INTERLAYERED SECURITY MODEL FOR CLOUD COMPUTING IN INTERNET OF THINGS (IoT) DOMAIN

Sarjiyus, O., El-yakub, M.B and Aleng E. A.

Department of Computer Science, Adamawa State University, Mubi, Nigeria
sarjiyus@gmail.com

Abstract: The way people see the world includes more than just the physical things around them. There is also a strong presence in cyberspace. However, this virtual part is not separate from the physical world. Many connected sensors collect data from the physical world and send it to cyberspace. This research focuses on creating a new, layered security model to deal with specific challenges like keeping data safe, ensuring privacy, and making sure systems work properly when cloud computing and IoT are used together. The research mainly used data from journal articles written by experts in the field. Tools like class diagrams and pseudocode were used to show how the system works. In this study, AES was used to encrypt data, and the AES key was further protected using RSA public key encryption to handle key management better and improve data security. When AES was combined with the ESA algorithm, it made the encryption more secure, though it took more time.
[Sarjiyus, O., El-yakub, M.B and Aleng E. A. **INTERLAYERED SECURITY MODEL FOR CLOUD COMPUTING IN INTERNET OF THINGS (IoT) DOMAIN.** *J Am Sci* 2025;21(8):30-41]. ISSN 1545-1003 (print); ISSN 2375-7264 (online). http://www.jofamericanscience.org. 02 doi:10.7537/marsjas210825.02

Keywords: AES encryption; ESA algorithm; Cloud Computing; Internet of Things (IoT); Multilayered Security

Introduction

The way people experience the world includes not only the physical things around them but also a significant part in cyberspace.

However, this virtual world is not separate from the physical. A large number of connected sensors bring data from the physical world to cyberspace. These data influence people connected to cyberspace, as well as the processes in the physical world, especially in control systems. Similarly, data created only in cyberspace can affect the physical world, either by influencing people's thoughts or through control systems connected to cyberspace. The connection between the physical and virtual world raises many important questions. What if the data is incorrect or even harmful? What if the processes are wrongly programmed or set to produce harmful results? Can people with bad intentions control our cyber systems and, through them, change the physical world in unexpected or forbidden ways? We know the answer is yes, and the risk of physical harm through the virtual world is real. Therefore, it is very important to focus on the security of cyber reality, especially in areas where it strongly interacts with the physical world. The main reason for the interaction between the physical and virtual world is the rise and spread of the Internet of Things. Like the traditional Internet, the Internet of Things is very complex. In the security field, a key principle is to keep things as simple as possible (Ishaya, 2021). Complex things are harder to secure, as attackers only need to find one weak point to exploit. On the other hand, defenders must protect every part of the system and every interaction between the system, its parts, and the outside world.

The study of a multi-layered security approach for cloud computing in IoT addresses the growing need for strong security in cloud-based IoT systems.

The merging of cloud computing and IoT has created powerful and scalable systems, but it has also introduced new challenges and vulnerabilities that need to be addressed to ensure data and device security (Zhang *et al*., 2018).

The Internet of Things involves connecting a large number of devices to the Internet, allowing them to collect and share information.

Cloud computing provides a flexible and scalable platform for processing and storing the huge amounts of data generated by IoT devices (Bonnet, 2021).

Cloud computing is a way of managing information, resources, and applications as services over the Internet, based on the needs of users.

Instead of buying servers, storage, or networking equipment, users can access these resources through cloud service providers. It is defined as a model that offers convenient and on-demand network access to a shared pool of computing resources, provided by service providers in the form of multiple services (Morabito, 2020). It creates a new Internet-based environment where computing resources can be accessed on demand, with dynamic allocation using different types of services on the cloud. These models are known as Software as a Service, Platform as a

Service, and Infrastructure as a Service. Because of this, it is difficult to manage security and privacy issues in the cloud due to sensitive data, outsourcing of infrastructure, multi-tenancy, and critical applications. This paper focuses on a framework that identifies and summarizes the security and privacy challenges in cloud services. It highlights specific cloud attacks and risks, and clearly explains their mitigation and countermeasures (Grance, 2018). It also presents a multi-level security framework for cloud computing that helps meet security and privacy needs in the cloud and protect against attacks. The purpose of this work is to demonstrate and introduce a security and privacy approach that considers various security issues when developing and using a cloud environment, whether by individuals or organizations (Al-Fuqaha *et al.*, 2022).

An interlayered security framework is therefore important to handle the varied and complex security challenges in cloud-based IoT systems.

This framework typically involves integrating security measures at different levels, including the device, network, application, and cloud layers (Roman *et al.*, 2021).

The interlayered security framework may include elements like encryption, authentication, access control, intrusion detection and prevention systems, secure communication protocols, and regular security audits.

Each layer plays an important role in protecting the entire system. The technology landscape is ever-changing, with new technologies and threats constantly emerging. The security framework should be flexible enough to incorporate new security measures and countermeasures as they become necessary (Botta, 2019).

Aim and Objectives

The main goal of this research is to create a strong security system that works well with both Cloud Computing and Internet of Things (IoT). This system is meant to solve specific problems like making sure data stays safe, private, and available when these technologies are used together.

The specific goals are as follows:

i. To look into and understand the security problems that are common in IoT devices.
ii. To build a system that stops unwanted people from accessing data and makes the security of data shared between IoT and the cloud better.
iii. To improve the RSA encryption method and privacy tools so that data from IoT devices is better protected as it goes into the cloud.

