Designing and developing a solution for data loss cloud computing security

Submitted By

Badsha Faysal

ID: 191-35-441

Department of Software Engineering

Daffodil International University

Supervised By

Dr Imran Mahmud

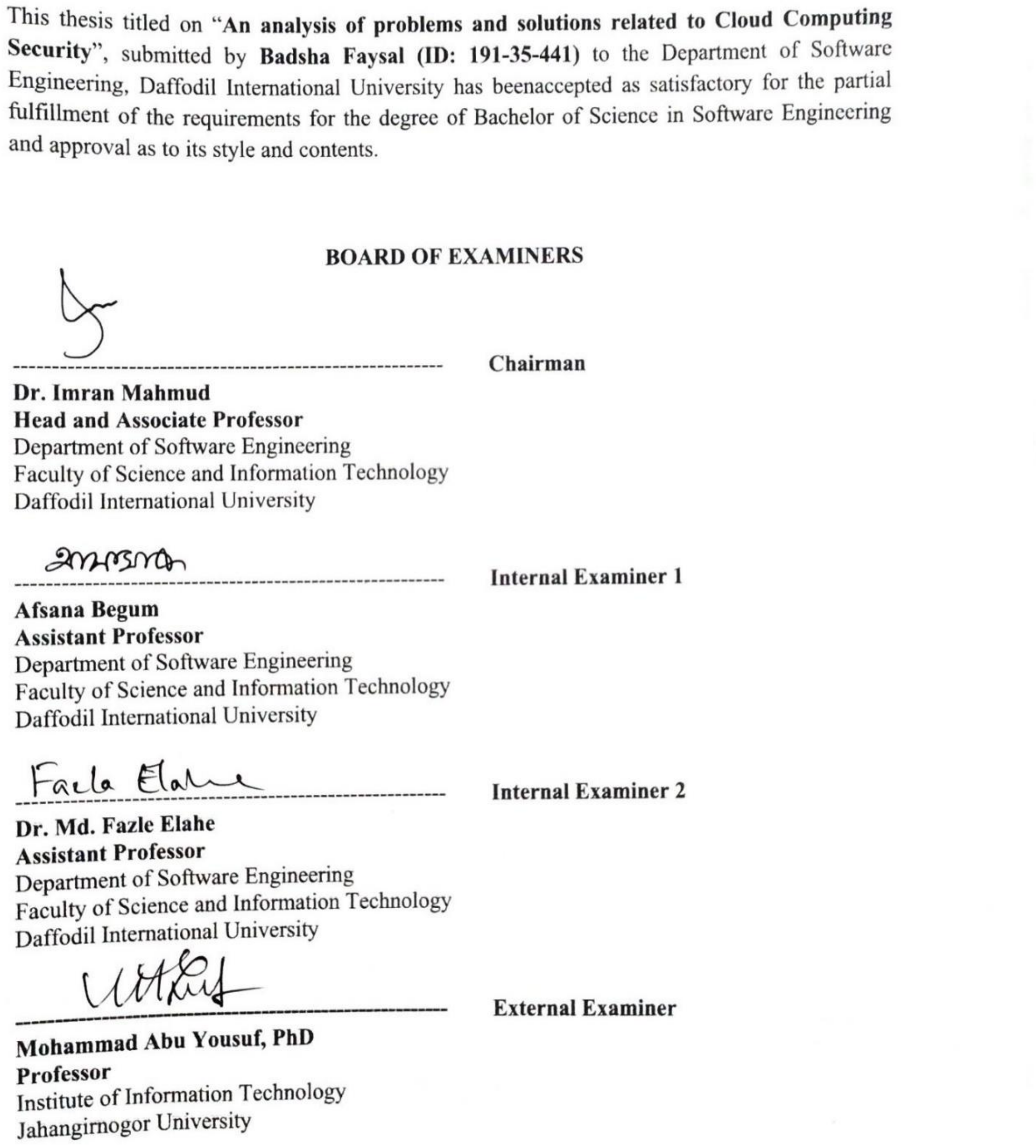
Associate Professor & Head

Department of Software Engineering

Daffodil International University

Date of Submission: 27th November

APPROVAL



This thesis titled on "**An analysis of problems and solutions related to Cloud Computing Security**", submitted by **Badsha Faysal (ID: 191-35-441)** to the Department of Software Engineering, Daffodil International University has beenaccepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. Imran Mahmud
Head and Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

