Secured Intrusion Detection in Adhoc Networks

Mahmoud Zaher [1,*], Nabil M. Eldakhly [2]

[1] Faculty of Artificial Intelligence, Egyptian Russian University (ERU), Cairo, Egypt
[2] Faculty of Computers and Information, Sadat Academy for Management Sciences, Cairo, Egypt & French University in Cairo, Egypt
Email: mahmoud.zaher@eru.edu.eg; nabil.omr@sadatacademy.edu.eg

Abstract

Adhoc network computing is necessary in the present IT business since adhoc networks play such a huge role in it. Making computer talents connected to information technology available on demand using the pay-as-you-use payment model is the practice under question (PAYU). It is conceptualized as a collection of computational resources that has been developed rationally. Only virtualization, a crucial component, makes it feasible to provide ad hoc network computing services. By utilizing the underlying physical computing resources, such as processing power, memory, servers, programs, and other essential resources for calculation, this approach enables the creation of logical or virtual resources (instances). Due to the cost savings associated with virtualization, Adhoc Network service providers could be able to reduce their initial investments. It results in more efficient use of the available computational resources. When employing a virtualization approach to generate many resources or instances, it is vitally crucial for the users to determine whether these virtual resources satisfy, the criteria that have been set users have set outtake several forms, one of which is the creation of Routing Protocols (VMs). When multiple Routing Protocols are created by utilizing the underlying physical computing resources, it is essential for the user that these Routing Protocols perform processing without interrupting the other, as well as without any interruption from outsiders such as intrusions, malware, hackers, etc., It is essential for the user that these Routing Protocols perform processing without interrupting the other It is necessary for the user that these Routing Protocols perform processing without interrupting the other It is of the utmost importance to have a thorough understanding of how to prevent assaults, incursions, and system failures. In this article, we introduce several different approaches, each of which makes use of a variety of security components, such as a security watchdog, an IDS/IPS system, a security framework, an access control framework, a security supervisor, etc., to provide the required level of security for the Routing Protocols and their required resources. This is accomplished by enabling the Routing Protocols to function normally and without any problems from the outside or the inside of the working environment, all while making use of the accessible.

Keywords: Routing Protocols (VM); Intrusion Detection System.; attacks; Certificate Authority and TPA; Peer to Peer.

1. Introduction

Virtualization is how the detachment of consistent resources from physical resources occurs to fulfill the many requests made by various customers [1]. For instance, the processes may allocate more memory than the actual physical memory that is available by using valid memory. This is accomplished by trading the information and data from primary to auxiliary memory and vice versa. Even if the physical resources are divided among the different customers and distributed to them, every client is given the impression that they have their own resources and are expected to operate as though they had access to physical resources. This method also works with several layers of resources, such as systems, [2] servers, desktops, platforms, and applications.

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

As soon as we have brought together systems that are similar into a more effective structure, we will be able to begin automating the management of those resources, allowing us to add and move capacity as required. Instead of relying on resource order to determine [3] how well the trade operates, businesses should be allowed to drive how resource components are used. Automating things like adding or reducing capacity can lead to advancements in task automation all allied with a given process or sub-process, such as application testing or release management of an updated production configuration. This can be accomplished by automating things like adding or reducing capacity. Another important action at this stage is to begin the process of gathering and organizing [4] the many components of the unified resource via the various firm activities. When this is done, a company can leverage resources that may be idle at various times of the day to execute tasks that are overloaded at the exact time as those idle resources.

When businesses can share these assets consistently, it offers them the ability to swiftly adapt to changing business demands without having to devote an excessive amount of resources to innovation. Companies may not let the standard procedure that may be in place today slow down the adaptation of help to new workloads if they want to get the most out of these resources and utilize them as efficiently as possible. We need tools and procedures [5] that enable the automatic orchestration of resources to adapt to those business concerns so that we can make the environment as fluid as possible and more accessible to work in.

We anticipate that enterprises will eventually be able to migrate to enterprise-wide virtualization that is made possible by a global virtualization fabric as their capabilities for virtualization and automation continue to advance inside their organizations [6]. This fabric makes use of sophisticated virtualization methods that are made accessible by grid technologies and more powerful mainframe virtualization platforms to provide smooth access to organization-wide resources, regardless of where they are physically located. It begins to remove barriers between resources that have been erected as a result of hierarchical data centers or administrative structures. To conclude, we see organizations utilizing these advanced virtualization concepts not only to access resources within their own organization but also to see resources on demand truly. This is true regardless of whether the resources are located within or outside the company at partner [7] or vendor locations. In this state, resource components are present when needed, uttermost loads can be tuned without keeping unused capacity on the floor for extended periods, and information flows seamlessly between organizational functions, both within and outside of the company. In this state, the resource components are present when needed.

Security Measures for Virtualization Used in Adhoc Network Computing Services [8] Located in Bengaluru, the Department of Computer Science and Engineering at Jain University. Security management is one of the most important components that must be present for effective enterprise-wide and inter-enterprise resource sharing, application integration, and cooperation on business processes. Authentication, authorization, and access control are three fundamentals that must be implemented across all systems, networks, and applications. Establishing roles and using identity management will, in the long term, save time and money while instantly increasing security levels. Suppose we have the correct solution providers for security and verification amongst our suppliers, partners, and customers. In that case, we will be able to more easily achieve the condition of being "always on." All of these infrastructure [9] management strategies are accessible today. Still, many businesses need help to implement them as quickly as they would want because their IT governance and management procedures need to be updated. Because of this, companies need to address the policies and cultures inside their organizations that prevent them from entirely using the technologies that are now accessible.

