting to cloud computing.

Table 1 includes the cloud computing studies carried out in the defense industry in the last 12 years. The common view in these studies is that if an organization in the defense industry is switched to cloud computing, it should classify the data to store and process sensitive and confidential data in a private cloud class (Onwubiko, 2010). Despite the vulnerabilities mentioned in Section 2.2 (Abdulsalam & Hedabou, 2022)private cloud class is the most secure cloud deployment class for sensitive data (Sen, 2014).

The existing infrastructure(intranet) does not provide the scalability, service reliability, high availability, cost effectiveness, and high responsive fault tolerance features provided by cloud computing (Alambo Tona & Prasad Sharma, 2020). Considering that these features are requirements and cloud computing is a cheaper and faster method compared to the existing on-premise IT infrastructure (Sethi, 2014), the transition to cloud computing is inevitable.

In the USA, which is the pioneer country in the use of cloud computing in the defense industry, cloud computing is defined as the most innovative, efficient, and secure information and IT services (Department of Defense United States of America, 2012). For cloud computing usage, hybrid is used as deployment class and IaaS is used as service class (Powell, 2013). Data is classified according to the impact level and stored on the private cloud or public cloud side of the hybrid cloud (Odell et al., 2015). They also maximized security by providing more control over the infrastructure built with the IaaS service class (Hashizume et al., 2013).

The Chinese, on the other hand, used cloud computing mostly in civilian areas (Lele & Sharma, 2014). On the subject of security, they kept their infrastructure up to date and took the necessary precautions. However, in areas where security is much more important, they emphasized the use of private cloud class instead of public (Ragland et al., 2013).

The Indian Defense Department has also created an encrypted cloud infrastructure for military. It has used private cloud class in the infrastructure and the data center has been built in India (Dudash, 2016). They also supported the use of private cloud class in government applications (Lele & Sharma, 2014). Thus, the private cloud class was once again emphasized in terms of security and privacy.

The United Kingdom, another country that wants to benefit from cloud computing, has directed all its opportunities to cloud computing with its cloud first approach (Sugumaran & Al-Mutawha, 2017). He also emphasized data privacy in the documents that published (The United Kingdom Ministry of Defense. (2013)). It is also seen that the benefits of cloud computing are interesting for countries and countries do not compromise on security.

The Australian Defense Department, on the other hand, gave importance to the use of cloud computing in public areas, but did not include it in the military sector because it found the security insufficient (Lele & Sharma, 2014). However, with the developing security measures, it started to serve in the defense industry with an IaaS service class in 2022 (Hendry, 2022).

The inadequacy of the existing infrastructure in Turkey has been mentioned and a strategy has been published to benefit from cloud computing. The cyber security requirements that must be implemented in the infrastructure are expressed in the strategy. This situation reminds once again the importance of security in cloud computing (Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, n.d.).

Cloud computing can be used in almost every industry, and it can processes and stores different types of data provided by these industries. The most important issue encountered while performing these operations is undoubtedly the security and privacy of the data (Avram, 2014). Each cloud class has its own security and privacy issues (Onwubiko, 2010). Private cloud class is more suitable for security, while public cloud class is more cost effective (Bolin, 2010). In the study conducted by evaluating the data in terms of category, classification, confidentiality, integrity, availability, privacy, and impact, it was concluded that the data at the confidential level is stored and processed in the private cloud structure (Onwubiko, 2010).

In addition, when looking at the security vulnerabilities studies for cloud deployment classes, it is seen that the private cloud structure, which is specified as the most secure class, also has some vulnerabilities (Abdulsalam & Hedabou, 2022). It is also observed that the number of vulnerabilities increases as the cloud deployment class moves from the internal network to the external network, as the working principle. For this reason, it is correct to say that the private cloud class is the most secure class. In addition, there are precautions that can be taken regarding the mentioned vulnerabilities. Cloud security can be ensured by taking the specified precautions and keeping them up to date (Sen, 2014).

In terms of cloud service classes, in the SaaS class, the service provider is responsible for almost all security. In the PaaS class, while the customer is responsible for the

security of the application running on the platform, the service provider is responsible for the security of the remaining parts. In the IaaS model, the service provider is only responsible for infrastructure security, while the security for the remaining parts is the responsibility of the customer (Sahandi et al., 2012). In comparison, if the customer's control over the infrastructure increases, his responsibility for security also increases at the same rate.

Because cloud computing can be used in many sectors, it should be able to provide trust to customers(Avram, 2014). If features such as preventing data loss in a possible disaster, 24/7 customer support, and high availability are not provided to the customer on the grounds that they increase the cost, a possible data loss or interruption may reduce the customer's trust in cloud computing (Mudawi et al., 2020). In addition, the failure of the cloud service provider to offer interoperability systems can put organizations in a difficult position (Brohi & Bamiah, 2011). For this reason, it is recommended to follow some of the produced standards (Dillon et al., 2010). Costs are also one of the emerging challenges in cloud computing transition. Many of the services offered for reliability also bring extra costs (Avram, 2014). For this reason, the organization that transitions to cloud computing must make a trade-off between reliability features and cost (Wyld, 2009). Another issue is that it is for the benefit of the organization that the IT personnel adapt to the changes made in the IT infrastructure. Otherwise, staff may lose their jobs (Diaby & Rad, 2017). Finally, cloud computing providers operating globally are required to provide services according to the laws of the countries (Wyld, 2009). This situation, which creates a disadvantage for service providers, can be solved by determining the requirements and constraints with the Service Level Agreement (SLA). However, with this agreement, when the customer makes a new request, the customer may be at a disadvantage with the right of the service provider to refuse (Dillon et al., 2010).

CHAPTER 3

METHODOLOGY OF RESEARCH

Within the scope of the thesis, a case study, the stages of that are shown in Figure 8, was conducted to find answers to the research questions given in section 1.2. The purpose of the case study is to create a framework that complies with all the constraints and requirements of the defense industry, using cloud computing infrastructure, and to ensure that software can be developed, and this framework verified. In this context, literature review, internet research and interviews were made for answering research question 1, a framework that allows software development using cloud computing infrastructure was created for answering research question 2, and created framework was verified for answering research question 3. As a result of the study, the findings were evaluated, and the problems encountered were compared with the examples in the literature and solutions were suggested.

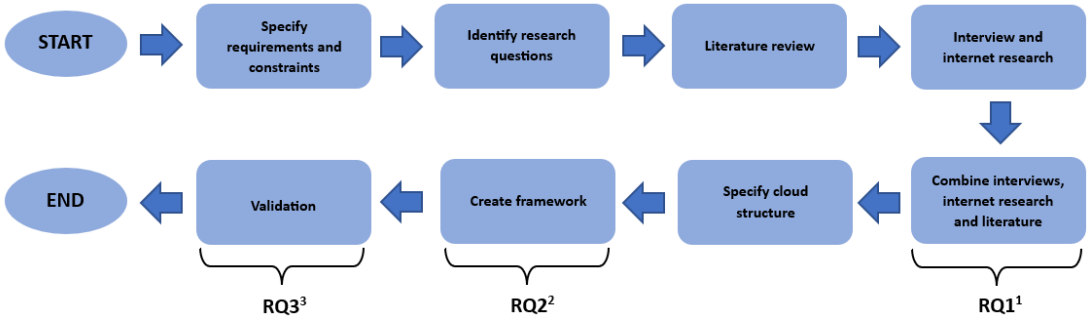

Figure 8. Flow diagram of the case study

During the study, data collected by using a qualitative approach. Interviews were made with 13 employees who have knowledge in cloud computing within the organization and the questions in appendix A were asked. In addition, internet research and academic literature review were made. When the results are compiled, it is recommended to choose a cloud class isolated from the external network and completely under organizational control in order to comply with the constraints and requirements of the defense industry. For this reason, private cloud was chosen as the

---

[1] Research question 1 is addressed here

[2] Research question 2 is addressed here

[3] Research question 3 is addressed here

deployment class and IaaS as the service class, and a framework was created on this infrastructure.