Afsana Begum
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

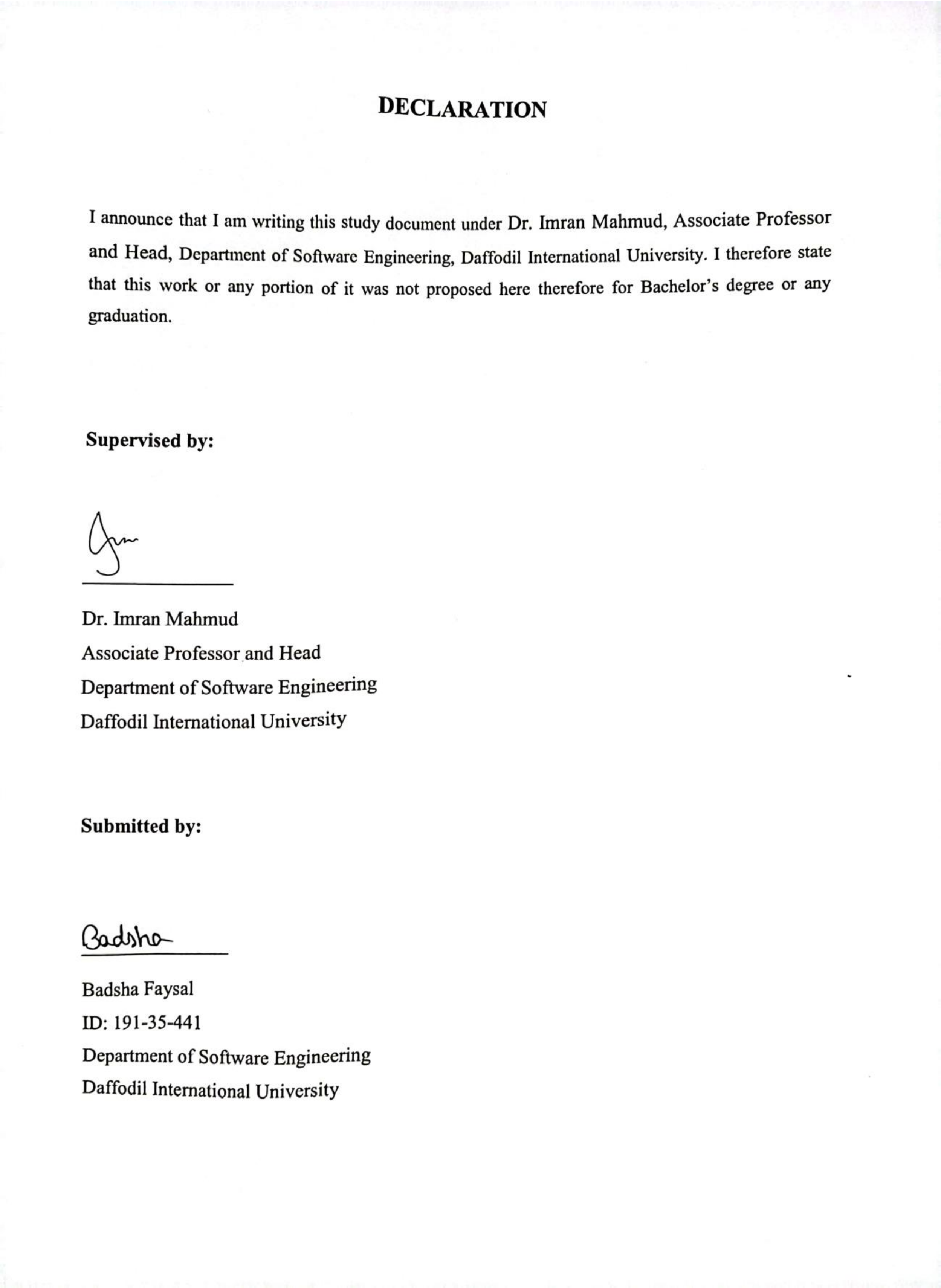
Fazla Elahe

Internal Examiner 2

Dr. Md. Fazle Elahe
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Mohammad Abu Yousuf, PhD
Professor
Institute of Information Technology
Jahangirnogor University



DECLARATION

I announce that I am writing this study document under Dr. Imran Mahmud, Associate Professor and Head, Department of Software Engineering, Daffodil International University. I therefore state that this work or any portion of it was not proposed here therefore for Bachelor's degree or any graduation.

Supervised by:

Dr. Imran Mahmud
Associate Professor and Head
Department of Software Engineering
Daffodil International University

Submitted by:

Badsha

Badsha Faysal
ID: 191-35-441
Department of Software Engineering
Daffodil International University

ACKNOWLEDGEMENT

In today's world of competition there is a race for survival in which they have to come forward for success. First of all, I would like to thank the Almighty Allah Who has clearly guided me to do the right thing in life. Without His grace this topic could not have become a reality. And my parents, whom I am extremely indebted to for bringing me to this stage with love and encouragement.

I feel compelled to talk about the opportunity to study at Daffodil International University. I would like to sincerely thank Prof. Dr. Imran Mahmud, Head of the Department of Software Engineering. Full of all the respected teachers who enjoy teaching me an interesting and understandable way. I am grateful for having them on my journey.

I am obligated to guide Daffodil International University to guide them through the constant supervision of Dr. Imran Mahmud to provide the necessary information as well as to honor the initiative and additionally their help in completing the research. Finally, I would like to express my gratitude to my batch mates, members of DIU for their kind co-operation and consolation that has helped me to accomplish this task.

ABSTRACT

The world of computing is about to undergo a transformation thanks to the next-generation networks known as cloud computing. It is very flexible, with resources and services available on demand. Security continues to be a major cloud computing paradigm concern. These difficulties include user-initiated data loss, data leakage, and privacy-related information disclosure. This study presents a thorough analysis of the available literature on the problems with and remedies for cloud computing security. The authors suggest a model for cloud computing security towards the conclusion of their paper.