The device on which the Hypervisor is running serves as the central control point. This device is responsible for allocating resources to the virtual instances that are created before the processing begins and then removing those resources from the cases once the processing is complete, which results in the termination of the virtual instances. It is possible that it will not be able to defend itself against attacks since it is in the position of creating, allocating, and de-distributing resources. The Routing Protocol Monitor (VMM) [10] has evolved into a critical vulnerability. The virtual instances of some other physical machine may attempt to access resources from this VMM. Additionally, these virtual instances may attempt to insert assaults into the virtual environment by compromising the security mechanisms. A number of fundamental characteristics, including service on demand and dynamic adaptability, distinguish Adhoc Network computing.

When there is customer demand for information technology resources, Adhoc Network specialist co-ops are obligated to make such resources available without falling short of the need. When a client makes a request for resources that is different from one they have made in the past, the security components for these resources need to be able to recognize [11] the differences and work with the client's private Adhoc Network provider to attempt to provide the necessary level of protection to the new request. These resources are equipped with some level of security systems. These solicitations go through a process of gradual adjustment as a direct result

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

of the needs that are expressed by the customers. The significance of Adhoc Network computing is steadily growing, and as a result, the quality and level of administration and protection ought to be increased. This is necessary so that customers can utilize Adhoc Network-based resources in a secure and risk-free manner, which may result in an expansion of the Adhoc Network business and enable Adhoc Network service providers to participate in the execution of extremely high standards of assurance and security systems while simultaneously satisfying more customers. It is widely recognized as the most significant challenge posed by Adhoc Network computing.

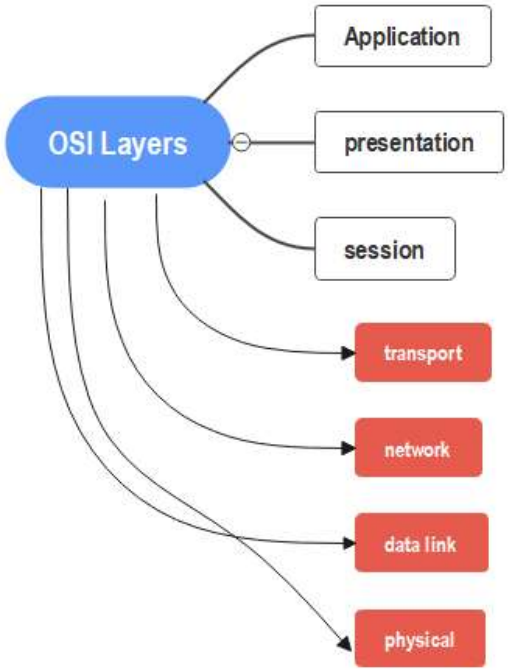

Figure 1: General layers in Wireless Network

Accessibility is not only a problem with regard to creativity; it is also a problem with regard to business. When it is functioning well, you are not aware that it is there; hence, it is easy for the administration to assume that it will, on average, be present. In most cases, achieving an exceptional level of asset accessibility calls for the Adhoc Network's owners to make significant investments in the Adhoc Network's foundation and various resources, as well as in the concept of virtualization, in order to create sensible resources that have sufficient security components to ensure both physical and consistent resources. Users and accesses that have been granted permission [12]: The authorized customers have access to a greater number of privileges than the regular customers have.

Because regular customers are typically kept away from the fundamental level of security in order to avoid genuine attacks at the underlying stage itself, the chances of infusing attacks and including risky access to resources are typically higher only with authorized clients [13]. This is due to the fact that the odds of infusing attacks and including risky access to resources are typically more with authorized clients. The most important challenge is identifying the authorized customers who are taking part in risky activities. These customers have permission to access the assets and enter the virtual environment, so they may successfully take part in risky activities. This is one of the key challenges. Data that can be relied on: the originality of data and information is of the utmost importance. There is no use in transmitting the information if the recipient does not get the original data. It is of the utmost importance to save and store the original data without allowing it to get corrupted or contaminated.

Because the internet is accessible to everybody and everybody and nobody owns it, any data that is being sent to or from a storage device or a server over the internet runs the risk of being corrupted by malicious actors or intruders. It is possible for limited users to pollute the original data and introduce attacks on it. This will result in the destination perhaps needing to receive the material in its original form. If data that has been damaged in

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

this way is utilized by IT organizations [14] to operate their businesses and make key choices, then those companies will suffer significant consequences for their operations. Amenity Users of Adhoc Network services place demands on Adhoc Network-based specialized cooperatives for the needed resources, such as virtual goods, applications, infrastructures, platforms, or capacities. Privacy is one of these requirements. In this particular scenario, the customer has to interact with the Adhoc Network specialist business and use the Adhoc Network services that they provide. During the course of this partnership, information and private data pertaining to Adhoc Network administrations will be traded via system exchanges. In this situation, it is essential to maintain the data of the customers and their current condition in a safe and secure manner. The restricted customers have the ability to try to hack the private data of other clients. This may cause serious problems for the customers.