Literature Review

The literature review looks at how Cloud Computing and Internet of Things (IoT) work together, seeing them as fast-growing technologies in the computer world.

It covers the benefits and chances these technologies offer to different kinds of organizations. It also looks at the problems and challenges that are making people interested in using these technologies more. To do this study, a conceptual framework was used, which involved gathering and reviewing both numbers-based and text-based information. The results from these reviews provided a general picture (Raj, 2021).

The current studies show where Cloud Computing is heading and the issues it faces with both Cloud Computing and IoT.

The theory suggests that researchers are hopeful about the growth of this area and are ready to come up with many ways to solve the problems in Cloud Computing and IoT. The summary of these studies gives insights into the promising future of Cloud Computing and IoT, focusing on both their potential and the challenges that need to be overcome for them to work well together (Raj, 2021).

In Cloud Computing, almost everything is provided as a service, from access to security.

The cloud has become a big topic with many terms. There are three main types of services that are very important today: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These are ways to deliver software over the Internet. The idea became real around early 2020, when it was first called Application as a Service (Joel, 2019).

In the SaaS model, the user pays for a subscription to a software product. The data and program are on a remote server, and the user can access them through the Internet. This gives user's access to software services without them having to manage the software themselves (Emmanuel, 2022).

Platform as a Service (PaaS) lets users build, test, and deploy applications on the service provider's platform. It gives flexibility by allowing users to use different programming languages or tools supported by the provider. Customers can set up their own software and apps in the cloud, which helps them save money and reduce the complexity of managing hardware and software (Shrikant, 2020).

Infrastructure as a Service (IaaS) is different because it offers hardware support to users.

While SaaS and PaaS provide ready-made applications, IaaS gives users the ability to put anything they want on the hardware (Joseph, 2020).

According to Bonnet (2021), Cloud and IoT have been developing separately. However, their combination has led to many shared benefits. The literature shows that this integration is expected to shape the future. On one hand, IoT can use the cloud to get unlimited resources and capabilities to overcome technical limitations. Cloud computing helps in managing IoT services, data, and apps. On the other hand, the cloud can benefit from IoT by expanding its reach to handle real-world objects in a distributed and flexible way, and providing services in various real-life situations. The combination of cloud and IoT is interesting because of the many ideas mentioned in the literature. The cloud works as a middle layer that hides the complexity of connecting things to applications.

IoT naturally involves a lot of data sources. It generates a large amount of data that is either unstructured or semi-structured. This data has three main features: Volume, Velocity, and Variety. This means that there is a need to collect, manage, process, and share large amounts of data. The cloud provides a convenient and affordable way to store data, with on-demand access and almost unlimited capacity.

This integration creates a new scenario where opportunities for data collection, sharing, and use with other parties arise.

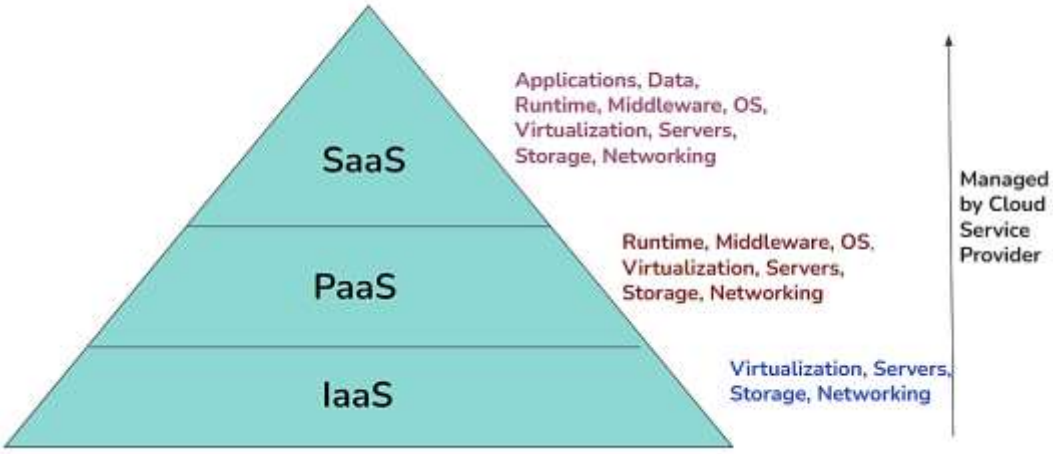
Once data is in the cloud, it can be accessed through a standard API, protected with strong security, used from anywhere, and visualized. The processing power of IoT devices is limited, so data is usually sent to a more powerful node for processing. However, this might not be scalable. The cloud, with its on-demand model and unlimited capacity, allows IoT to handle complex data analysis.

With the cloud, data-driven decisions and prediction systems can be made at a low cost, leading to higher profits and fewer risks.

One of the main needs for the Internet of Things is to allow devices to connect and talk to each other through special hardware. But making this communication work can be quite costly. Cloud connection offers a good and affordable way to do this. With cloud technology, you can track and manage anything at any time, from anywhere, using a custom website and built-in tools. Using the cloud helps solve many of these challenges and adds benefits like easier access, simpler use, and lower setup costs (Bollag, 2021).

Infrastructure-as-a-Service (IaaS) is the base part of cloud computing.

IaaS gives you virtual resources like servers, networks, storage, and machines. With this service, users can build their own virtual groups. Cloud providers not only supply the hardware but also take care of maintaining and updating it as new versions come out. These resources can be easily increased or decreased as needed, which helps in cutting down costs. The main benefit of IaaS is that companies don't have to buy and maintain their own hardware and software. This is especially helpful for small businesses with limited budgets that can't afford expensive equipment and software (Ferreira, 2018).