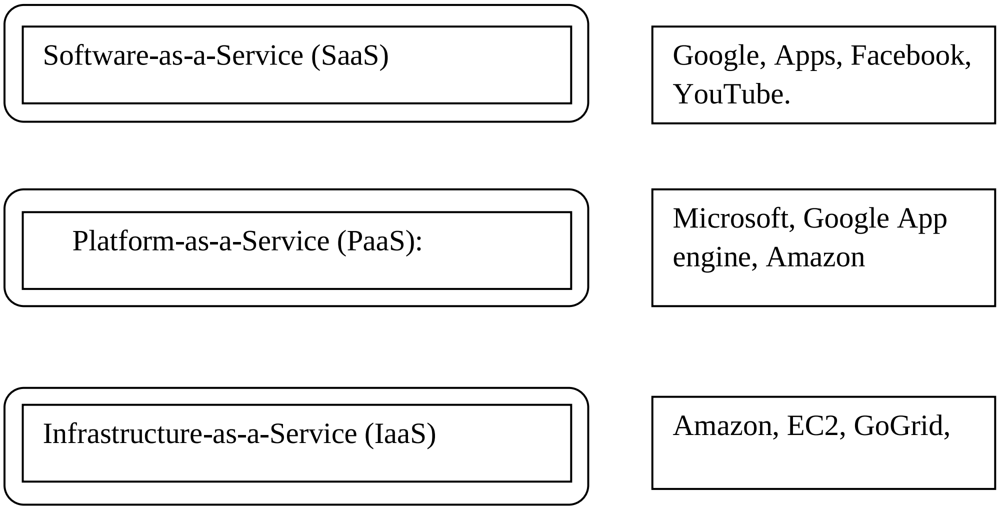
Keywords: *Cloud Computing, Cloud Security, IaaS, PaaS, SaaS*

Table of Contents

1. INTRODUCTION

Recently, a new paradigm for hosting and providing services over the Internet called "cloud computing" has arisen. The utilization of software, data, and services in the cloud, which is an internet-based environment, is possible from anywhere and on any web-enabled device (B, 2014). Researchers define cloud computing as "a kind of computing where massively scalable IT enabled capabilities are supplied "as a service" to external consumers utilizing Internet technology" (M. P. Boss G, 2007) (Heiser, 2009)(Whyman, 2008). Companies and organizations rank cloud computing as the top technology among the top 10, with a stronger future outlook in coming years (Keiko Hashizume, 2013). In (S. Subashini, 2011), experts predicted that between 2011 and 2021, 12% of the software business would migrate to the cloud, with a $95 billion increase in market size. A variety of services are offered by cloud computing, and these services present three infrastructure model layers: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) (Hassan Takabi, 2010)(Mahesh U. Shankarwar, 2014).

Customers can access the services offered by cloud service providers thanks to cloud delivery methods, as depicted in Figure 1. These are covered in greater depth below.


Software-as-a-Service (SaaS)
Google, Apps, Facebook, YouTube.
Platform-as-a-Service (PaaS):
Microsoft, Google App engine, Amazon
Infrastructure-as-a-Service (IaaS)
Amazon, EC2, GoGrid,

1.1. Software-as-s-service (Saas)

This model consumer can use application services that cloud provider offer. Thin clients (like web browsers) or APIs can be used by users to connect to the service. Consumer has no control over the app or operating system and infrastructure that run underneath it. The only thing the user can do is change the settings for user configuration. Google Apps, Face book, YouTube, Salesforce, and many more are all examples of SaaS providers.

1.2. Platform-as-a-service (PaaS)

This model user can build or run their own apps on the cloud provider's platform, which includes languages, libraries, and tools. Consumers don't have any say over the operating systems and infrastructure underneath (servers, network, etc.). The environment (platform) settings won't be easy for consumers to change. Microsoft Azure, IBM Bluemix, Google AppEngine, etc. are all examples of PaaS providers.

1.3. IaaS stands for Infrastructure as a service (IaaS)

This model the consumers can set up processing, storage, network, and other resources that can be used to build or run an application. The user cannot control underlying infrastructure of the cloud, but they can control the operating system, storage, firewall, and application that are running. Amazon EC2, GoGrid, Flexiscale, etc. are all examples of IaaS providers. Aside from the features and service that cloud computing offers, there are a number of things that make it hard to use (Bulusu, 2012) (Rao, A Study on Data Storage Security Issues in Cloud computiong, 2016.). Based on the survey that Right Scale, a top SaaS provider, didshown in Figure (Suryateja, Threats and Vulnerabilities of Cloud Computing: A Review, 2018).