Since the infrastructure is under organizational control, the created framework works by communicating with cloud servers in the IT department. Any packet request that a user makes through the framework on his computer is first checked in repository on the internal network. If the package is found here, it is presented to the user. However, the package is not found, the IT department is contacted through predetermined network paths and the package is requested. The packet is brought by the IT department from trusted sources on the external network and passed through the firewall. If it is found safe, it is sent to the repository in the internal network and to the user who made the request. If it is not found safe, the request is rejected, and the packet is destroyed in its isolated environment. In the scenario where the package is found safe, the user who obtains the package makes the necessary software developments and sends it to the code repository. After a series of automated testing and packaging processes that take place here, the generated software version is sent to the OpenShift development environment. Afterwards, stable versions determined by the user are sent to the Rancher deployment environment. The main reason for keeping development and deployment environments separate and using different software is to prevent possible confusion and provide ease of use. The working logic of the framework is shown in Figure 9.

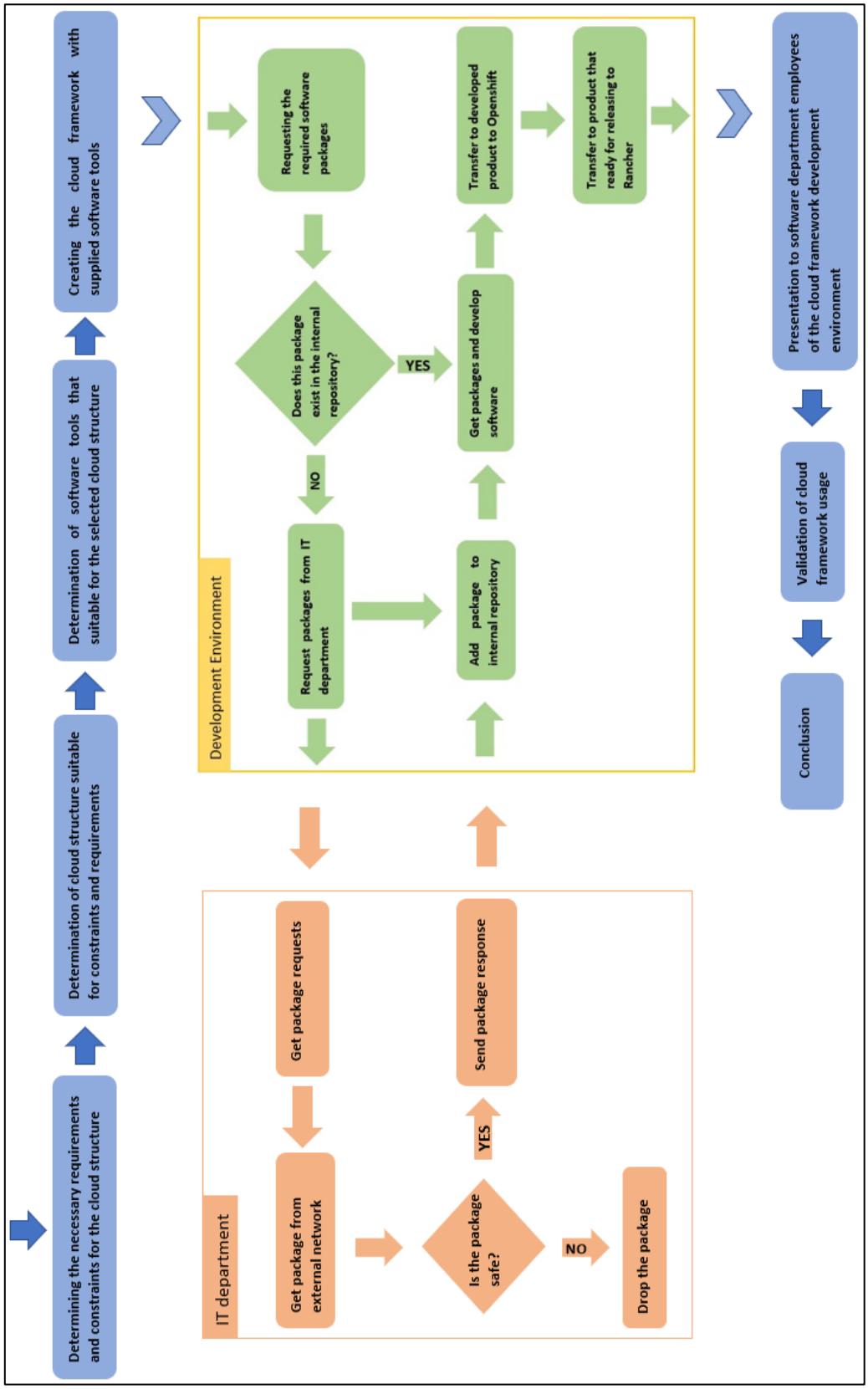

Figure 9. Working flow of the framework

3.1. Requirements and constraints

The biggest constraint brought by the defense industry is security and privacy. It was requested that the measures to be taken on these issues should be given priority. For this reason, it was decided to establish authentication and authorization mechanisms while creating the framework. In addition, while granting authorization to users, the run with least privilege principle is applied to ensure that users are not given unneeded privileges. During the packet transfer, the filtering ability of the IT department with the firewall was used.

The framework running in the software development environment should never be connected to the external network and should perform all operations on the internal network. In addition, the framework on which critical applications can be developed should also provide scalability, high fault tolerance, high availability, and service reliability.

3.2. Tools

Spring is an open-source framework for the Java programming language. It is preferred because of its easy integration and modular structure. It consists of different modules with database connection, web interface and container services (IBM, n.d.).

Maven is the necessary automation tool for software development. It has been preferred because of its ease of integration, dependency control and development environment possibilities (Apache Maven Project, n.d.).

YogaDNS is a routing application that enables receiving and processing DNS (Domain Name System) requests coming to it. It allows users to define rules, operate them and configure addresses (YogaDNS, n.d.).

Gitlab is a repository where the code and development environment parts are located, and the public and private options are available. It provides fast code integration and backup without disk (GitLab, n.d.).

Jenkins is an open-source continuous integration (CI) and continuous delivery/deployment (CD) tool used in project development in the software world. The main task of the tool is to facilitate the management of software development processes. It executes the build operations by taking the resources specified in the CI process. After the compilation process is finished, it executes the predefined test operations. If there is no error in this process, it is passed to the delivery process. However, if any error is detected, feedback is given to the user and the process is stopped. The project, which passes the tests without any errors, is stored as a workable package. The aim is to make the project ready for the real working environment and to store it that way. Apart from these studies, it is also frequently used in software version control and announcement processes (Toro Marin, 2019).

Rancher is an open-source virtualization management tool that provides container management. Since it uses Kubernetes in the background, it provides tracking and management of the work carried out in containers. When any application crashes, it ensures that it is reactivated and load balanced. Its difference from other cloud management tools is that it allows much larger scale container management (Toro Marin, 2019).

OpenShift is an open-source service that works just like Kubernetes. It provides management of services, reporting of statuses, management of data traffic. Tools, languages, databases, and applications to be used in a software system are stored in this system. It is the control system required for re-booting a crashed application via a new pod. Java, Ruby, Python, PHP, Perl, JavaScript languages are supported. Scaling and backup are executed automatically. It is a paid service (Lomov, 2014).

Although both OpenShift and rancher services provide Kubernetes-based management, they have some differences. OpenShift is a tool that takes longer to install process due to its content. However, users can give feedback to the problems encountered in it. While Rancher adheres to industry standards, OpenShift releases new versions based on feedback. While Rancher has limited supporters, OpenShift is supported by worldwide partners such as OCM and IBM. OpenShift has more security controls for users' applications and data sharing. Rancher, on the other hand, is a more preferred tool for managing CI/CD processes (Rancher By Suse, 2021).

The company private firewall is a gateway system developed by the Defense Industry at the EAL4+ security level. The aim is to provide a two-sided and reliable data flow between the servers. It is used to filter request and response packets and provides encrypted protection.

Nexus is a repository manager that hosts docker packages with the rpm extension. It can work as an agent in different networks by allowing different users. This structure enables end systems in different locations to communicate with each other. It is compatible with tools like Eclipse, Jenkins, and Docker (Moore, n.d.).

Yarn was used instead of npm as the package manager. Yarn commands are preferred because they are shorter and more effective. For npm, the commands to run an action are longer and more complex. In addition, unnecessary packages are also downloaded. Therefore, the more practical yarn was preferred. Yarn has license checking capability to ensure package integrity and security. It allows to manage the package download process more securely. Both npm and yarn contain a cache function for quick access to downloaded packages. Yarn installs all packages simultaneously, while Npm installs sequentially. This provides speed in the use of yarn (Jacobs, 2019).