The technologies and ideas that are used in Adhoc Network services have yet to achieve their full potential, and a number of the capabilities still need to be created and investigated to a degree that enables their manipulation to reach its full potential. Adhoc Network computing necessitates the use of virtualization in a significant way. It is unrealistic for us to anticipate excellent business from the Adhoc Network (from the perspective of Adhoc Network service providers) and good services from the Adhoc Network (from the perspective of Adhoc Network service consumers). Because users anticipate having access to scalable resources, the Adhoc Network will only be able to offer really excellent outcomes if it has been virtualized, standardized, and automated. Virtualizing, standardizing, and automating [15]our processes is the only way we are going to be able to achieve the necessary level of expertise. And as a result, costs will be reduced while also leading to an improvement in service. This is without a doubt an alluring equilibrium, and we are seeing businesses that are adopting this strategy get very genuine quantitative trade results. Today, the creation of logical instances at all phases (system, storage, and network) is becoming more important as a means of enhancing system security, trustworthiness, and readiness, lowering costs, and providing greater flexibility. It is necessary for us to express our expectations and provide clarification on the virtualization security in the Adhoc Network computing environment. Providing security for virtualization is always a tough process, regardless of the complexity of the computer environment in which it is being performed, whether it be basic or complicated. In addition to this, when working in an environment like the Adhoc Network, which consists of many types of Adhoc Networks such as public Adhoc Networks, private Adhoc Networks, and hybrid Adhoc Networks, it becomes much more difficult to do so because of the heterogeneous nature of Adhoc Network computing services.

.

2. Related Work

It is vital to have some level of deep awareness of the contributions made by a variety of different researchers in the past in order to be successful in any form of activity, particularly research. It is extremely crucial to have a correct analysis of the previous contributions, as this will allow us to get to a level where we can clearly and technically describe the issue statement, which will allow the research that is being done to have a more objectively focused directions. In terms of reducing the amount of time spent on experimentation and design, this provides us with a means to think about what should not be done. During the course of our investigation, we read a variety of research articles, and a synopsis of each of them is presented in the following order:

[16] describe "another technique to cope with combining virtual bunches, security-enhanced datacenters, and trustworthy information gets to directed by reputation frameworks." It is proposed to use a chain of the significance of P2P notoriety frameworks in order to defend information objects at the document get-to level and to secure mists and data centers at the site level. Distinct security countermeasures are being offered in order to guarantee Adhoc Network benefit models such as IaaS, PaaS, and SaaS, which are now being carried out independently by Amazon, IBM, and Google respectively.

[17] "Virtualization provides a coarse-grained detachment mechanism that results in vast frameworks, with entire operational frameworks and a complete programming stack as its establishment." Despite the fact that a significant portion of this foundation is not totally vital, the automatic weight of constructing Virtualization Security for Adhoc Network Computing Services remains the same. systems at a finer granularity, on a smaller establishment, have previously been shown to be difficult to achieve. This research was conducted in the Department of Computer Science and Engineering at Jain University in Bengaluru. They decided to introduce Macro Components as an alternative, lightweight, and composable method for dealing with virtualization. Macro Components are programming parts that keep running independently from the rest of the framework but without the full establishment of their more typically virtualized partners. They argue that this technique will provide a more flexible and supportable method for developing strong services in Adhoc Network environments, both in terms of specific framework aspects and programming designing attributes. Large-scale segments provide a lightweight compartment for programming parts that maintain operating disconnected from

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

whatever is left of the framework, but without the complete setups of its more generally virtualized companions. These parts keep running in isolation from the rest of the framework. This strategy may provide a more adaptable and controllable method for developing powerful services in Adhoc Network benefit environments by reducing the setup upon which virtualization is manufactured and by consolidating basic principles of component-based software development.

[18] "Web mists operate as administrative businesses working around web-scale server farms." The adaptable Adhoc Network resources and enormous datasets that are produced are vulnerable to security threats, abuse of protection, and violation of copyright laws. Adhoc Network assets that are sent in response to a request are especially defenseless against digital attacks. The Adhoc Network platforms that have been developed by Google, IBM, and Amazon all reveal these deficiencies. They provide an alternative approach to dealing with coordinating virtual bunches, security-fortified server farms, and trustworthy information access that is directed by reputation frameworks. At the site level, it is suggested to implement a chain of the significance of P2P notoriety frameworks in order to protect mists and server farms. At the record obtain level, it is recommended to protect information objects. It is advised to take a variety of security precautions in order to guarantee the following Adhoc Network benefit models: infrastructure as a service, platform as a service, and software as a service, which is now being independently carried out by Amazon, IBM, and Google [19]. They suggest creating a chain of the significance of notoriety frameworks in order to regulate the access to the server farm on a coarse-grain level and to restrict the information accessible on a fine-grain document obtain level. They implemented Adhoc Network engineering with incorporation as a means of strengthening the protection and safety afforded by Adhoc Network applications. To further protect the common populace, it has been suggested to add a few more layers of protection. It is imperative to implement these technologies in order to expedite the mainstream acceptance of web-scale distributed computing in personal, commercial, and governmental applications. Department of Computer Science and Engineering, Jain University, Bengaluru Web Virtualization Security for Adhoc Network Computing Services 42 Adhoc Networks act in a way that is constructively congruent with the goal of globalizing information technology. Regardless of this, there remains a significant gap between operability and fundamental Adhoc Network benchmarks, both of which still need to be solved.