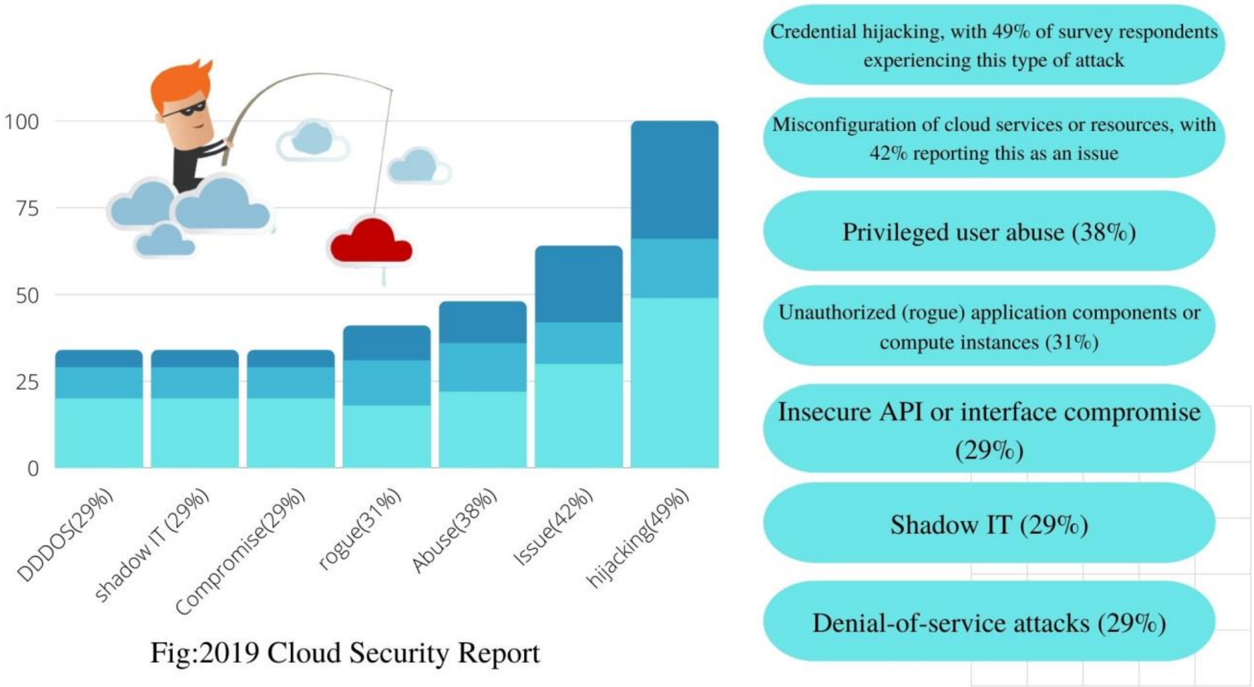


Fig:2019 Cloud Security Report

What kind of problem can happen in Bangladesh is shown below with gives some point that will clear for all.

1.4. Problem in Bangladesh

1.4.1. Increased security vulnerabilities

When company data is transferred to the cloud, the cloud provider now shares responsibility for data protection. The consumer of the cloud must expand their trust boundaries to include the external cloud in order to use information technology resources remotely. Setting up a security architecture that can measure such a trust boundary without creating vulnerabilities might be exceedingly challenging (Puttini, 2013).

1.4.2. Reduced operational governance control

Customers who use the cloud typically receive a lesser level of governance control than those who use on-premise IT resources. This could increase vulnerabilities related to the cloud management practices of the cloud provider as well as the reliance on external connections for cloud-to-cloud communication (Thomas Erl, 2013).

1.4.3. Limited portability between cloud providers

Public clouds are frequently owned to different degrees since the cloud computing industry lacks clear industry standards. It can be difficult for cloud users to switch between cloud providers if their unique solutions depend on these ownership environments [32]. Cloud "Barriers to Adoption" cited by Carnegie Mellon's Software Engineering Institute Mellon College. Utilizing a cloud service will be advantageous and helpful if these issues can be resolved with the service provider (Cloud Computing: Barriers to Adoption, 2017).

1.5. Problem in World

What kind of problem can happen in world is shown below with gives some point that will clear for all. Flex era recently did its annual State of the Cloud Survey to find out what's going on in the cloud. They asked 997 technical workers from a wide range of organizations about how they were using cloud infrastructure. Their results were helpful, especially when it came to problems that are happening now with cloud computing. To answer the main questions of what the problems are with cloud based computing, we have expanded on some of their finding and listed other problem that business may need to deal with. First, let's talk about cyber security, which is always important. Flexera's annual state of the cloud survey puts a lot of attention on cloud problems.

1.6. Security Issue

In our complete guide to business intelligence trends, we talked about the heated debate about how to protect data. In the world of cloud-based computing, security is a big issue, just like in many other fields of technology, because you can't see where your data is being stored or processed. This makes it more likely that something bad will happen during the process of implementation or management.

At the moment, 93(%) of top company across all industries very worried about a major data breaches in their cloud-based ecosystems.

The main things people worry about when it comes to cyber threats in general are:

- Compromised credentials
- Broken authorization
- Human mistake
- massive data breaches involving sensitive information
- Hacked interface and APIs
- Account hijacking

All of this make it hard for some people to give sensitive and private data to a third party, and it also shows how hard cloud computing can be. As both providers and users, it's good to know that mature fortification capabilities are always getting better. Make sure the SaaS provider has secure user identity management, authentication, and access control in place to protect your organization's privacy and security. Also, check which privacy and security laws apply to their databases.

When you check a provider protection and privacy laws, you should also make sure that third most important things, compliance, is taken care of. No matter where yours data is stored, your business needs to be able follow rules and regulation. When talking about storage, you should also make sure that the provider has strict policies in place for data recovery.

By keeping your finger on the pulse of new trend and knowing how each part of your ecosystem handles cyber security, you will reduce the risk of breaches or attack by a large amount.

Every business, no matter how big or small, now has to deal with the risks of cloud computing. Because of this, it's important to use a secure BI cloud tool that can use the right security measures.

1.7. Cost control and management

The cost of cloud computing is the next risk on our list. Most of the time, computers can help businesses save money. In the cloud, a company can quickly increase its processing power without having to buy a lot of new hardware. Public providers, on the other hand, offer pay-as-you-go models for extra processing that businesses can use. But because cloud computing services can be used on demand and can be scaled up or down, it can be hard to define and predict quantities and costs. There is several ways to keeps cloud cost in check, such as cost optimization through improved financial analytics and reporting, automation of decision-making procedures, or keeping the management reporting practice on track, so that these problems in computing can be lessened. Multi-cloud computing tools are another recent innovation that helps cut costs and solve one of the most important problems in cloud computing. At the moment, 32 % of business use multi-cloud cyber security tool to reduce the risk of financially devastating data breaches. The return on investment (ROI) is good in both cases. Because of this, we think that the number of people who use it will grow in the near future.