3.3. Implementation

Spring is a framework and Maven is a tool used for software backend development based on Java projects, and yarn is a package manager tool used for software frontend

development based on JavaScript projects in the organization. Under the normal conditions, the package requests that these tools depend on are used by downloading them directly from the internet. However, the framework in our study is prohibited from connecting to any external network. Therefore, dependent packages that used for the projects are hosted in nexus repositories. YogaDNS first forwards packet requests from the user to the nexus repository in the internal network. If the dependent package is in the nexus repository in the internal network, the package is delivered directly to the user. But if the packet is not found nexus repository in the internal network, the request is forwarded to the nexus repository in the IT department (Figure 10).

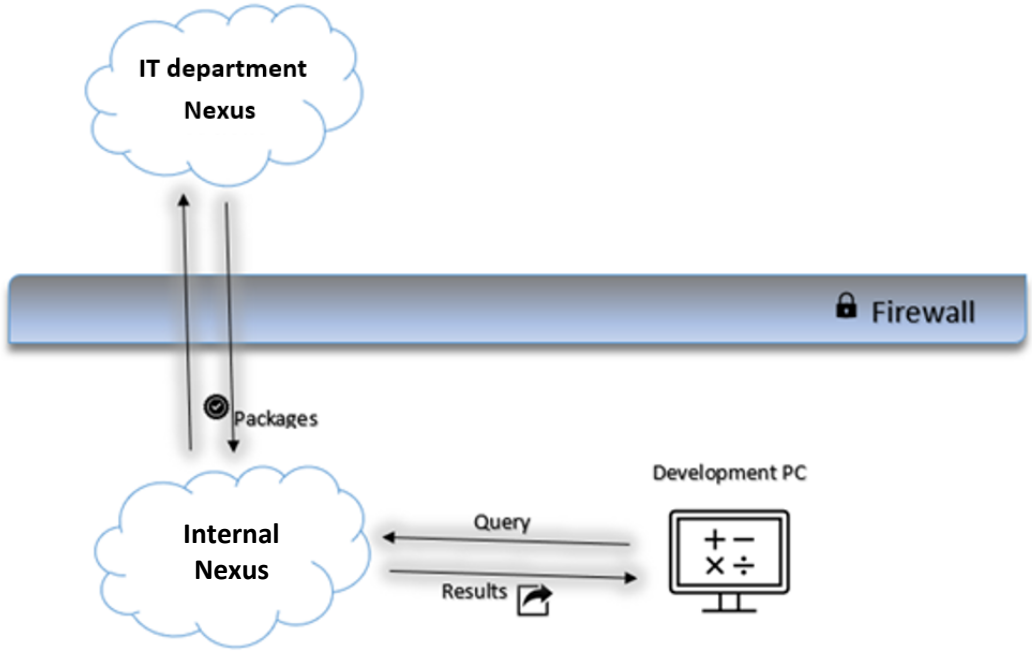

Figure 10. Flow of the package request between internal nexus and IT department nexus

After the necessary packages are obtained, software developments are implemented by the user and the codes are stored in the GitLab code repository. Any code changes here trigger Jenkins and starts a series of testing and packaging processes. It initiates the continuous integration process by performing predefined tests on the codes. If the codes do not pass the test, it informs the user about it and stops the rest of the process. If the codes pass the test, it starts the continuous delivery/deployment process, turns the codes into an executable package and uploads them to the OpenShift development environment.

OpenShift is a container orchestration and cloud managements system. It is used for development environment. In case of any integration problems, packages are stored in this area due to the low cost of error. In addition, OpenShift meets the requirements with scaling and backup features on servers. When stable version is decided for software, stable version packages are stored in a separate cloud called Rancher which is the deployment environment (Figure 11).

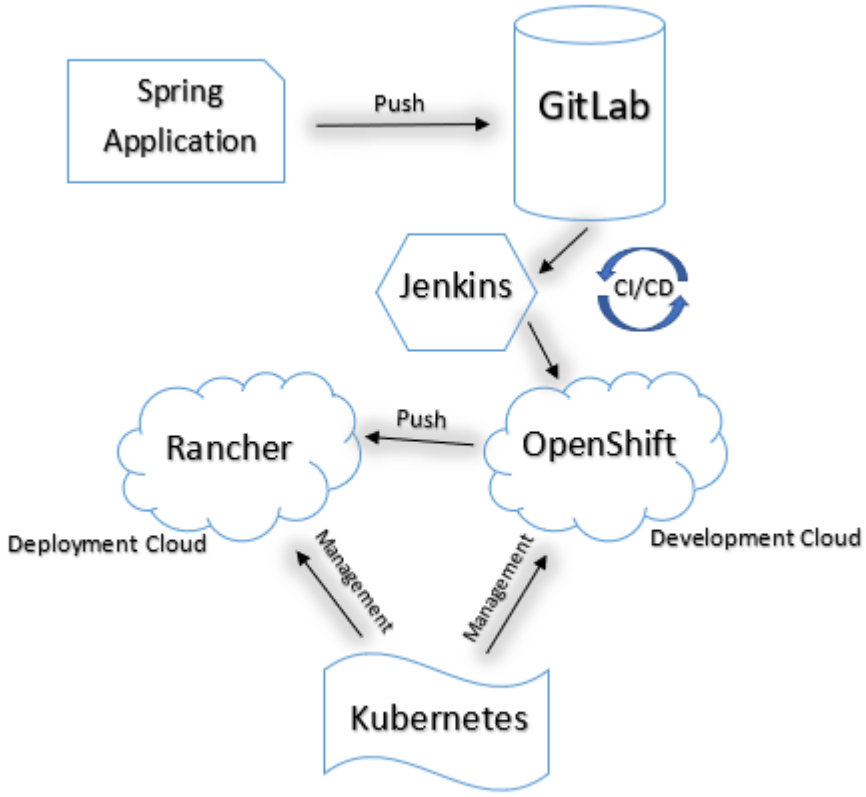

Figure 11. The architecture designed for cloud development

Nexus repository manager works on both internal network and IT department. An admin user has been created for the management of this repository. Only authorized personnel who know the admin username and password are allowed to interfere with the packages. On the other hand, it is a one-way request flow from user to nexus repository. A limited authorized user can only receive a package from the nexus repository and cannot send any packages.

Passing through the firewall of the package obtained by the IT department nexus repository may vary depending on the package size. Because large packages take a long time to transfer, the user displays the package as not found and the software development process is interrupted. To solve this problem, a development was made within the framework and the package size was checked for firewall scanning.

Timescale database was used in the study. Timescale database is used for event logging. All logs created by users are recorded in the Timescale database. It is possible to record from all servers in the same cluster to this time-based database.

Each operation made in a time sequence is logged. Each of the transfer, integration, pull and push operations of a package are recorded. Thus, the events of the last few

minutes can be played back if needed. Before the events are recorded in the Timescale database, they are recorded in a in memory database called Redis. This database is located in each server and works with memory logic. This database, which has a simple key, value logic, acts as a temporary area during the operation of the system. Data is recorded on a per second basis.

In addition, the intrusion detection system (IDS), which is instantly alarmed in case of a possible suspicious situation, is integrated into the cloud framework to increase security. Traffic flows through this system and is analyzed with machine learning. In case of suspicious packet flow or user act, it notifies authorized users by giving an alarm without interfering with the traffic.

With the help of an external tool, the data is taken from this field and saved in the Timescale database, which is the real database. Since the servers are in the same cluster, they share the same time zone. Thus, there is no time-dependent data conflict in the Redis temporary field.

The danger here is that in case of temporary or permanent crash of the server, the data in the Redis field will be lost without being recorded in the Timescale database. As a precaution against this situation, the advantage of cluster structure with more than one server was used. There are common Redis on each server and they are copies of each other. All the instantaneous data are available in all Redis. Thus, it was possible to take precautions against a possible collapse.

One of the processes in the background is to convert and save the data to the desired format. Easy-to-use protocol buffers are used for data storage. Data is written and read in byte type and converted to each other.

After the all implementation process is finished, cloud framework is presented to software development department. Following section, the survey study results are presented to validate framework is implemented and work correctly.