[20] "Making the virtual assets from existing physical assets i.e., virtualization is another worldview for investigation recently, and virtualization innovation can bring comfort (regarding the diminished venture, simplicity of support, sharing) to the administration of processing assets. The invention of system virtualization is given new opportunities as a result of this, in addition to the enhancement of the system and the registration of the system. The innovation known as distributed computing administrations makes use of the virtualization technique simultaneously.

Because of the rapid evolution of technology, it is susceptible to a number of security flaws, including attacks such as rootkits and destructive modifications. Unsavory projects [21] have the potential to infiltrate the framework and might be booted up at any time the virtualized assets are used. The amount of study that has been done hypothetically on booting a put stock in a virtualized framework is really little. They suggest a dynamic trusted model with the ultimate objective of providing a hypothetical model for not only examining the state of a virtualized framework but also designing trust in the Routing Protocol application. In other words, they want to present a model that can be used for both of these things. A process known as TBoot is used to boot a reliable virtual computer. They make use of their model to demonstrate that TBoot is capable of booting a trustworthy Routing Protocol in a hypothetical scenario. The model illustrates the separation of the measuring and confirming processes. By using this approach, it is possible to implement complicated logic on the stage of the put stock in Routing Protocol. It is also possible to define the essential state of a trusted machine as one in which a system has at least one base of trust for estimation, and each component in the system is either an individual from a putting stock in root set or has a chain of trusting between one of the putting stock in roots and components.

[22] "The notion of Adhoc Network storage has gained substantial support and extensive attention from leading suppliers." [citation needed] Because the notion of virtualization plays such an essential part, they advise using a layered and universal Adhoc Network storage architecture that combines the technologies traditionally associated with virtualization. It has two layers of virtualization, the first of which converts physical space into logical volume, and the second of which converts logical volume into virtual volume. As a result, it offers users the ability to customize the size of the virtual space that they have available to meet their needs. It significantly improves the usage of the storage space while also being expandable. They gave some thought to the Adhoc Network storage system that was offered by their storage virtualization framework.

[23] "Constancy is one of the most important plans to strengthen the security of existing heterogeneous Adhoc Network stages." They demonstrated that the test results can affirm that the model can productively and securely develop reliable relationships in heterogeneous Adhoc Network conditions. They proposed a novel constancy to demonstrate CDSV to improve the security of heterogeneous Adhoc Network situations by utilizing framework-level virtualization methods. The framework-level virtualization provides enormous

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

opportunities for the adaptability, security administration, and transmission of Adhoc Network-based frameworks.

According to a survey of research papers that are reviewed for the purpose of identifying the problem statement, it has been observed that the majority of researchers primarily concentrate on the security of the Routing Protocol Monitor (VMM) or the Hypervisor. This is because the Hypervisor plays the leading role in the process of creating virtual resources based on the requirements of the situation. According to the findings of the researchers, the primary security risk is posed by the Hypervisor itself; consequently, it is essential to focus primarily on the safety of the Routing Protocol Monitor [24]. A large number of researchers have proposed a variety of frameworks with the intention of providing security to the Routing Protocol Monitor. These frameworks are designed to address particular problems that arise in the IT industry. Some of these frameworks offer security solutions to particular Adhoc Network service models, such as infrastructure-as-a-service (IaaS) or platform-as-a-service (PaaS), while others offer solutions that are unique to particular deployment models, such as public Adhoc Network or private Adhoc Network. The majority of the proposed solutions are tailored to the particular business models of the respective vendor products, such as Xen and VMware, amongst others.

The majority of the approaches that were proposed have their primary focus on identifying the intrusions, security vulnerabilities, threats, and malware that are injected into the virtualization environment rather than on healing them. This is because the majority of these problems are preventable.

The overarching goal of our system is, first and foremost, to recognize and then eliminate those issues. In addition, the processing of Routing Protocols that are infected with the problems described above should be halted so that it is possible to avoid the interruption or corruption of other Routing Protocols that are working. The fact that this security system can be used in any Adhoc Network service model or deployment model is the primary benefit of this system. It is applicable to any circumstance in which there is a possibility of danger to the virtual environment, particularly for Routing Protocols [25], and can be utilized in these contexts. In addition to this, it entails the utilization of multiple levels of security mechanisms in order to identify and fix the virtualization environment.

2.1.1 Current access control methods in Adhoc Network Computing

Access control has been one of the most pressing concerns in Adhoc Network computing because Adhoc Network computing involves the sharing of applications and physical resources with a variety of users and organizations. Nevertheless, the Adhoc Network system will only fulfill its intended function as a shared service if the IT department chooses to restrict access only for concerns of security.