1.8. Lack of expertise

One problem that companies and enterprises are having with the cloud right now is that they don't have enough resources and/or know-how. As cloud technologies continue to improve quickly, organizations are putting more and more work into the system. Because of these things, it's hard for organizations to keep up with the tools. Also, the demand for experts keeps growing. These problems can be made less of a problem by giving IT and development staff more training. A strong CIO who supports moving to the cloud also helps. As Drew Firment, a Cloud Engineer says: "The success of adoptions and migrations depends on your people and how much you invest in a talent transformation program. Until you fix the number one thing stopping people from using the cloud, any other changes you make will not help. Small and medium-sized businesses (SME) may find that adding specialists to their IT teams is too expensive. Many of the common tasks that these specialists do can, luckily, are done by machines. For this reason, companies are using DevOps tools like Chef and Puppet to do things like track how resources are used and set up automatic backups at set times. These tools also help you get the most out of the cloud in terms of cost, management, and security.

1.9. Governance/ control

Cloud computing faces many problems, and control is the fourth one. IT assets should be implemented and used in accordance with established policies and procedures thanks to good IT governance. Additionally, it should guarantee that these resources are appropriately managed, maintained, and supported by your organization's strategy and objectives. In the cloud-based world of today, IT does not always have full control over how infrastructure is set up, taken down, and run. This has made it harder for IT to provide the required governance, compliance, risk, and data quality management. IT must change its traditional IT control processes to include the cloud in order to reduce the risks and unknowns that come with moving to the cloud. In this way, the role of the system's central IT teams has changed over the last few years. Along with business units, central IT is taking on a bigger role in choosing cloud services, acting as a broker, and making rules about them. On top of this, third-party providers of cloud computing and management are gradually giving support and best practices.

1.10. Research Question

In this thesis, we have one core research questions which are given below:

RQ: Does your proposed model give more security than other?

1.11. Research Objective

RO: In this thesis, we have three core research questions which are given below: A comprehensive analysis of the existing literature on cloud computing security challenges and solutions examines the combination of three levels of user identification through proper authentication, data identification encryption, and cryptography techniques.

1.12. Organization of the chapter

To discuss more about the thesis, the rest of the chapters are organized like chapter 1 are provides an introduction to cloud computing and the need for giving importance to the security in cloud computing. After chapter 2, Give overview of threats & vulnerabilities of cloud computing. In chapter 3, literature review which reflected previous works on cyber security and the discussion also mentioned in research gap. In chapter 4 give propose model.And the Result section, we displayed the result that will show a plain text to cipher text; in the first security phase there is user identification through proper authentication that Data identification and Encryption then the cryptography technique then show the result. Finally, chapter 5 is Conclusion.

2. THREATS AND VULNERABILITIES

A threat is something that could cause something bad to happen that could hurt a system or an organization. A weakness in an asset or system that can be used by a threat is called vulnerability. A threat agent makes threats by taking advantage of one or more flaws. Through a thorough review of the literature, different cloud computing threats and weaknesses are found. They are talked about in more depth below:

Data Loss (i): This is when data gets messed up or isn't available because of things like earthquakes, floods simple human mistakes like when a cloud administrator delete files by accident, a hard drive fails, the power goes out, or a malware infection. The best way to keep from losing data is to back it up in more than one place. This way, if data get corrupted or lost in one place, it can be replaced with copy from another place.

Data Breaches (ii): A data breach is a security incident that happens when sensitive, private, or confidential information about a person or organization is accessed, copied, or sent by someone who shouldn't have been able to. Data breach is the most dangerous threat in cloud computing (Jr., 2018)(Rao, 2016). It is ranked as the number one threat. Only in 2017, data breaches led to the loss of more than 1.4 billion records, many of which were stored on cloud servers. At least 143 million people were hurt by the Equifax breach. In May 2017, hackers broke into One Login, a cloud service that manages identities and lets users sign in once to all of them. Targeted attacks, simple human error, bugs in applications, or bad security practices can all lead to data breaches.

Malicious Insiders (iii): A malicious insider could be the most dangerous threat with the most damage. A former employee, a system administrator, a third-party contractor, or a business partner is all examples of different types of insider threats. A threat from the inside can be very bad. As an example a recent insider breach at Sage caused the stock price to drop by 4.3%, which cost the company millions of dollars. When it comes to security, systems that rely only on cloud services provider are at a higher risk. A malicious insider, like a system administrator, can get to potentially private informations and can gain access to more and more important systems, which could lead to a data breach.

Denial of Service DDOS (iv): DoS (Denial of Service) attack makes a system unavailable. Denial of Service (DoS) attack, there is only one machine from which attack comes, and its can be stopped. DoS attacks are meant to make it so that legitimate user of a service can't get to their data or apps.

Account Hijacking (v): Cloud services make account or service hijacking even more dangerous. Account hijacking is when the login information of a legitimate user is stolen and used for bad things. If attackers get their hands on someone else's credentials, they could break the cloud services' security, reliability, or availability. Phishing and fraud are two ways that attackers can get hold of account credentials. Enterprises should make it harder for users and cloud services to share account credentials and use multifactor authentication whenever possible. Due diligence is process of checking out CSP to make sure that best practices are being used. Part of this process is making sure that the cloud provider can offer the security controls that are needed and provide the level of service that the customer wants. Enterprises should look at the ISO 9001, DCS, PCI, and HIPAA certifications and standards that CSPs have earned. Application security is greatly affected by not doing what needs to be done, which leads to a breach shown in Figure 2.

Not Taking Care of Things (vi): People who use cloud services often think that the CSP is the only one responsible for security. As a result, they don't always protect their cloud-based apps. Cloud providers don't have to protect their customers' workloads or data beyond what's outlined in the Service Level Agreement (SLA) (Suryateja, Threats and Vulnerabilities of Cloud Computing: A Review, 2018).