CHAPTER 4

VALIDATION

Within the scope of the thesis, cloud deployment and service classes were examined, and a literature was reviewed. The results obtained from the literature review were evaluated by comparing them with the constraints and requirements of the defense industry. As a result of the evaluation, a cloud framework was created using a private deployment class and IaaS as a service class. The framework has been made available to defense industry employees. The framework was started to be used in 9 different military projects and it was used for approximately 8 months. The projects are designed according to the constraints and demands of the defense industry to serve the army.

A survey study was conducted to verify the use of the framework by the employees. As seen in the Figure 12, 95 employees from different positions and titles participated in the survey. The survey was conducted with the system usability scaling method, which is a reliable validation method for a system (Brooke, 1996), and the questions directed to the employees are given in appendix B. Employees were asked 10 questions and they were asked to answer the questions as 1-5, 1 strongly disagree and 5 strongly agree.

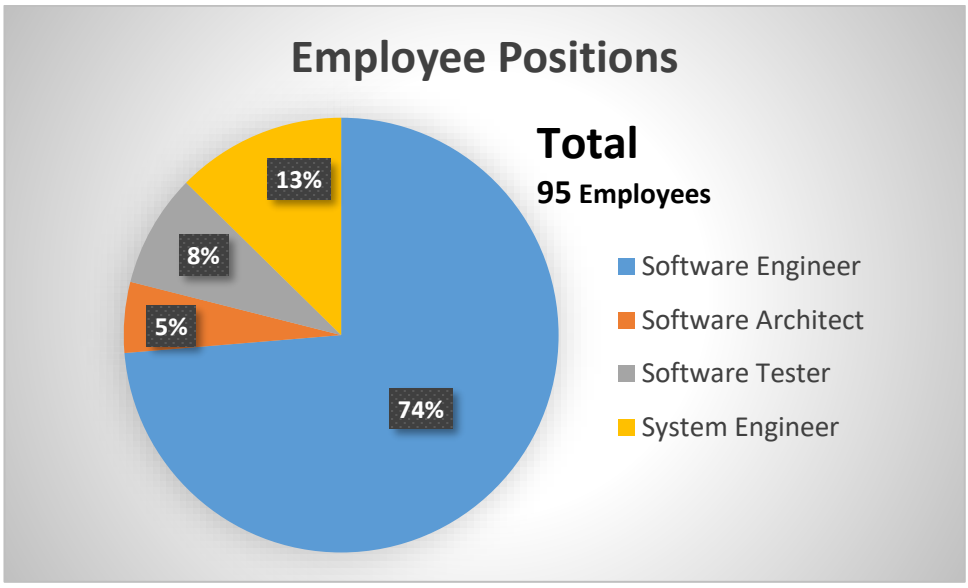

Figure 12. Employee position distribution chart

To calculate the SUS score, first sum the score contributions from each item. Each item's score contribution will range from 0 to 4. For items 1,3,5,7, and 9 the score contribution is the scale position minus 1. For items 2,4,6,8 and 10, the contribution is 5 minus the scale position. Multiply the sum of the scores by 2.5 to obtain the overall

value of SU. SUS scores have a range of 0 to 100. According to Figure 13, while 80 and above are excellent, between 68 and 80 are good, and 68 is considered okay, the system should be researched according to scores below 68 (Brooke, 1996).

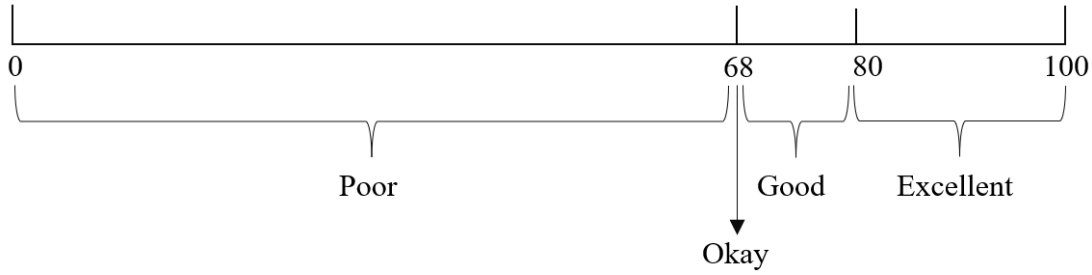

Figure 13. System usability scale measurement

According to the survey results in Figure 14, 65% of 95 employees found the framework excellent, 27% good, 5% okay, and 3% poor. While evaluating the survey results, the calculations suggested in the literature were implemented. In this case, looking at the chart in Figure 14, the sum of excellent, good and okay levels is 97%. The result proves the usability of the framework.

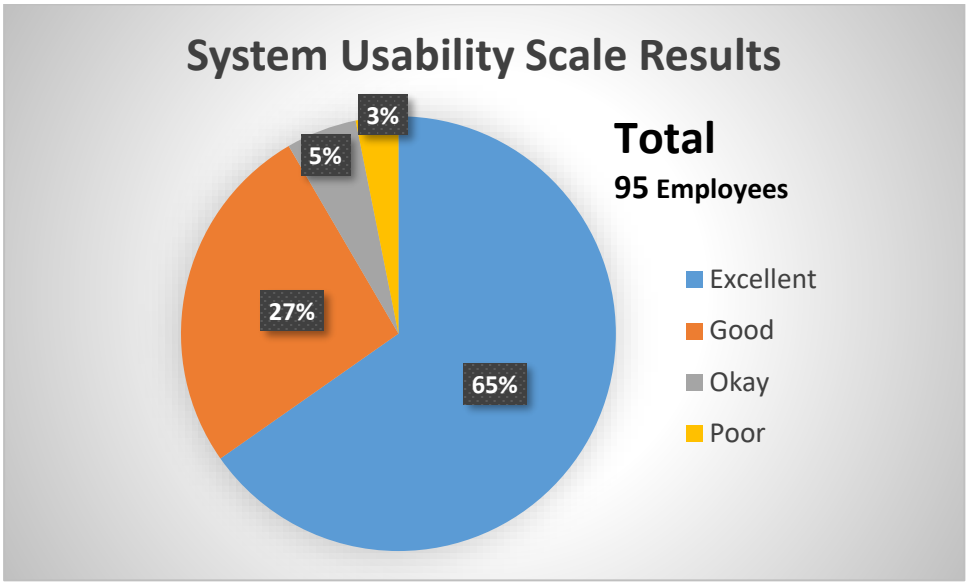

Figure 14. System usability scale method result chart

As can be seen in Figures 15, 16, 17 and 18, it has been revealed that the framework is mostly liked by software engineers and software architects. There appears to be a more diverse distribution for system engineers and software testers.