Table 1: Summary of existing password authentication technique limitations.

```
FG_TIMEOUT = 880;
    HELLO_INTERVAL = 1000;
    HELLO_TIMEOUT_INTERVAL = 3000;
    JT_REFRESH = 160;
    MEM_REFRESH = 400;
    MEM_TIMEOUT = 960;
    RTE_TIMEOUT = 960;
    RT_DISCV_TIMEOUT = 30000;
    TTL_VALUE = 32;
    version = 0;
    overhead = 64;
    m sender = [1 0 0];
    m node = [1 1 0];
    m receiver = [33 205 163] ./ 255;
```

Therefore, flexibility is a necessity when designing the access control mechanism since it must be able to accommodate different types of policies and domains.

Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) [26] are the four major access control methods used for various Adhoc Network infrastructures. There are many methods designed to prevent an unauthorized user from accessing an Adhoc Network computing system.

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

The first approach is to put on a safety mechanism within the virtualized computing environment, to screen the stream of traffic flow between the Routing Protocol Monitor and one or more Routing Protocols. The upper part of the diagram is the one where we don't have any security system. To make the virtual environment safe, the lower part is provided with a security system, which is called an Intrusion Detection System, and Intrusion Prevention System. It is shown in the figure given below:

Figure 3: Security mechanism applied between VMs and VMM Virtualization Security for Adhoc Network Computing Services

The security mechanism ie., Intrusion Detection and Prevention System (IDS/IPS) [27] system provides protection against attacks originating on the network. This protection mechanism checks each and every request and replies message that is communicated between Routing Protocols and the Routing Protocol Monitor. When they receive each and every message, they check for malware, threats, and any other type of problems that may be present in the messages. If it encounters any such problem, then they immediately avoid that infected message to transfer in between Routing Protocol and Routing Protocol monitor to avoid the problems which may arise with the Routing Protocol environment. The system tries to make those messages free from infections. But there are some significant limitations to this option:

• Security mechanism is available between Routing Protocol [28] and Routing Protocol Monitor, which cannot prevent attacks, threats, or malware between Routing Protocols.

• If we enable the Routing Protocols 29] [to move from one physical machine to another, the security setting is lost. It is important to arrange the gathering of security apparatuses for each potential goal to which a Routing Protocol could be moved, bringing about a comparing negative effect on execution.

• The Security mechanism must handle all the communication traffic between all the Routing Protocols, Routing Protocol Monitor, and the network, this will result in performance degradation. • There are chances of malware, threats, and viruses that may be injected from outside directly into the Routing Protocols or into the Routing Protocol Monitor, which makes Routing Protocols and Routing Protocol monitor behave abnormally by consuming more computing resources such as processing power, memory, network, etc., This cannot be identified by the security mechanism which is installed between the different Routing Protocols and the Routing Protocol monitor. These are the limitations that make the security mechanism that is installed between Routing Protocols and Routing Protocol monitor not in the position to provide security to a whole virtual environment, to make Routing Protocols work normally without consuming more computing resources. Virtualization Security for Adhoc Network Computing Services.

This approach is simulated using the Adhoc Network sim simulator tool [30]. The results are given in the Result section. This is the simplest approach, which provides security for the transactions between different Routing Protocols and Routing Protocol monitors. Here Routing Protocols are created using Adhoc Networksim and allow them to interact with VMM for resource allocation. We make them send the requests to VMM for more resources such as processor time, memory, etc. than they actually required. This cannot be handled by the IDS/IPS system. Since it is there for avoiding threats, it can detect only the transactions that are infected. It cannot identify the requests from VMs for more resources than actually required.

3. Proposed Methodology

When thinking about the safety of Adhoc Network data, the major focus of attention should be placed on the protection of data when it is resting in the Adhoc Network. There are still worries over the customers' right to privacy and the protection of their data, even though consumers are informed of the location of their data and that there is no mobility for the data. There is no doubt that the sector of Adhoc Network computing has grown owing to the versatility and broad network access that is provided by it. On the other hand, dependability in the sense of offering a setting that is free from danger and safe for the user's personal information and data is very necessary.

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

The Advanced Encryption Standard (AES) is a method that is used throughout this work, and before uploading any sensitive information to the Adhoc Network, it is encrypted. Instead of storing the original data, the Adhoc Network database stores the encrypted data that has been stored there.

The computer's memory is cleared of the original data. The data will be encrypted and made accessible to the user after they have submitted a request to utilize the data. This request must come from an authorized user. This solution can handle multi-tenant infrastructures, which means that inside such infrastructures, material may be delivered in a quick iteration cycle.

Simply refreshing the browser will cause any newly introduced functionality to become immediately visible in the user interface. When this occurs, it means that new features have been introduced. The implementation of extra functions is segmented into more manageable chunks, which, in turn, serves to reduce the threshold for effective change management. It provides support for Adhoc Network computing and will be updated regularly to fulfill the current needs of consumers after obtaining feedback and data on usage from millions of users. This was done to satisfy the current demands of consumers. The data that is provided by customers is not stored in a single place or on a single piece of equipment; rather, it is stored in several reliable nodes that are spread out over the network. This is done to ensure that the needs of clients may be satisfied no matter where in the world those customers may be situated. This program gives many users the ability to swiftly and concurrently access its features from a wide range of places. It also makes it possible for this access to take place at the same time

. 3.1.1 Algorithm based on the AES

The Advanced Encryption Standard (AES) encryption algorithm is a kind of symmetric encryption technique. It is recommended that the length of plaintext be 128 bits, whereas the key length may be one of three possible values: 128 bits, 192 bits, or 256 bits. The AES method was finished after Nr iterations, which were determined by the secret key length. The following table illustrates the link between the number of times played and the length of the key.