(Balogh, 2018)

Private cloud is a type of cloud that is only available within a single organization.

It is controlled and managed by the company itself. This model helps organizations use low-cost hardware for better performance and improves how well servers are used. It also lowers administrative and operation costs. Still, there are some downsides, especially the high initial cost to set up and manage the cloud. Eucalyptus Systems is a good example of a private cloud setup.

Community Cloud model lets groups or organizations share services and systems. Facebook is an example of this type of cloud. This model is managed by a shared organization or a third party. Data and resources are shared among the organizations, making the model more cost-effective. However, since all data is stored in one place, it can be accessed by non-members, so users must be careful about what they store (David, 2017).

Cloud computing is a powerful, virtual, secure, and affordable IT solution. It offers on-demand computing infrastructure that is flexible and cost-effective. Cloud computing provides three main service types: IaaS, PaaS, and SaaS. It uses four main deployment models: Public, Private, Hybrid, and Community Cloud. Cloud computing allows users to use rented services like web apps instead of buying them. This means users can access services anytime and anywhere. The main idea of cloud computing is resource virtualization. Benefits include less need for hardware and software licenses, lower maintenance, easy access, flexibility, and more. However, cloud computing comes with some challenges such as security and dependence on internet quality.

These issues need to be addressed in the future. Experts predict that by 2020, most people will use online applications and share information using remote servers instead of their own devices. They believe that in the next decade, cloud computing will become more popular than desktop computing. Some recent examples showing the growing use of cloud services include 400 million active Facebook users, Hotmail and Yahoo users, Twitter users, YouTube for videos, Flickr for photos, Google Docs for documents, Delicious for bookmarks, eBay for business, and Yelp and Trip Advisor for reviews and ratings. These numbers are expected to grow even more, making it hard to tell the difference between working with local devices and cloud services in the future. Future internet technologies will have a big impact on research and be key to the future of cloud computing.

As internet speeds increase and cloud security gets better, more companies will use cloud services.

Cloud computing is not only used by social media companies. It is also growing in engineering fields, especially in IoT applications at home and in businesses. The cost of devices like microcontrollers, memory, and sensors is falling, while processors are getting faster and more reliable. This means cloud computing will have a big role in engineering applications in the coming years as more companies invest in this technology (Alajjer, M. 2021).

Cloud service models can be set up in one of four different ways;

1. A private cloud is used only by one organization, which might have several parts, like different departments. The organization itself, or another company, or both, can own, manage, and run this cloud setup. It can be located either on-site or off-site.
2. A community cloud is used by a group of organizations that share common goals or needs, such as security or legal rules. This cloud can be owned, managed, and run by one or more of these organizations, or by a third party, or a mix of both. It can also be set up either on-site or off-site.
3. A public cloud is available for anyone to use. It is usually owned, managed, and operated by a business, educational institution, or government body, or a mix of these. This type of cloud is typically located at the provider's location.

Current Trends in Cloud Computing

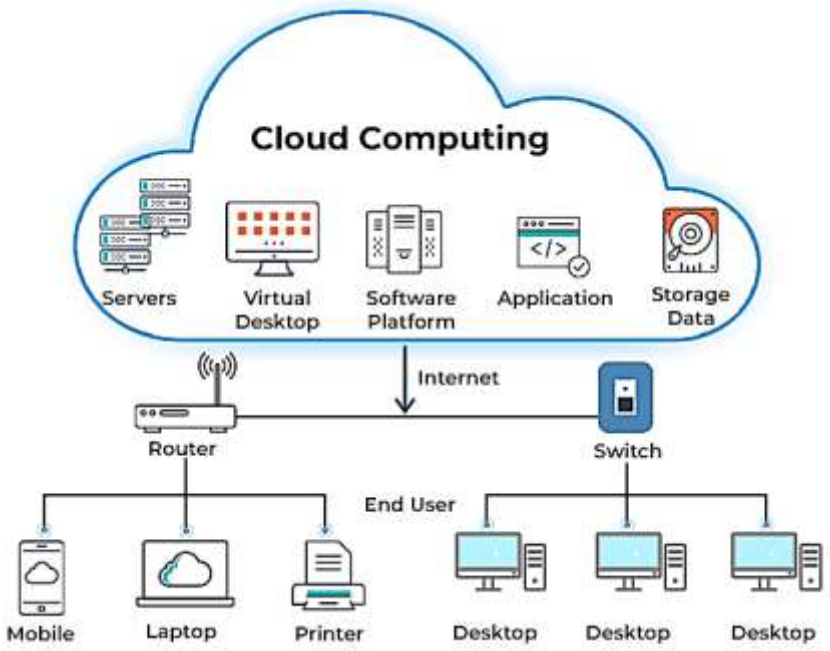


Figure 2.1: Cloud computing (Raj, 2019)

Methodology

This research explains the steps and methods used to carry out the study.

In the project called "An Improved Multilayered Security Framework for Cloud Computing in Internet of Things," the methodology explains how the research goals and objectives will be reached. The system is designed to produce results by processing the right inputs. This involves looking closely at different factors, understanding them, and finding the best or at least a good solution or plan of action. A detailed study of the process is done using various methods like interviews and questionnaires. The data collected from these sources is carefully examined to reach a conclusion. The conclusion is an understanding of how the system works.

Method of Data Collection

The data collection method used in this research is the secondary approach.