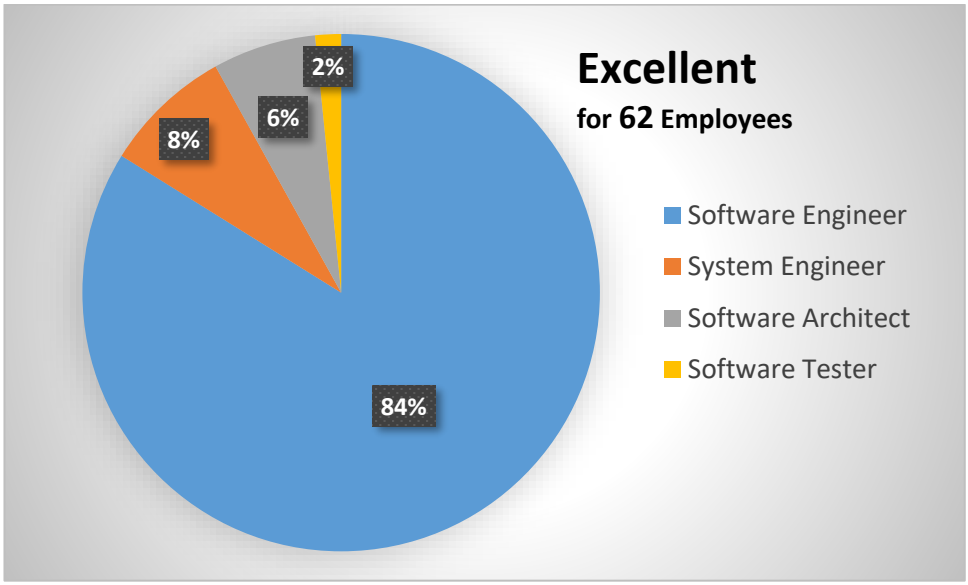

Figure 15. Distribution chart of the excellent result by positions

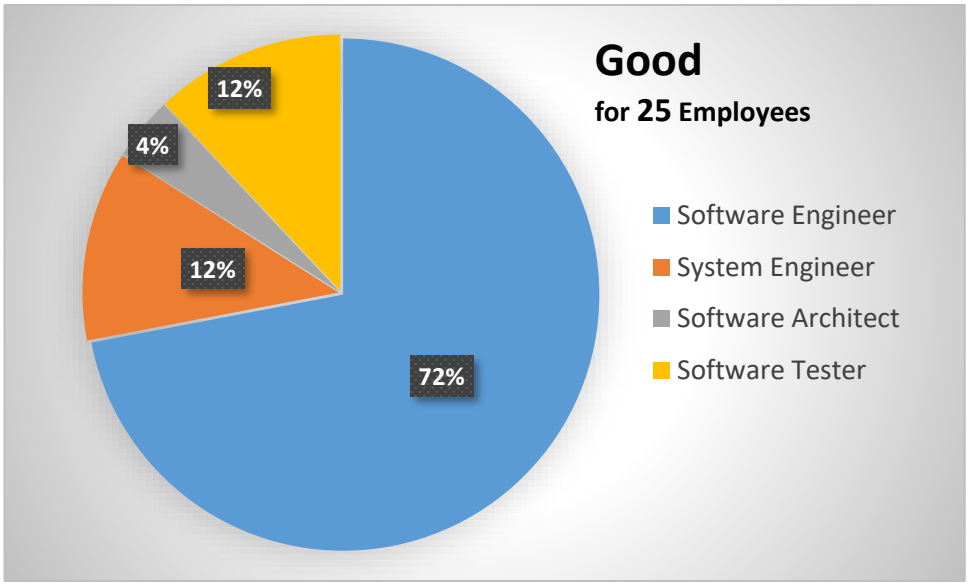

Figure 16. Distribution chart of the good result by positions

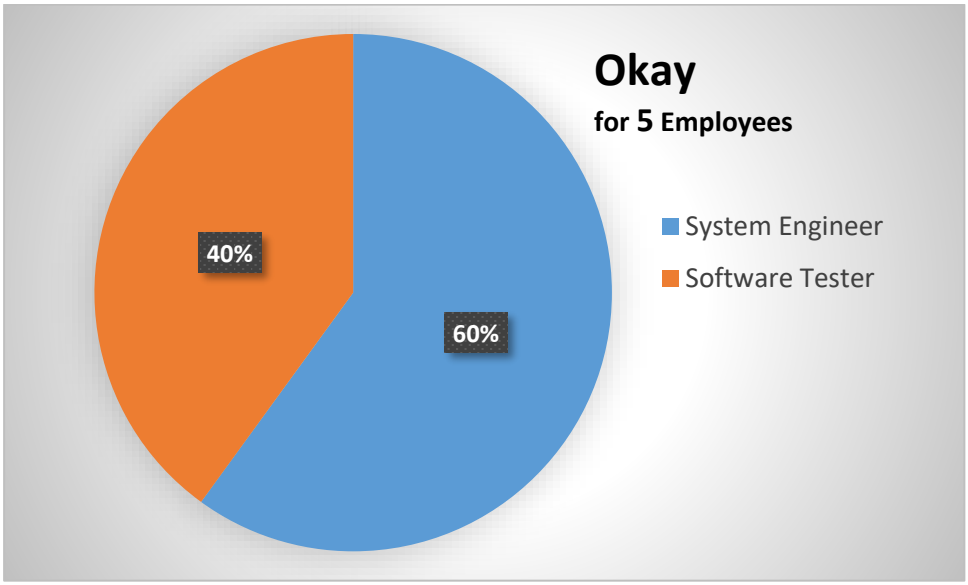

Figure 17. Distribution chart of the okay result by positions

It was revealed that system engineers and software testers had problems with the framework in Figure 18. System engineers and software testers were asked about their difficulties using the framework to find the cause of the problems. In the answers given by the employees, it was determined that the problem was caused by the fact that they could not use the framework properly due to network problems related to IT department.

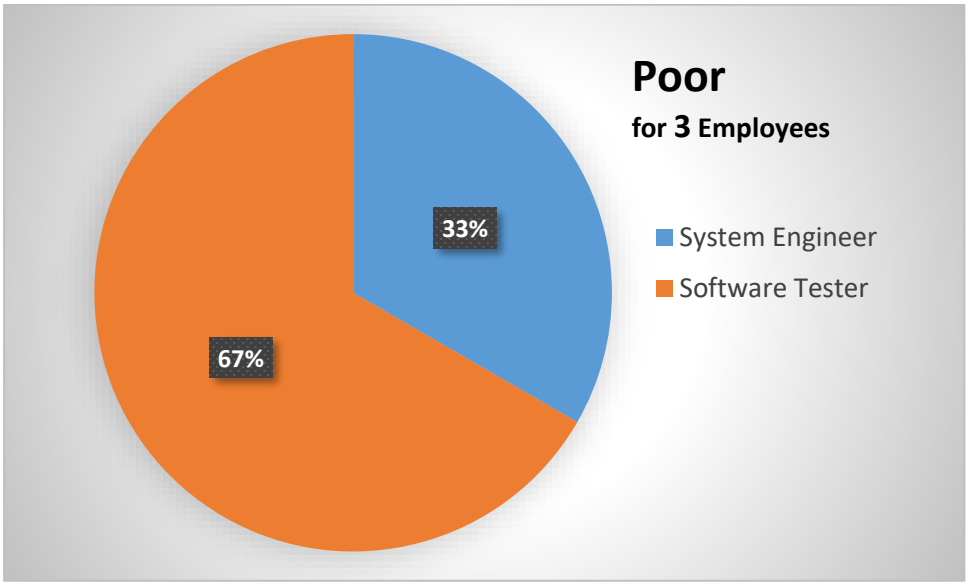

Figure 18. Distribution chart of the poor result by positions

When the same question was asked to software engineers, software architects, system engineers and software testers who found the framework is successful, it was revealed that software engineers and software architects were able to reach a solution because

they had encountered the problem before or based on the training they received on the subject.

In this section, the cloud framework created was verified by conducting a survey with the system usability scale method. When the results are compared with the limit values of the system usability scale method, it is confirmed that the framework is usable. In addition, the results were evaluated in the discussion section.

CHAPTER 5

DISCUSSION

In this section, the findings obtained as a result of the study are compared with the studies in the literature. Similarities and differences were discussed, and their reasons were examined. In addition, some explanations were made about the findings and validation.

Although cloud computing is not a new concept, it has been seen that security factors are the main reason why it took its place in the defense industry late. In this respect, it has been seen that it is similar to the defense departments of other countries (Department of Defense United States of America, 2012). In the study, a cloud framework was created using private cloud as the deployment class and IaaS as the service class, in line with the constraints and requirements determined by the defense industry. When the created cloud framework is compared with the studies in the literature, similarities and differences are seen. First of all, in the previous cloud computing studies conducted in the defense industry, given in Table 1, it was revealed that the private cloud was proposed in systems where data security and privacy were the major problem. The private cloud that used in the study supports the literature.

This study was carried out in the defense industry because the existing IT infrastructure was not sufficient for scalability, service reliability, high availability, cost effectiveness, high responsive fault tolerance and high performance with security provided features, and there were similarities in the studies conducted for cloud computing transition of on-premise IT infrastructures in the literature (Alambo Tona & Prasad Sharma, 2020).

When the studied about defense departments of the countries are examined, they have studies to make innovations in USA Department of Defense legacy applications and to transfer services such as data storage (Odell et al., 2015) from the existing IT structure to an operationally efficient, secure, cost-effective, scalable infrastructure (Powell, 2013). Cloud computing was deemed appropriate as the most innovative, efficient, and secure IT service for this process (Department of Defense United States of America, 2012). The use of cloud computing by the USA Department of Defense is similar to the purpose of our study. They used hybrid as cloud deployment class and IaaS as service class (Powell, 2013). The use of IaaS as a service class in order to increase security was similar to our study. Because all infrastructure control belongs the organization (Odell et al., 2015). But it differed with our work as a deployment class. While the USA Department of Defense classifies the data and processes it in the hybrid cloud, all the data used in our study is stored in the private cloud model due to its confidentiality.