Table 2: Relationship of Nr times and key length

Key length	128	192	256
Nr times	10	12	14

1. The 128-bit plaintext input is broken up into 16 bytes, which is often represented as a four-by-four matrix; the size of each matrix element is 8 bits (one byte).

2. The sequence of characters found in the plaintext, from left to right, is as follows: S00, S10, S20, S30, S01, S11, S21, S31, S02, S12, S22, S32, S03, S13, S23, S33. The term "state" is given to the block of plaintext that is present in each step of the wheel transform.

3. Initial plaintexts block M consists of the following: s00 s01 s02 s03 s10 s11 s11 s13 s20 s21 s12 s23 s30 s31 s13 s33

4. The following are the stages involved in AES encryption:

We carried out a game of secret key plus operator in the first round.

5. Carried out iterations of the Nr-1 kind. Utilize the S block to do a substitution on each byte, then perform the displacement on the output of the substitution, followed by the mix column transform. Following this, a round of the game secret key plus operator will be played.

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

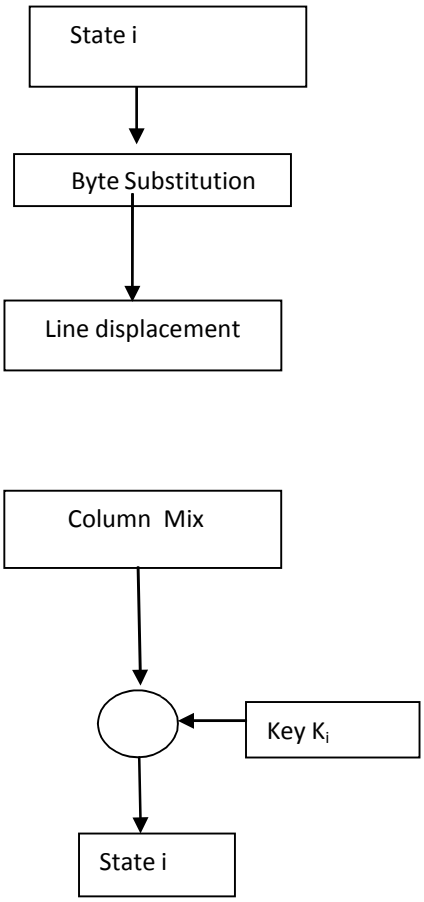

Figure 2: Encryption process

1.1 The design of the Adhoc Network storage system with AES algorithm

The purpose of this system is the development of secure Adhoc Network storage services

The module of system file operation uploads, downloads and deletes data by a call to the interface for Adhoc Network storage, and the platform provide a Restful Web Service interface. The Adhoc Network storage interface uploads files using PUT and sends a request to the server using GET, server returns the link of file-download and sends a request for file deletion to the platform server using GET to delete files, finally server will return the corresponding result.