Insufficient Security Tool (vii): Public provider has a variety of tool and service to improve cloud security, check the state of cloud resource, and stop attack. Some attacks, like a DDoS, can make it almost impossible for cloud users to handle them.

Human Error (viii): Even though we live in the age of computers, people are still one of the weakest link in IT security. The cloud chance of a person making a mistake is higher because stolen credentials can mess up applications and data. Hackers can steal credentials and take over cloud accounts through phishing, fraud, and other forms of social engineering. Administrators should teach users about security and give them security certifications. They should also write clear acceptable use policies and follow other best practices for security.

Ransom ware (ix): Ransomware is a type of malware that locks files or other resources on the system of the victim, usually by encrypting them. For the attacker to decrypt the files, he or she wants a ransom. Even if the ransom is paid, there is no guarantee that the attacker will send the key to decrypt the files. In 2017, WannaCry ransom ware made it impossible for businesses and government agencies around the world to access their data. The FBI says that there were 4000 ransomware attacks every day in 2016, which is a 300% increase from the year before. Ransomware can come from many places, like an email, a video, a PDF file, a link to a website, a device that is connected to your computer, or even a stolen password. Ransomware locks up everything connected to a computer. Backups should always be kept in different cloud locations to be safe.

3. LITERATURE REVIEW

The cloud has changed the world we live in. People are now moving their data to the cloud because data is getting bigger and needs to be accessible from many devices. So, it's become normal to store data in the cloud. But there are many problems with data that is stored in the cloud. These problems start with a virtual machine, which is how resources in the cloud are shared, and end with problems with cloud storage itself. In this paper, we talk about the problems that are stopping people from using the cloud. We also do a survey and show a diagram of what has been done to solve these problems and make them less dangerous. (Suryateja, Threats and Vulnerabilities of Cloud Computing: A Review, 2018) This paper says what kind of problem occurs in cloud computing, how the data is lost, what is the reason for the loss. But there is nothing written about how to remove data loss, my paper mentions how data loss occurs, what can be done to reduce data loss, how to give more security to data. (hussain, 2022)This paper talks about byzantine failure of cloud computing, how byzantine failure causes data loss, how it happens and why it happens but no solution is given but my paper mentions how data loss occurs, what can be done to reduce data loss, how to give more security to data. Some papers discuss the problems of cloud computing. Some papers have discussed the problems of cloud computing, and how data is lost. I haven't found any solution anywhere, some papers have shown surveys, and I have proposed a diagram in my paper on how to prevent data loss. We have shown in our diagram 3 layers of data protection. In the first layer, proper authentication techniques can be used to check the user's identity. Data identification and encryption are the keys to security in the second layer. At the last layer, encryption is used to make sure the data is sent safely.