The Chinese Government has heavily used public cloud in civilian areas (Lele & Sharma, 2014), while they emphasized private cloud when it comes to security and military use (Ragland et al., 2013). Similarly, the Indian Department of Defense has proposed a private cloud for noncommercial data. They have created an encrypted cloud infrastructure headquartered in India to store personnel and operational data (Dudash, 2016). Both China and India emphasize the private cloud for data privacy. In addition, the United Kingdom has adopted a cloud first approach to benefit from the capability of cloud computing (Maude, 2013). Data privacy is emphasized as the main issue in the document they published (The United Kingdom Ministry (2013)). The Australian Department of Defense is also a country that spends a lot of money on the adoptation to cloud computing. Although it has taken its place in the defense industry late due to security problems (Lele & Sharma, 2014). It has started to take its place with the IaaS service class (Hendry, 2022). Another factor supporting our work is that the private deployment model and IaaS service model are considered by the United Kingdom and Australian Department of Defense in areas where security and privacy are important. In addition, the cyber security requirements of Turkey in its cloud computing strategy also emphasized the importance of security (Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, n.d.).

In literature studies where security and privacy are the main issues, it has been concluded that private cloud is the best option (Onwubiko, 2010) because control and configuration belong to the organization (Sen, 2014). In addition, as a service class, IaaS has been described as more secure than other service classes (Hashizume et al., 2013).In SaaS and PaaS service classes, the control of the service provider in the cloud infrastructure poses a security threat (RoyChowdhury, 2014).

When the cloud deployment classes specified in Table 5 are examined, it is seen that the least vulnerability is in the private cloud compared to other cloud classes (Abdulsalam & Hedabou, 2022). For this reason, private cloud is the most suitable cloud deployment class in systems where security is critical. Although it is stated as the most secure cloud class, there are some security vulnerabilities. Defense mechanisms listed in Table 6 have been developed against these vulnerabilities (Sen, 2014). Authentication, authorization, filtering, run with least privilege features (Sen, 2014) used in the study are similar to the defense mechanisms given for private cloud in the literature in order to increase security. Unlike the study, encryption (data at rest and data in transit), incident response, throttling, quality of service (QoS) features (Sen, 2014) in the literature could not be implemented in the first stage when the framework was created. It is being evaluated for future work.

In the literature review section, the difficulties experienced in the transition to cloud computing are also stated. The most important of these challenges is security and privacy ((Sajid & Raza, 2013), (Avram, 2014)). Potential difficulties have been minimized by developing the framework created in the study based entirely on security and privacy elements (Bashari Rad et al., 2017). Another requirement of the defense industry is high availability. If a running cloud infrastructure experiences high availability issues, trust in the system decreases (Mudawi et al., 2020). Because

applications that should always be running state in the established framework can be developed. A possible system outage can be catastrophic for these applications (Avram, 2014). In order to overcome this challenge and ensure high availability, generators and uninterruptible power supplies (UPS) in the IT infrastructure were used and possible interruptions were prevented. In addition, ready-to-use backup servers are constantly kept on standby. The interoperability problem arising from the incompatibility of cloud systems with each other (Brohi & Bamiah, 2011) was not encountered in the cloud infrastructure created. Since the infrastructure management is completely owned by the organization, services were not received from different cloud service providers. Another problem mentioned in the literature review is cost. Changing the existing IT infrastructure brings some costs (Wyld, 2009). However, since the defense industry is very strict in terms of constraints and requirements, the desired features were specified beforehand and unexpected costs did not arise. In addition, it has been stated that in organizations using private cloud, the cost is as high as security. By sacrificing security, it is possible to get services from a service provider and reduce costs (Wyld, 2009). Since safety is the main factor in our work, no compromises have been made in any way. As another challenge stated, the changes in the IT infrastructure did not create major problems in the study. Because in a large-scale organization, IT infrastructure and personnel can resist changes and prefer to use the existing ones (Wyld, 2009). The IT infrastructure is prepared for change, as the demands and constraints are specified in advance. However, it has been observed that training the personnel who will use the framework will increase the validation of use of the framework. There may be policy problems in services received by a cloud provider (Parrilli, 2010). The service to be provided is determined by the Service Level Agreement (SLA) and the service provider has the right not to fulfill the requests other than this agreement (Dillon et al., 2010). In the study, there was no problem because the cloud infrastructure and the service to be provided belong to the organization.

In addition, according to the results in the validation section, the framework was found to be successful by 97% of the employees. When the problem experienced by 3% of the employees was examined, it was seen that it was caused by the network. It has been observed that employees who find the framework successful and encounter this problem have experienced the problem before or received training on this subject. For this reason, prior training for the employees who will use the framework will increase the success rate of the framework.

CHAPTER 6

CONCLUSION

The thesis study has shown how a cloud framework can be created in defense industry organizations where security and privacy are critical, the possible difficulties that may be encountered while creating this framework, and how valid it is for using after the framework is created. For the study, private cloud was chosen as the deployment class and IaaS was chosen as the service class. Other cloud classes in the literature were also examined and private and IaaS were observed as the most secure classes. In addition, as one of the constraints brought by the defense industry, the cloud infrastructure to be created should not be connected to any external network. It is not possible to provide this with other deployment cloud classes other than private cloud. Also IaaS was chosen to be able to control all infrastructure management within the organization in order to maximize security instead of receiving services from any cloud provider. In other classes of service clouds other than IaaS, service providers play a role in management at different levels.

While creating the framework, the limits, and requirements (security, confidentiality, high availability, service reliability, high responsive fault tolerance, high performance and scalability) brought by the defense industry were taken into account. Solutions created for similar problems in the literature have been applied to the difficulties that arise while fulfilling these requirements.

As security and privacy are taken as a basis in the created cloud framework, priority has been given to these issues. Although the private cloud is determined as the most secure cloud class, it has been determined that it is not 100% secure. Despite the security vulnerabilities it has, some precautions have been developed. Authentication and authorization mechanisms, which are also mentioned in the literature, have been established. In addition, by adopting the run with least privilege principle, users are not given unneeded privileges. In addition, a logging system has been integrated into the framework in order to track the movements of the users in the framework and to identify in a suspicious situation. All packages and libraries used within the cloud framework are filtered by the organization firewall. Another recommended security measure is encryption. Security can be increased by encrypting the data at rest and data in transit. However, this mechanism could not be integrated since there was a time constraint in the first stage when the framework was created, and it was foreseen to be integrated for future studies. Likewise, the proposed throttling, and quality of service (QoS) defense mechanisms were also planned for future developments.

Unlike the literature, an intrusion detection system (IDS) is integrated into the cloud framework. With this system, traffic is only analyzed with machine learning and alarmed. However, after the alarm is given, the response time of the authorized person to the system may be long. In this case, the system may be damaged. For this reason,

it has been seen that the framework is sufficient for the first stages but needs to be developed for the later stages.

At the end of the study, a questionnaire study was conducted to verify the use of the framework. According to the survey study, it was seen that some users had difficulties in using the framework and the reasons were investigated. While 97% of the employees found the use of the framework acceptable and above, 3% of them responded to the revision of the framework. When these employees were interviewed, it was understood that the problem they experienced was a network problem that occurred during the installation of the framework and should be resolved with the IT department. When interviewed users who did not experience this problem, it was concluded that they had the knowledge to solve the problem, or they knew the solution because they had experienced the problem before. For this reason, personnel training was planned to solve possible problems.

As a result, a cloud framework has been created in line with the constraints and requirements given in the defense industry. Necessary measures have been taken for framework security and planning has been made for deficiencies. The difficulties encountered while creating the framework were overcome by taking examples from the relevant literature studies. Finally, the framework was validated by users through a survey study. Thus, it has been proven that software development can be done safely using cloud computing in the defense industry and contributed to the literature.

6.1. Suggestions for future work

According to the results obtained at the end of the study, future studies can be made to improve the framework and infrastructure. First of all, encryption, throttling, quality of service (QoS) defense mechanisms given in the literature can be added to increase security. Instead of IDS, a more advanced and machine learning-based intrusion prevention system (IPS) can be used to instantly intervene in the traffic flow in a suspicious situation, allowing the system to take control of the situation with minimal or no damage. In addition, possible security problems can be prevented in advance by following the security procedures for cloud computing published by organizations such as NIST and OWASP. After any update to be applied, users can be informed and the survey study in the verification part can be repeated. Thus, a problem that can be occurred after the update but can only occurred during usage will have arisen. With the system up-to-date and the environment of trust created by the private cloud, its use in the defense industry will become widespread. The management of the cloud infrastructure can be facilitated by providing integration with central management tools for the created framework.