This means data was collected from existing sources such as lecture notes, journal articles, and conference papers.

Analysis of the Existing System

Data from these secondary sources was used to understand the current system.

Observations show that the existing system lacks the ability to send data from a local host to a cloud server. The Internet of Things (IoT) could offer security features that can effectively handle the increasing number of attacks on the system. However, the current system may not fully address many security issues related to collecting, storing, and processing sensitive data from IoT devices, which can put user privacy and regulatory compliance at risk. Also, the lack of standardization among different IoT devices and cloud platforms can make it hard to integrate and communicate effectively, making it difficult to apply consistent security rules and procedures.

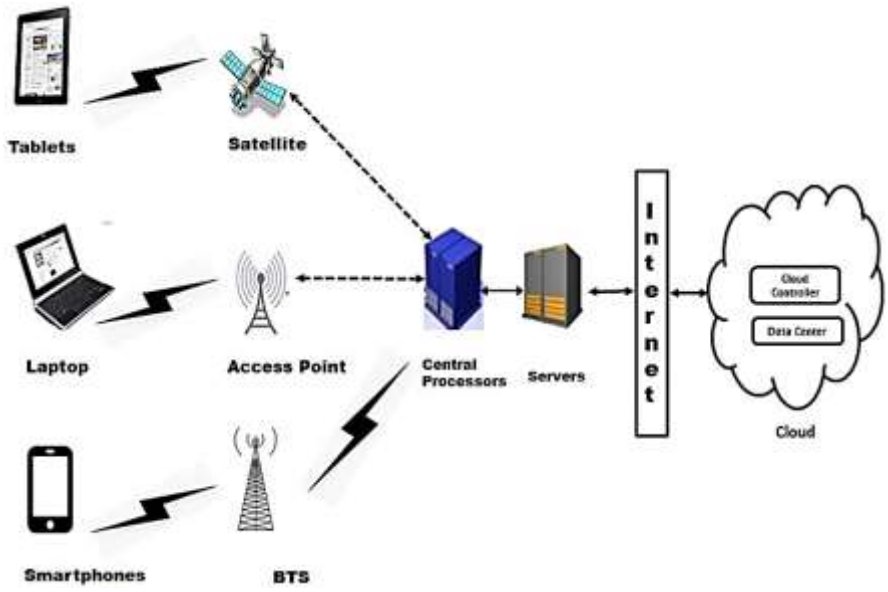


Figure 3:1 **Existing System Model**

The tablets, laptops, and smartphones are all devices that users use to send data from the system to a cloud server through communication channels such as satellite, access point, and base transceiver station (BTS).

These channels allow data to be sent via communication lines to the central processor. A domain host can act as a server, helping users to store and retrieve information in the cloud. The system involves multiple layers of security in a cloud computing environment integrated with IoT devices.

Analysis of the Proposed System

The proposed system aims to reduce the use of satellite and access points.

It offers a complete approach to protecting against threats. The central processor and server enhance security by handling a wide range of potential security risks in the cloud computing and IoT environment. The proposed system may include strong encryption methods and solid authentication processes to keep data transmission secure and ensure that communication between IoT devices and the cloud remains intact.