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

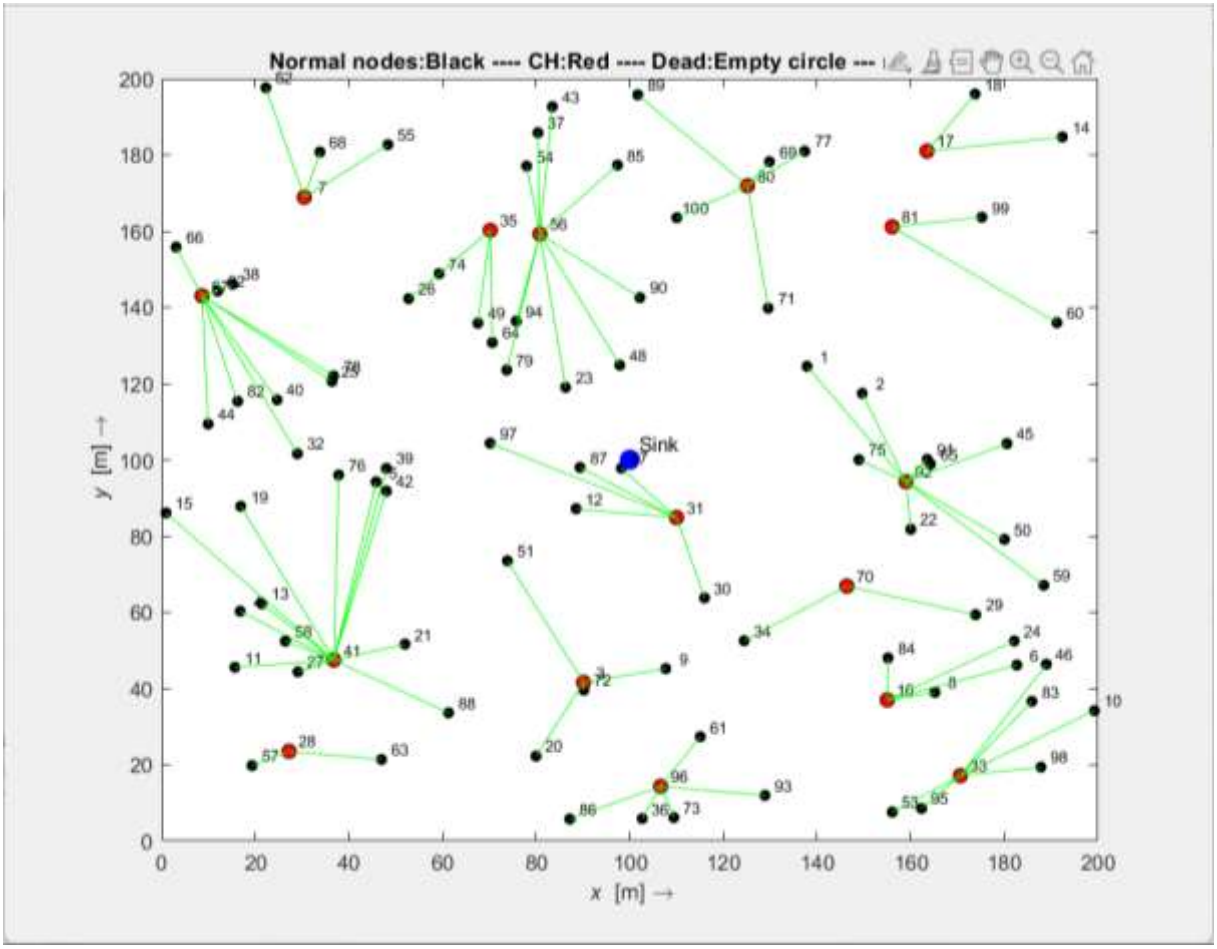

Figure 3: Adhoc Network Storage System

1. Implementation of the Advanced Encryption Standard

2. In the modules that handled the uploading and downloading of files, encryption and decryption of files were employed, respectively.

3. The process of encryption

4. A byte transformation is defined by the AES as an S-box matrix that is built of a 16 × 16 array of bytes. When searching the S-box table, use the high four bits of the eight matrix elements as the row value and the low four bits of the eight matrix elements as the column value. The value that corresponds to each search result is the result of the transformation matrix elements.

5. Move a row in the state matrix by using the row displacement operator.

6. For the column mix, AES decided to use a constant polynomial, which makes the calculation much simpler. The formula for the polynomial is as follows: c(x)=03x3+01x2+01x+02.

7. Key Expansion: the key that has to be determined as the fundamental unit of bytes is represented by a matrix that consists of four lines. Round key length equals block length multiplied by (Round Nr+1).

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

The process of decryption

1. Inverse byte substitution: This technique, which is quite similar to the byte substitution technique, searches each byte through the table.

2. Inverse row displacement: This refers to the procedure that contrasts with row displacement.

3. Inverse column mix is an operation that is quite similar to column mix; however, inverse column mix has its polynomial to work with. The formula for the polynomial is as follows: d(x)=0Bx3+0Dx2+09x+0E.

4. Key plus: this is the same as the key plus operation that is performed during the encryption procedure.

a) File Upload

This section will walk you through the many processes involved in the process of uploading files:

1. Request the user's login name and password and save them.

If the user has been authenticated, a connection should be established with the Adhoc Network. In such cases, display the authentication error.

2. Instruct the user to choose an upload file before sending it to the Adhoc Network.

3. To begin the encryption process, the user should be asked to provide a password.

4. Write down this password, then create a key using this password.

5. Start using the technique for encryption

6. Place the file in an Adhoc Network storage location.

7. After the file has been uploaded, ask the user if he wants to remove it and provide him with the option to do so. Delete the file if the user chooses to delete it using the option that's provided.

8. Cut off your connection to the Adhoc Network.

This section will walk you through the many processes involved in the process of uploading files: Step 1: Request the user's login information and then accept it.

The technique that we have given tries to stop any attacks that might be launched against the user data. Authentication is the first step in accomplishing the same goal. The user's submission of their username and password will be accepted by the system. After these two things have been confirmed, the user will have access to their data. After the username and password have been entered, you should confirm the authenticity of the information. The system will only create a connection with the Adhoc Network if the username and password that were supplied are correct. If the user's name and password are incorrect, the system will display an error message and refuse to allow the user to proceed.

Step 2: Instruct the user to choose a file to save in the Adhoc Network and ask for their approval.

The subsequent stages will only function properly if the user has already been authorized and an operational connection has been established with the Adhoc Network. In this section, you will choose the file that will be uploaded. The user can pick any text file that is presently stored in the memory of the system that they are using. After selecting the file that is going to be uploaded,

Step 3: To continue with the encryption procedure, the user will be asked to input a password.

In this stage of the encryption procedure, the user will be prompted to input a password. It is strongly advised that the user make use of lengthy passphrases wherever possible. This password will be necessary to generate a key.

Step 4: Write down this password, and then produce a key using the password you just wrote down. This is a very important step for the system. During this stage of the encryption procedure, a key will be produced for use. The Advanced Encryption Standard (AES) is a symmetric key technique, which

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

means that it employs the same key for decrypting the material as it does for encrypting it. Through the use of a key generator function, this key is produced using the password. We suggest that you make use of PBKDF2 (Password-Based Key Generation Function 2). The increased amount of processing makes it much more difficult to break a password. This technique is referred to as key stretching. It is important to note that even if the keys used for the AES method are not vulnerable to any known attack, there is still a chance that the password might be compromised by a Brute-force assault. This is something that should be kept in mind. Because of this, it is strongly suggested that the user make use of lengthy passphrases when it comes time to generate the key. Therefore, after the password is input, the system will immediately begin to produce a random encryption key and will also remember the password.