REFERENCES

Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. In *Future Internet* (Vol. 14, Issue 1). MDPI. https://doi.org/10.3390/fi14010011

Alambo Tona, A., & Prasad Sharma, D. (2020). DPS-AA: Intranet Migration Strategy Model for Clouds. *International Journal of Modern Education and Computer Science*, *12*(5), 55–63. https://doi.org/10.5815/ijmecs.2020.05.05

Ali, Kh. E., Mazen, Sh. A., & Hassanein, E. E. (2018). A proposed hybrid model for adopting cloud computing in e-government. *Future Computing and Informatics Journal*, *3*(2), 286–295. https://doi.org/10.1016/j.fcij.2018.09.001

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*, 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Almorsy, M., Grundy, J., & Müller, I. (2016). *An Analysis of the Cloud Computing Security Problem*.

Alshomrani, S., & Qamar, S. (2013). Cloud Based E-Government: Benefits and Challenges. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING*, *4*(6). www.ijmse.org

Apache Maven Project. (n.d.). *What is Maven?* Retrieved May 3, 2023, from https://maven.apache.org/what-is-maven.html

Ashraf, I. (2014). An overview of service models of cloud computing. *International Journal of Multidisciplinary and Current Research*, *2*(1), 779–783.

Asma, A., Chaurasia, M. A., & Mokhtar, H. (2012). Cloud Computing Security Issues. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, *1*(2).

Auditboard. (2021, July 26). *What Is an Audit Trail? Everything You Need to Know*. https://www.auditboard.com/blog/what-is-an-audit-trail/

Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, *12*, 529–534. https://doi.org/10.1016/j.protcy.2013.12.525

Bashari Rad, B., Diaby, T., & Ehsan Rana, M. (2017). Cloud computing adoption: A short review of issues and challenges. *ACM International Conference Proceeding Series*, *Part F129684*, 51–55. https://doi.org/10.1145/3108421.3108426

Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K. (2016). Cloud computing service models: A comparative study. *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 890–895.

Bolin, J. S. (2010). *Use case analysis for adopting cloud computing in Army test and evaluation*. https://hdl.handle.net/10945/5125

Brohi, S., & Bamiah, M. (2011). Challenges and Benefits for Adopting the Paradigm of Cloud Computing. *International Journal of Advanced Engineering Sciences and Technology*, *8*.

Brooke, J. (1996). SUS: A "Quick" and "Dirty" Usability Scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & I. L. McClelland (Eds.), *Usability Evaluation in Industry* (pp. 189–194). Taylor and Francis.

Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, *1*, 647–651. https://doi.org/10.1109/ICCSEE.2012.193

Cheng, Y. (2022). Design and Implementation of Cloud Computing Network Security Virtual Computing and Defense Technology. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/7876199

Cho, S., Hwang, S., Shin, W., Kim, N., & In, H. P. (2021). Design of military service framework for enabling migration to military saas cloud environment. *Electronics (Switzerland)*, *10*(5), 1–18. https://doi.org/10.3390/electronics10050572

Choi, S. O., & Kim, J. B. (2021). National Defense Cloud Strategy. *Proceedings - 2021 21st ACIS International Semi-Virtual Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD-Winter 2021*, 87–89. https://doi.org/10.1109/SNPDWinter52325.2021.00026

Deparment of the Environment and Energy Australian Government. (2019). *Cloud Strategy*.

Department of Defense United States of America. (2012). *Cloud Computing Strategy*.

Diaby, T., & Rad, B. B. (2017). Cloud Computing: A review of the Concepts and Deployment Models. *International Journal of Information Technology and Computer Science*, *9*(6), 50–58. https://doi.org/10.5815/ijitcs.2017.06.07

Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: Issues and challenges. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 27–33. https://doi.org/10.1109/AINA.2010.187

Dudash, S. C. (2016). *The Department of Defense and the Power of Cloud Computing: Weighing Acceptable Cost versus Acceptable Risk*. http://www.jstor.org/stable/resrep13826.1

Ďulík, M. (2016). Security in Military Cloud Computing Applications. *Science & Military Journal*, *11*(1), 26–33.

Gibson, J., Rondeau, R., Eveleigh, D., & Tan, Q. (2012). Benefits and challenges of three cloud computing service models. *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, 198–205. https://doi.org/10.1109/CASoN.2012.6412402

Gillis, A. S., Lutkevich, B., & Brunskill, V.-L. (n.d.). *digital signature*. Retrieved May 3, 2023, from https://www.techtarget.com/searchsecurity/definition/digital-signature

GitLab. (n.d.). *About GitLab*. Retrieved May 3, 2023, from https://about.gitlab.com/company/

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 5. https://doi.org/10.1186/1869-0238-4-5

Helvacioglu Kuyucu, A. D. (2011). The playground of cloud computing in Turkey. *Procedia Computer Science*, *3*, 459–463. https://doi.org/https://doi.org/10.1016/j.procs.2010.12.077

Hendry, J. (2022, June 9). *Defence begins search for cloud provider to carry secret data*. https://www.itnews.com.au/news/defence-begins-search-for-cloud-provider-to-carry-secret-data-581130

IBM. (n.d.). *What is Java Spring Boot?* Retrieved May 3, 2023, from https://www.ibm.com/topics/java-spring-boot

Jacobs, A. (2019). *Comparison of JavaScript package managers* [Bachelor's].

Jadeja, Y., & Modi, K. (2012). Cloud computing - Concepts, architecture and challenges. *2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012*, 877–880. https://doi.org/10.1109/ICCEET.2012.6203873

Jasti, A., Shah, P., Nagaraj, R., & Pendse, R. (2010). Security in multi-tenancy cloud. *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, 35–41. https://doi.org/10.1109/CCST.2010.5678682

Jedynak, D. (2013). Beyond Victory – Cloud Computing In Military Vehicles. *2013 Ndia Ground Vehicle Systems Engineering And Technology Symposium*.

Kumar Gupta, S. (2018). *Cloud Computing in Indian Aerospace and Defense Sector: Relevance and Associated Challenges*.

Kushwaha, K. S. (2021). Security Issues In Cloud Computing And Its Precautions. *Advances and Applications in Mathematical Sciences*, *20*(12), 3129–3134.

Lele, A., & Sharma, M. (2014). Relevance of Cloud Computing for Defence. In *Journal of Defence Studies* (Vol. 8, Issue 2). http://www.idsa.in/journalofdefencestudiesURLhttp://idsa.in/jds/8_2_2014_RelevanceofCloudComputingforDefence

Li, W., & Mehnen, J. (Eds.). (2013). *Cloud Manufacturing*. Springer London. https://doi.org/10.1007/978-1-4471-4935-4

Lomov, A. (2014, March 3). *A High-Level Overview of OpenShift and Cloud Foundry: Features and Architectures*. https://www.altoros.com/blog/a-high-level-overview-of-openshift-and-cloudfoundry-features-and-architectures/

Lutkevich, B., & Finnell, K. (2021). *quality of service (QoS)*. https://www.techtarget.com/searchunifiedcommunications/definition/QoS-Quality-of-Service#:~:text=Quality%20of%20service%20(QoS)%20refers,of%20data%20on%20the%20network

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks andCompliance*.

Maude, F. (2013, May 5). *Government adopts "Cloud First" policy for public sector IT*. https://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public-sector-it

Moore, L. K. (n.d.). *Nexus: An open source repository for build artifacts*. Retrieved May 4, 2023, from https://www.ibm.com/garage/method/practices/deliver/tool_nexus/

Mudawi, N. Al, Beloff, N., & White, M. (2020). Issues and Challenges: Cloud Computing e-Government in Developing Countries. *International Journal of Advanced Computer Science and Applications*, *11*(4). https://doi.org/10.14569/IJACSA.2020.0110402

NIST. (n.d.). *tampering*. Retrieved May 3, 2023, from https://csrc.nist.gov/glossary/term/tampering

Odedra, N. (2021). Cloud Computing in Defence Sector. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, *5*(2). https://doi.org/10.48175/568

Odell, L. A., Wagner, R., & Weir, T. J. (2015). *Department of Defense Use of Commercial Cloud Computing Capabilities and Services*.

Ogigau-Neamtiu, F. (2012). Cloud Computing Security Issues. *Journal of Defense Resources Management*, *3*(2), 141–148.