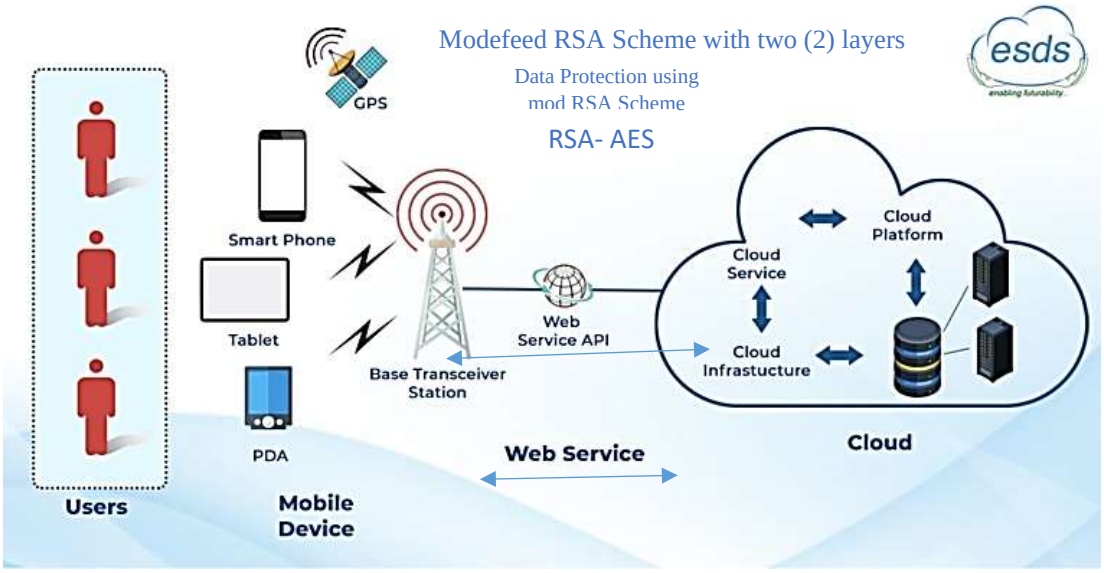


Figure 3:2 **Model of the Proposed System using RSA-AES**

Flowchart

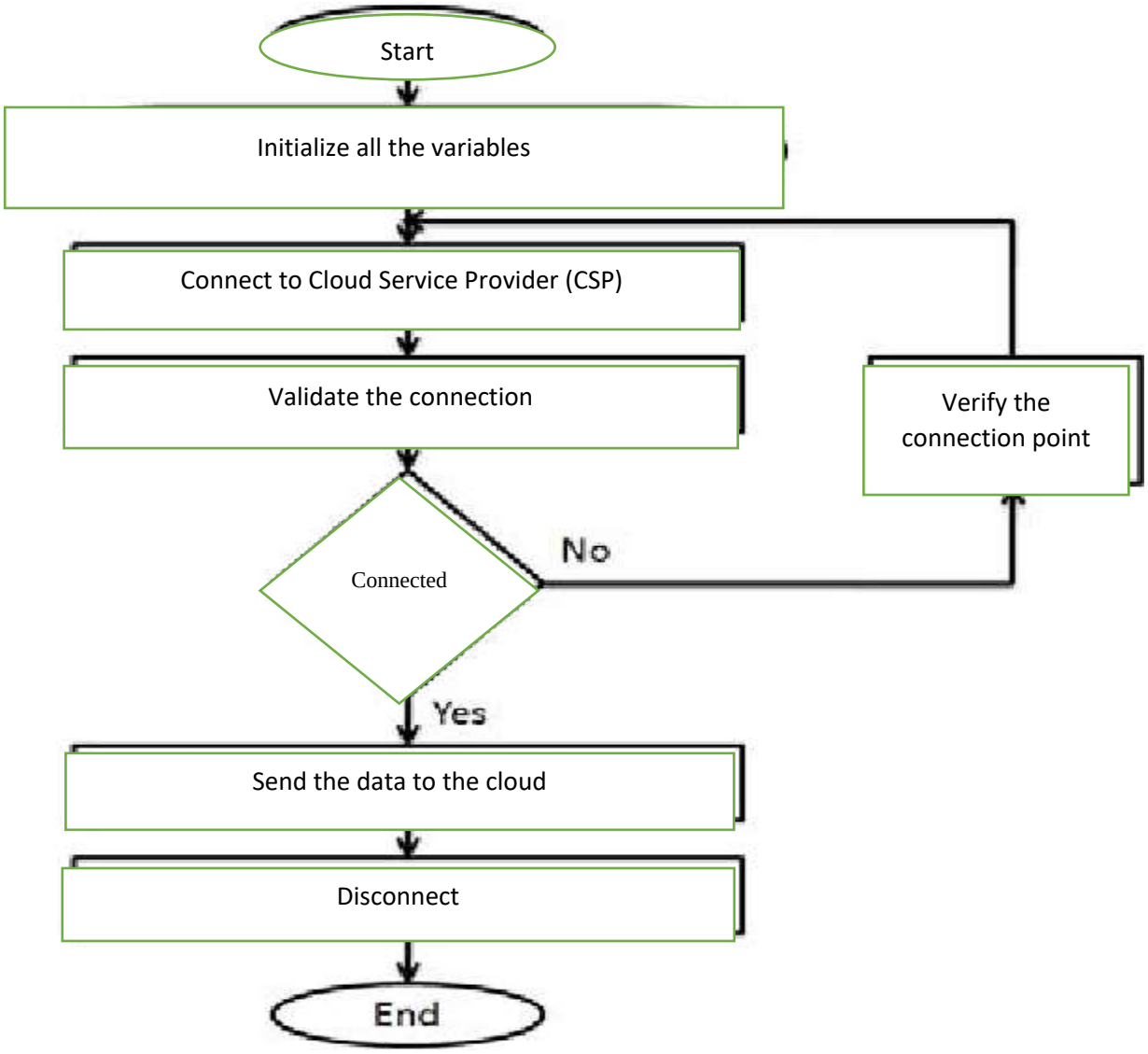


Figure 3:3 **System Flowchart of the Proposed System**

Algorithms Design

RSA Algorithms

1. Generate keys: (n, e), (n, d) = RSA_key_gen().
2. Encrypt message: c = RSA_encrypt(m, n, e).
3. Decrypt ciphertext: m = RSA_decrypt(c, n, d).

RSA Algorithm Steps

Key Generation

1. Generate p and q keys:
   - p = random_key()
   - q = random_public_key()
2. Calculate n:
   - n = p * q
3. Calculate phi:
   - phi = (p - 1) * (q - 1)

4. Choose public exponent:
   - e = random_exponent(phi)
5. Calculate private exponent:
   - d = multiplicative_inverse(e, phi)
6. Return keys:
   - public_key = (n, e)
   - private_key = (n, d)

Encryption method

1. Convert plaintext:
   - m = plaintext_to_number(m)
2. Calculate ciphertext:
   - c = mod_exp(m, e, n)
3. Return ciphertext:
   - c

Decryption method

1. Calculate plaintext:
   - m = mod_exp(c, d, n)
2. Convert plaintext:
   - m = number_to_plaintext(m)
3. Return plaintext:
   - m

AES algorithms

```
// Encryption
function AES_encrypt(plaintext, key) {
  // Key expansion
  round_keys = expand_key(key)
    // Initial round
  state = xor(plaintext, round_keys[0])
    // Rounds
  for i = 1 to Nr {
    state = substitute_bytes(state)
    state = shift_rows(state)
    state = mix_columns(state)
    state = xor(state, round_keys[i])
  }
  // Final round
  state = substitute_bytes(state)
  state = shift_rows(state)
  state = xor(state, round_keys[Nr+1])
  return state
}
// Decryption
function AES_decrypt(ciphertext, key) {
  // Key expansion
  round_keys = expand_key(key)
  // Initial round
  state = xor(ciphertext, round_keys[Nr+1])
  // Rounds
  for i = Nr to 1 {
    state = inv_substitute_bytes(state)
    state = inv_shift_rows(state)
    state = inv_mix_columns(state)
    state = xor(state, round_keys[i])
  // Final round
```

```
  state = inv_substitute_bytes(state)
  state = inv_shift_rows(state)
  state = xor(state, round_keys[0])
  return state
}
```