4. PROPOSED MODEL

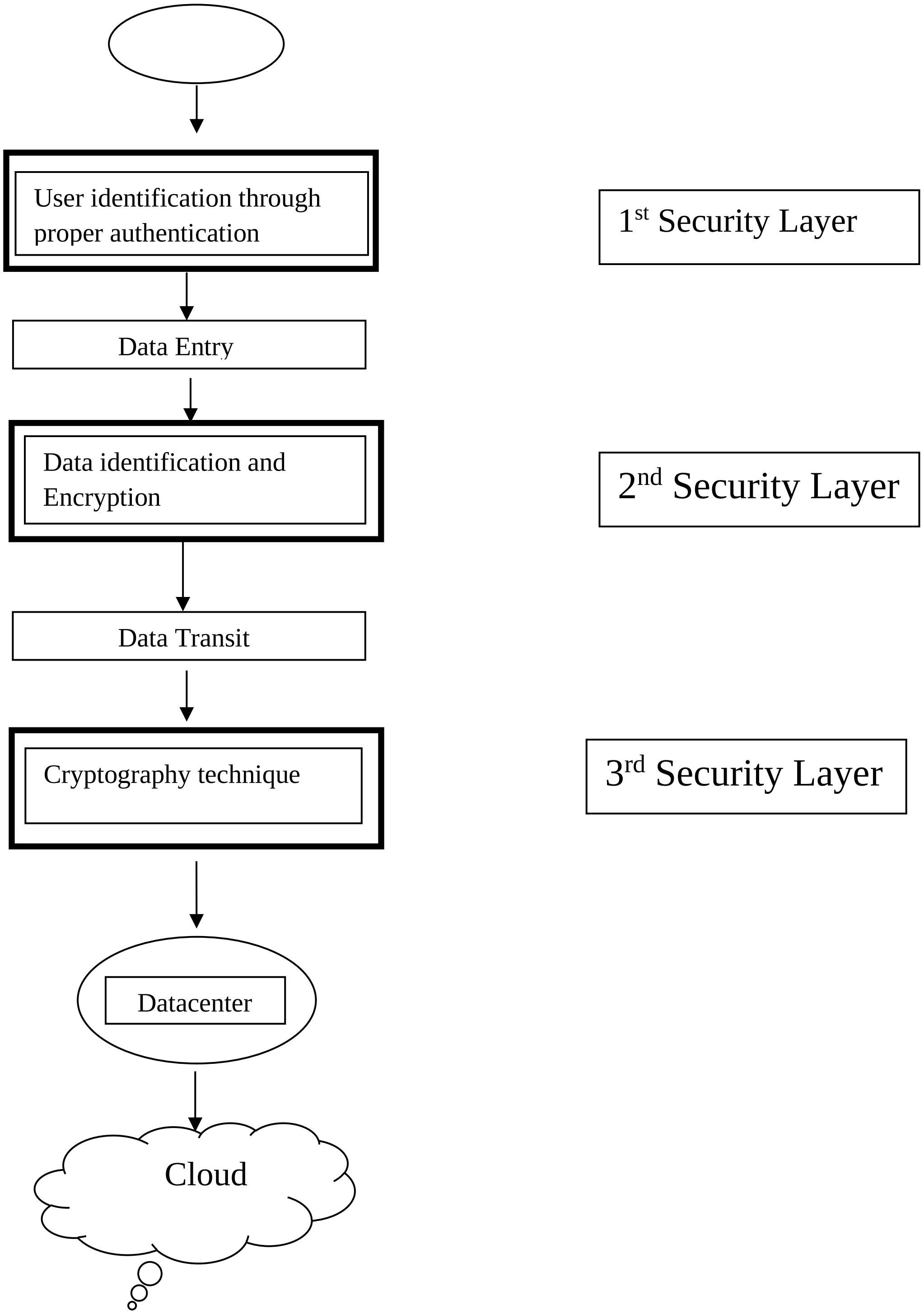


Fig - 1

Three layers make up the proposed security model for the cloud. In the first layer, proper authentication techniques can be used to check the user's identity. Data identification and encryption are the keys to security in the second layer. At the last layer, encryption is used to make sure the data is sent safely. Figure 1 show how the proposed model would be put together.

5. RESULT & DISCUSSION

First of all Given below I am given my Code:

```
// Here GIve below C++ code to implement Hill cipher .
#include<iostream>

Using namespacestd;

/* function generates the
key matrix for the key*/
void getKeyMatrix(stringkey, intokkeyMatrix[][3])
{
    intkop = 0;
    for (intl = 0; l<3; l++)
    {
        for (intp = 0; p<3; p++)
        {
            okkeyMatrix[l][p] = (key[kop]) % 65;
            kop++;
        }
    }
}

/* Here we can see function encrypts the message*/

voidOutencrypt(intshowcipherMatrix[][1],
            inttokeyMatrix[][3],
            intgivemessageVector[][1])
{
    inty, i, j;
    for (i = 0; i<3; i++)
    {
        for (j = 0; j<1; j++)
        {
            showcipherMatrix[i][j] = 0;

            for (y = 0; y<3; y++)
            {
                showcipherMatrix[i][j] +=
                    tokeyMatrix[i][y] * givemessageVector[y][j];
            }

            showcipherMatrix[i][j] = showcipherMatrix[i][j] % 26;
        }
    }
}

/* Here we can see  function to implement HillCipher*/

voidCheckHillCipher(stringCheckMessage, stringCheckkey)
{
    // Here Get key matrix from the key string

    intGivekeyMatrix[3][3];

    getKeyMatrix(Checkkey, GivekeyMatrix);

    intGiveMessageVector[3][1];

    //Here generate vector for the message

    for (intj = 0; j<3; j++)
        GiveMessageVector[j][0] = (CheckMessage[j]) % 65;

    intShowcipherMatrix[3][1];

    //function generates the encrypted vector

    Outencrypt(ShowcipherMatrix, GivekeyMatrix, GiveMessageVector);

    string takeCipherText;

    // Generate the encrypted text from
    // the encrypted vector
    for (intj = 0; j<3; j++)
        takeCipherText += ShowcipherMatrix[j][0] + 65;

    // Finally print the ciphertext
    cout <<" takeCipherText:"<<takeCipherText;
}

// Start from the main function for above code
intmain()
{
    // Here get the message to be encrypted
    string Givemessage = "ACT";

    // Here get the key
    string GiveKey = "GYBNQKURP";

    CheckHillCipher(Givemessage, GiveKey);

}

```

Given below description showing:

Above is my code, I wrote the code to pass data from my fig-1 diagram. My program will start working from the main function then we need to provide encrypted data and gives a key.

Then I am creating a function name HillCipher to implement Hill Cipher. In this function I, get the key matrix from the key string and then run a loop to generate a vector for the message, now I have created another function with the name of the function is encrypt that will help to generate the encrypted vector. I have another function is getKeyMatrix that will help me generates the key matrix for the key string.

Get the message and key to be encrypted.

Input: cloudcomputing

Key: GYBNQKURP

The output is

Output: IEV

So here we can see when we give the plain text “cloudcomputing” then our program will gives a result cipher text is “IEV”.

6. CONCLUSION

Regarding the security and privacy of users' sensitive data in the cloud environment, this article provides an overview of several dangers and solutions in the cloud computing environment. The study focuses on the security issues and solutions for the various layers of cloud computing. Authors have put out a security model for cloud computing.

7. REFERENCES

B, D. K. (2014). fuzzy keyword search over encrypted data in multicloud . *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 67.

Bulusu, S. (2012). A Study on Cloud Computing Security Challenges.

Cloud Computing: Barriers to Adoption. (2017).

Hassan Takabi, J. B. (2010). Cloud Computing Security and Privacy Challenges in Cloud Computing Environments. *IEEE*.

Heiser, J. (2009). What you need to know about cloud computing security and compliance.

hussain, S. (2022). Byzantine Failure against Colluding Attacks in Cloud Data.

Jr., J. P. (2018).

Keiko Hashizume, D. G.-M. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*.

M. P. Boss G, Q. D. (2007). Cloud computing, White Paper. *IBM* .

Mahesh U. Shankarwar, A. V. (2014). Security and Privacy in Cloud Computing.