Onwubiko, C. (2010). *Security Issues to Cloud Computing* (pp. 271–288). https://doi.org/10.1007/978-1-84996-241-4_16

Parrilli, D. M. (2010). Legal Issues in Grid and Cloud Computing. In *Grid and Cloud Computing* (pp. 97–118). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-05193-7_7

Perkins, C. J. (2014). Cloud Computing Implementation Organizational Success in the Department of Defense. In *Theses and Dissertations*. Air Force Institute Of Technology.

Powell, D. (2013). *The Military Applications of Cloud Computing Technologies*.

Ragland, L. A., Mcreynolds, J., Southerland, M., & Mulvenon, J. (2013). *Red Cloud Rising: Cloud Computing in China*.

Rancher By Suse. (2021, May 5). *Rancher vs. OpenShift – A Consultant's View*. https://www.suse.com/c/rancher_blog/rancher-vs-openshift-a-consultants-view/

Rosencrance, L. (n.d.). *principle of least privilege (POLP)*. Retrieved May 4, 2023, from https://www.techtarget.com/searchsecurity/definition/principle-of-least-privilege-POLP

RoyChowdhury, R. (2014). Security in Cloud Computing. *International Journal of Computer Applications*, *96*, 24–30. https://doi.org/10.5120/16870-6767

Sahandi, R., Alkhalil, A., & Opara-Martins, J. (2012). *SMEs' Perception of Cloud Computing: Potential and Security*. 186–195. https://doi.org/10.1007/978-3-642-32775-9_19ï

Sajid, M., & Raza, Z. (2013). *Cloud Computing: Issues & Challenges*.

Sen, J. (2014). *Security and Privacy Issues in Cloud Computing* (pp. 1–45). https://doi.org/10.4018/978-1-4666-4514-1.ch001

Sethi, S. (2014). What Does Cloud Computing Mean for the Indian Army? *Scholar Warrior*, 86–90.

Seyrek, İ. H. (2011). Bulut bilişim: İşletmeler için fırsatlar ve zorluklar. *Gaziantep Üniversitesi Sosyal Bilimler Dergisi*, *10*(2). http://search/yayin/detay/119549

Smith, W., Kuperman, G., Chan, M., Morgan, E., Nguyen, H., Schear, N., Vu, B., Weinert, A., Weyant, M., & Whisman, D. (2017). Cloud computing in tactical environments. *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, 882–887. https://doi.org/10.1109/MILCOM.2017.8170823

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. https://doi.org/10.1016/j.jnca.2010.07.006

Sugumaran, H., & Al-Mutawha, K. A. (2017). Bahrain Cloud Transformation :Cloud First in eGovernment. *Information EGovernment Authority*.

Surbiryala, J., & Rong, C. (2019). Cloud Computing: History and Overview. *2019 IEEE Cloud Summit*, 1–7. https://doi.org/10.1109/CloudSummit47114.2019.00007

Tevaseu, S. N. (2020). *Exploring Defense Federal Acquisition Regulations Supplement (Dfars) Compliance Strategies in Cloud Computing: A Case Study*.

Tibenszky-Forika, K. (2012). Application of cloud computing in the defense industry An academic and practical viewpoint. *AARMS, Vol. 11*, 195–206.

Timmermans, J., Stahl, B. C., Ikonen, V., & Bozdag, E. (2010). The ethics of cloud computing: A conceptual review. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 614–620.

ŢIGĂNUŞ, D. (2015). Cloud Computing In Private Defence Networks. *Romanian Military Thinking*, *3*.

Toro Marin, A. (2019). *Containerizing ONAP using Kubernetes and Docker*. Universitat Politècnica de Catalunya.

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (n.d.). *Kamu Bulut Bilişim Stratejisi*. Retrieved May 3, 2023, from https://cbddo.gov.tr/bulut-bilisim-stratejisi/

United Kingdom Ministry of Defence. (2013). *Defence Information And Communications Technology Strategy*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/255880/Defence_ICT_Strategy_2013_Final.pdf

Wikipedia. (n.d.-a). *Authentication*. Retrieved May 4, 2023, from https://en.wikipedia.org/wiki/Authentication

Wikipedia. (n.d.-b). *Authorization*. Retrieved May 4, 2023, from https://en.wikipedia.org/wiki/Authorization

Wikipedia. (n.d.-c). *Bandwidth throttling*. Retrieved May 4, 2023, from https://en.wikipedia.org/wiki/Bandwidth_throttling

Wikipedia. (n.d.-d). *Cloud computing security*. Retrieved May 3, 2023, from https://en.wikipedia.org/wiki/Cloud_computing_security

Wikipedia. (n.d.-e). *Message authentication code*. Retrieved May 4, 2023, from https://en.wikipedia.org/wiki/Message_authentication_code

Wyld, D. C. (2009). *Moving to the cloud: An introduction to cloud computing in government*. IBM Center for the Business of Government.

YogaDNS. (n.d.). *YogaDNS Documentation*. Retrieved May 4, 2023, from https://www.yogadns.com/docs/

Zaerens, K. (2011). Enabling the benefits of cloud computing in a military context. *Proceedings - 2011 IEEE Asia-Pacific Services Computing Conference, APSCC 2011*, 166–173. https://doi.org/10.1109/APSCC.2011.42

Zola, A. (2021, June). *hashing*. https://www.techtarget.com/searchdatamanagement/definition/hashing

APPENDICES

APPENDIX A

QUESTIONS FOR EMPLOYEES WITH CLOUD EXPERIENCE

What are the most critical challenges in the adopting to cloud computing?
What are the main measures to be taken to keep security at the highest level in cloud computing?
How many users can work simultaneously in the cloud?
Will there be performance issues in applications running on the cloud during scaling?
Is there any cloud management software that you think works stable and efficient?
Is it possible to receive service from any service provider in line with security and privacy restrictions?
What are the precautions that can be taken against data loss and system interruptions?
How often should 3rd party software be updated in the infrastructure that is planned to be installed without being connected to any external network?

APPENDIX B

SYSTEM USABILTY SCALE SURVEY QUESTIONS

		Strongly disagree				Strongly agree
		1	2	3	4	5
1	I think that I would like to use this cloud framework frequently.					
2	I found the cloud framework unnecessarily complex.					
3	I thought the cloud framework was easy to use.					
4	I think that I would need the support of a technical person to be able to use this cloud framework.					
5	I found the various functions in this cloud framework were well integrated.					
6	I thought there was too much inconsistency in this cloud framework.					
7	I would imagine that most people would learn to use this cloud framework very quickly.					
8	I found the cloud framework very cumbersome to use.					
9	I felt very confident using the cloud framework.					
10	I needed to learn a lot of things before I could get going with this cloud framework.					

TEZ İZİN FORMU / THESIS PERMISSION FORM

ENSTİTÜ / INSTITUTE

Fen Bilimleri Enstitüsü / Graduate School of Natural and Applied Sciences ☐

Sosyal Bilimler Enstitüsü / Graduate School of Social Sciences ☐

Uygulamalı Matematik Enstitüsü / Graduate School of Applied Mathematics ☐

Enformatik Enstitüsü / Graduate School of Informatics ☐

Deniz Bilimleri Enstitüsü / Graduate School of Marine Sciences ☐

YAZARIN / AUTHOR

Soyadı / Surname : .....
Adı / Name : .....
Bölümü / Department : .....

TEZİN ADI / TITLE OF THE THESIS (**İngilizce** / English) : …….....
.....
.....
.....
.....

TEZİN TÜRÜ / DEGREE**:** **Yüksek Lisans** / Master ☐ **Doktora** / PhD ☐

1. **Tezin tamamı dünya çapında erişime açılacaktır. /** Release the entire work immediately for access worldwide. ☐
2. **Tez iki yıl süreyle erişime kapalı olacaktır.** / Secure the entire work for patent and/or proprietary purposes for a period of **two year. *** ☐
3. **Tez altı ay süreyle erişime kapalı olacaktır.** / Secure the entire work for period of **six months**. ***** ☐

***** *Enstitü Yönetim Kurulu Kararının basılı kopyası tezle birlikte kütüphaneye teslim edilecektir.*
A copy of the Decision of the Institute Administrative Committee will be delivered to the library together with the printed thesis.

Yazarın imzası / Signature ..... **Tarih** / Date .....