Combination of RSA and AES algorithms

Key Factor

1. Generate an AES key (128, 192, or 256 bits): `AES_key`
2. Generate an RSA key pair (1024, 2048, or 4096 bits): `RSA_public_key`, `RSA_private_key`

Encryption method

1. Encrypt the data using AES: `AES_ciphertext = AES_encrypt(data, AES_key)`
2. Encrypt the AES key using RSA: `RSA_ciphertext = RSA_encrypt(AES_key, RSA_public_key)`

Decryption method

1. Decrypt the AES key using RSA: `AES_key = RSA_decrypt(RSA_ciphertext, RSA_private_key)`
2. Decrypt the data using AES: `data = AES_decrypt(AES_ciphertext, AES_key)`

Result and Discussion

The fast use of Internet of Things (IoT) devices in many areas has greatly increased what connected systems can do. But this growth has also created big security problems, especially in cloud computing where a lot of important data is handled and kept. Because of this, this project presents a strong, multi-layered security system for cloud computing and the Internet of Things.

Result

Table 4.1: Encryption Time (Secs) for Existing AES vs Hybrid (RSA – AES) Scheme

S/N	Size(kb)	Existing AES	Hybrid (RSA-AES)
1	50	8.1	8.1
2	500	9.22	9.32
3	550	10.55	10.55
4	5000	13.62	13.62
5	5500	13.9	14.03
6	50000	14.85	16.41
7	50500	16.01	17.33
8	500000	20.8	22.02

Table 4.1 Encryption Table

Table 4.2: Decryption Time (Secs) for Existing AES vs Hybrid (RSA – AES) Scheme

S/N	Size(kb)	Existing AES	Hybrid (RSA-AES)
1	50	8.1	13.66
2	500	9.22	13.98
3	550	10.55	14.04
4	5000	13.62	17.63
5	5500	13.96	17.9
6	50000	15.5	18.32
7	50500	16.25	20.44
8	500000	22.94	28.67