Puttini, T. E. (2013). CloudComputing Concepts Technology & Architecture - The Prentice Hall Service Technology Series. 45.

Rao, B. T. (2016). *A Study on Data Storage Security Issues in Cloud Computing*, 128–135.

Rao, B. T. (2016.). A Study on Data Storage Security Issues in Cloud computiong. 128–135.

S. Subashini, V. K. (2011). A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications. 1-11.

Suryateja, P. (2018). Threats and Vulnerabilities of Cloud Computing: A Review. *International Journal of Computer Sciences and Engineering*.

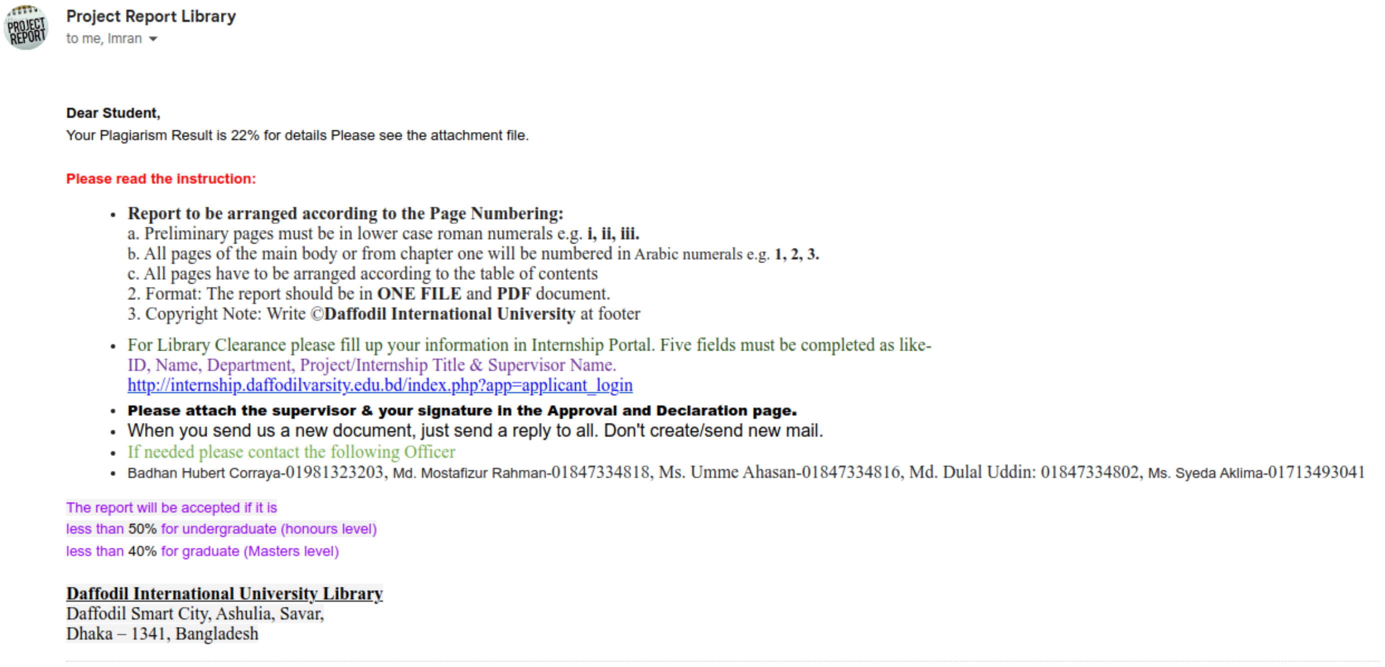
Suryateja, P. (2018). Threats and Vulnerabilities of Cloud Computing: A Review. *International Journal of Computer Sciences and Engineering*.

Suryateja, P. (2018). Threats and Vulnerabilities of Cloud Computing: A Review.

Thomas Erl, Z. M. (2013). Cloud Computing Concepts Technology & Architecture - The Prentice Hall Service Technology Series. 45.

Whyman, B. (2008). Cloud Computing, information Security and Privacy Advisory Board. 11-13.

PLAGIARISM REPORT



Project Report Library
to me, Imran

Dear Student,
Your Plagiarism Result is 22% for details Please see the attachment file.

Please read the instruction:

- **Report to be arranged according to the Page Numbering:**
  a. Preliminary pages must be in lower case roman numerals e.g. **i, ii, iii.**
  b. All pages of the main body or from chapter one will be numbered in Arabic numerals e.g. **1, 2, 3.**
  c. All pages have to be arranged according to the table of contents
  2. Format: The report should be in **ONE FILE** and **PDF** document.
  3. Copyright Note: Write ©**Daffodil International University** at footer
- For Library Clearance please fill up your information in Internship Portal. Five fields must be completed as like-
  ID, Name, Department, Project/Internship Title & Supervisor Name.
  http://internship.daffodilvarsity.edu.bd/index.php?app=applicant_login
- **Please attach the supervisor & your signature in the Approval and Declaration page.**
- When you send us a new document, just send a reply to all. Don't create/send new mail.
- If needed please contact the following Officer
- Badhan Hubert Corraya-01981323203, Md. Mostafizur Rahman-01847334818, Ms. Umme Ahasan-01847334816, Md. Dulal Uddin: 01847334802, Ms. Syeda Aklima-01713493041

The report will be accepted if it is
less than 50% for undergraduate (honours level)
less than 40% for graduate (Masters level)

Daffodil International University Library
Daffodil Smart City, Ashulia, Savar,
Dhaka – 1341, Bangladesh