Table 4.1 Decryption Table

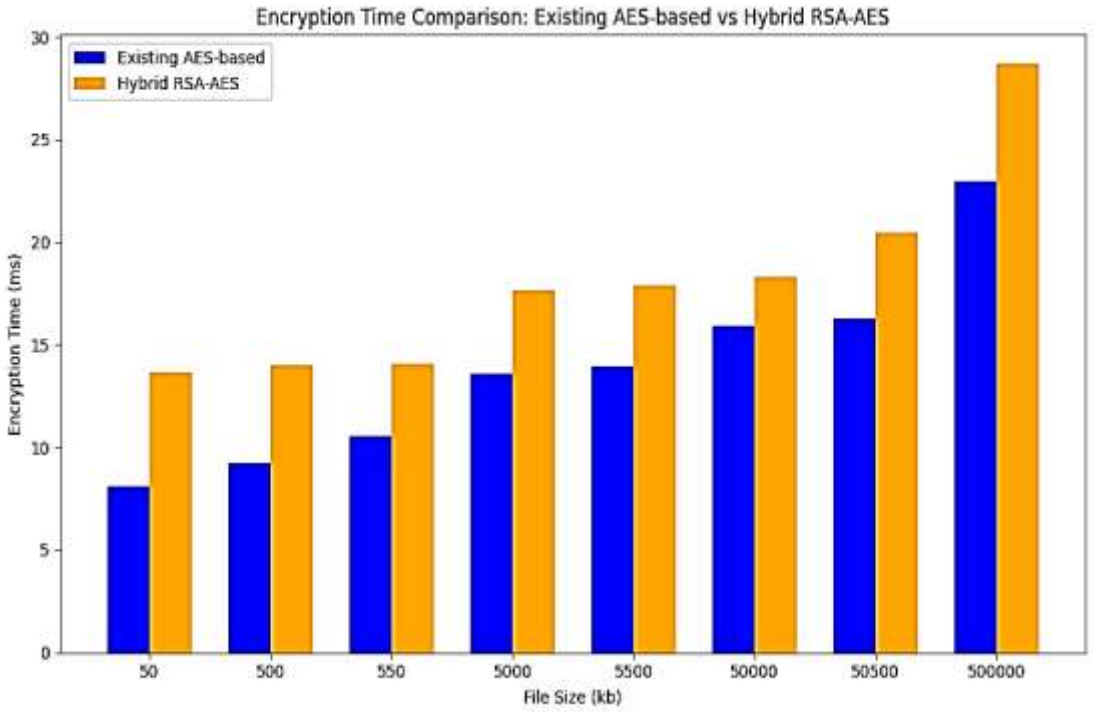


Figure 4.1: Encryption Time (AES vs RSA-AES) Graph

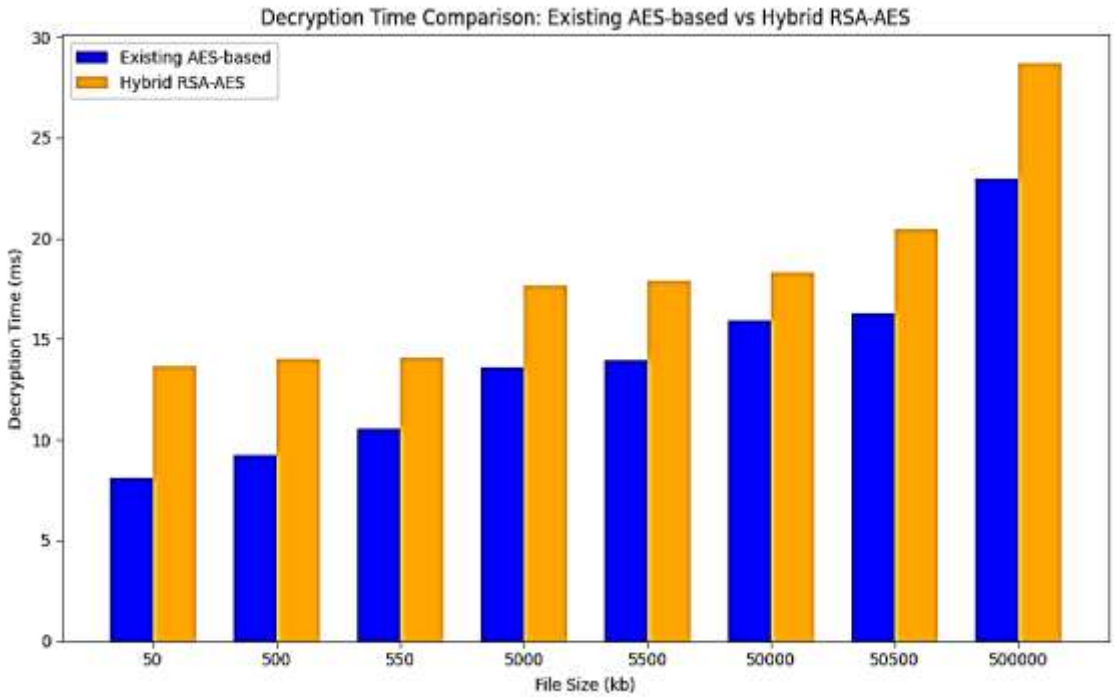


Figure 4.2: Decryption Time (AES vs RSA-AES) Graph

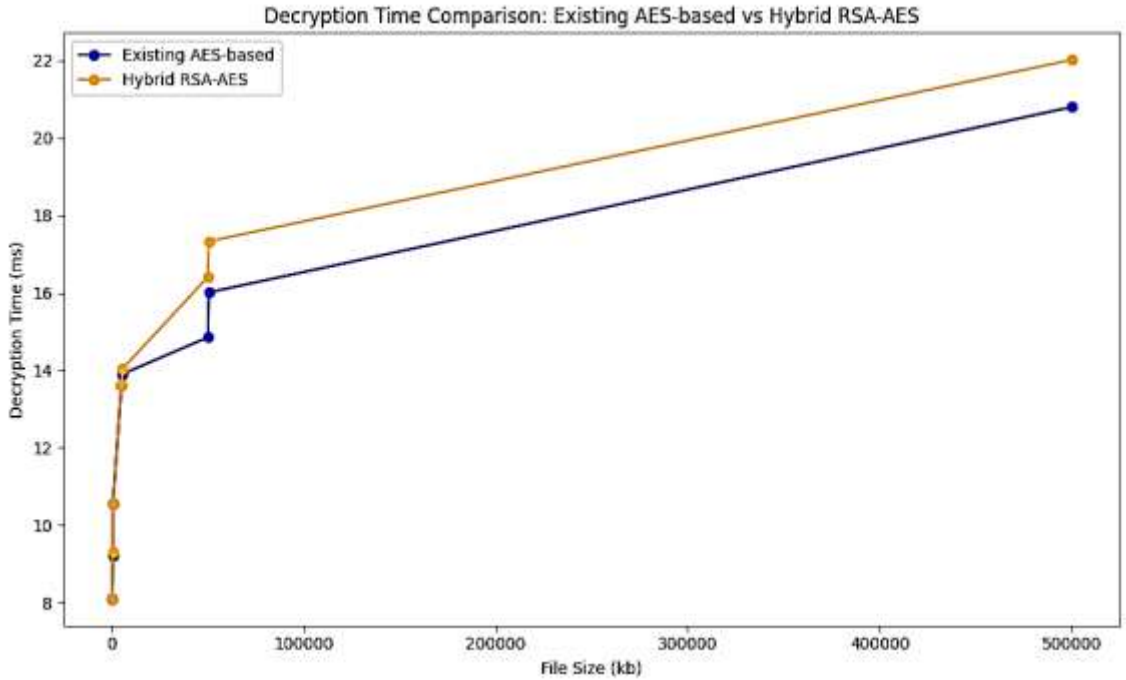


Figure 4.3: Decryption Time Frame (AES vs RSA-AES)

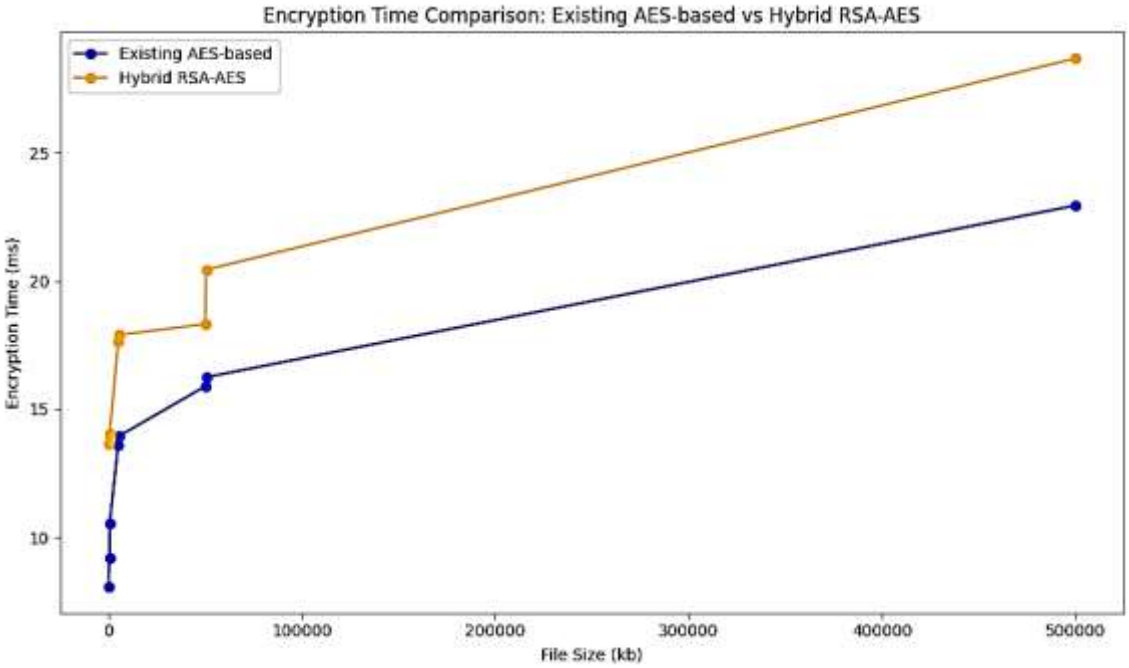


Figure 4.4: Encryption Time Frame (AES vs RSA-AES)

Conclusion

Cloud computing is an emerging technology that uses shared computing resources instead of local servers or personal devices to run applications. It provides services over the Internet, allowing users to access different software online. Many studies have been conducted, and various security frameworks have been suggested to address security issues in cloud computing. However, most of these frameworks do

not use a quantitative approach to assess and evaluate the privacy and security of data in cloud computing systems. In this research, we identify the main security concerns in cloud computing systems, analyze the threats, and suggest ways to counter them. We use a quantitative security risk assessment model to present a multilayered security framework to deal with security threats in cloud computing systems. To evaluate the performance of the proposed security framework, we used an Own-Cloud platform based on a 64-bit quad-core processor embedded system. The Own-Cloud platform is flexible and allows for the implementation of various analytics, machine learning algorithms, and signal processing techniques using the wide range of Python libraries available for these purposes.

Corresponding Author:
Dr. Omega Sarjiyus
Department of Computer Science
Adamawa State University, Mubi
Nigeria.
Telephone: +234 810 1825 010
E-mail: sarjiyus@gmail.com

References

1. Ishaya, T. (2021). Complexity and security in cyberspace. *Journal of Information Security*, 12(2), 56-71.
2. Zhang, Y., Zhang, J., & Liu, H. (2018). Security challenges in cloud-based IoT systems. IEEE Transactions on Cloud Computing, 6(4), 1234-1251.
3. Bonnet, T. (2021). The intersection of cloud computing and IoT: A conceptual framework. Cloud Computing Review, 12(4), 56-72.
4. Morabito, R. (2020). Cloud computing models: A comparative analysis. *Journal of Cloud Engineering*, 19(1), 34-49.
5. Grance, T. (2018). Security and privacy in cloud computing. *Cloud Security Journal*, 9(1), 67-82.
6. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2022). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
7. Roman, R., Lopez, J., & Mambo, M. (2021). Mobile edge computing and the IoT: Security challenges. Future Generation Computer Systems, 78, 680-695.
8. Botta, A. (2019). Multi-layer security in IoT and cloud computing. *Journal of Network Security*, 11(3), 123-140.
9. Raj, T. (2021). Security challenges in IoT and cloud computing. *Journal of Internet Security*, 19(2), 76-90.
10. Joel, R. (2019). Evolution of cloud computing service models. *Journal of Internet Technologies*, 10(2), 56-69.
11. Emmanuel, K. (2022). SaaS model and its impact on cloud computing. Cloud Computing & Applications, 14(2), 87-99.
12. Shrikant, N. (2020). Cloud account hijacking: Risks and mitigation strategies. *Journal of Cybersecurity*, 14(3), 45-60.
13. Joseph, D. (2020). Infrastructure-as-a-Service: An overview of cloud computing benefits. *Cloud Tech Journal*, 8(1), 90-103.
14. Ferreira, B. (2018). Infrastructure-as-a-Service: Benefits and limitations. Cloud Infrastructure Review, 7(3), 45-60.
15. Bollag, R. (2021). Computer-aided assessment in cloud-based learning environments. *Educational Technology Journal*, 29(1), 78-92.
16. David, P. (2017). Community cloud computing: A case study on Facebook. *Journal of Internet Computing*, 9(4), 210-225.
17. Alajjer, M. (2021). Availability in cybersecurity: Ensuring data accessibility. *Journal of Cybersecurity Management*, 14(1), 78-90.
18. Rajman, K. (2019). Frameworks in cybersecurity: A layered approach. *International Journal of Security Research*, 22(1), 112-127.

7/12/2025