The fifth step is to use the encryption algorithm.

In this stage of the encryption process, our encryption method, which is known as the AES algorithm, is applied to the plain text to produce the encrypted text. As was previously established, there are no known attacks that can be used to break AES. Therefore, the user may have peace of mind knowing that his data is protected from the myriad of risks associated with Adhoc Network security. The data of a user is protected in two ways: first, a person can only access the data if the entered user name and password are valid; and second, even if the login password of the user is compromised, the uploaded file is encrypted, and the file can only be decrypted if the user enters the password that they entered during the encryption process. This provides an additional layer of security for the user's data. This guarantees that the information is kept private.

$$y_k(n) = \boldsymbol{\theta}_0^T \mathbf{x}_k(n) + \eta_k(n), 1 \leq k \leq 10 \quad (1)$$

Step 6: Place the file in an Adhoc Network storage location.

The information that is uploaded is encrypted, and the cypher text cannot have any changes made to it. This guarantees that the data is accurate. After the encryption text has been prepared, the encrypted file should be uploaded to the Adhoc Network storage.

Step 7: After the file has been uploaded, inquire with the user about whether or not he wants to remove it.

It has to do with removing the original plain text file from the machine's memory, which is the focus of this issue. After a file has been uploaded to the Adhoc Network, the user is offered the option to remove the file from their local device. The user has the choice to forego this action and instead keep the file in its original state by going with the second available option. We strongly suggest that the original file be discarded in its entirety. Because of this, the plain text file that is saved on the system will not be accessed in an unauthorized manner at any point. If the user chooses the delete option, the system will remove the initial file from the device and delete it from its storage location. Step 8: After ensuring that the cypher text file was successfully transferred to the Adhoc Network and that the user does not have any other files that need to be uploaded, The connection to the Adhoc Network must be severed.

The user's account is logged out automatically by the system, and the previously established connection to the Adhoc Network is severed. The procedures for uploading files are shown diagrammatically in Figure10 :

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

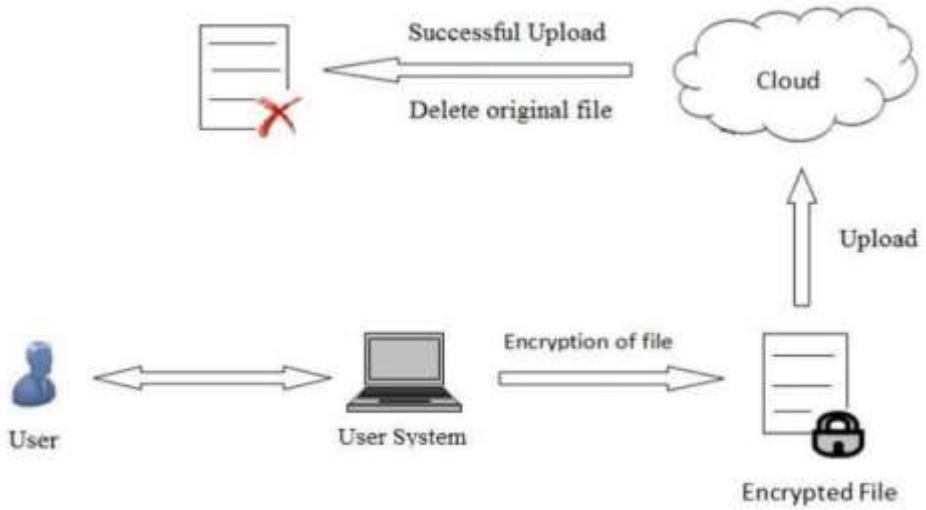

Figure 4: File upload

This section will walk you through the processes involved in the process of downloading a file: Step 1: Request the user's login information and then accept it.

It is the same as the first step in the file upload process. During this stage, the user's identity will be checked and validated.

$$a_{mk} = \begin{cases} \frac{1}{max(n_k, n_m)}, & k \neq m, k, m \text{ are neighbors,} \\ 0, & m \neq k, \\ 1 - \sum_{i \neq k} a_{ik}, & m = k. \end{cases} \quad (2)$$

Step 2: Ask the user to choose the file that they want to download.

The user's whole collection of files that have been stored in the Adhoc Network up to this point is shown. It is up to the user to choose one of the files that are available from the list.

Step 3: Before beginning the decryption process, the user should be prompted to provide a password.

In this part of the process, the user will be prompted to enter the password that he chose to use when he encrypted the file.

4. Determine whether or not this password is still valid.

If the user enters a password it matches the one that was used to encrypt the file, the cypher text file that was uploaded by the user will be decrypted and made available for download. This is the reason why the password is kept while the encryption procedure is being carried out; more specifically, the password that has been saved is used to verify the password that has been submitted. In AES, encrypting and decrypting the data requires the use of the same key.

$$MSD(n) = 10\log_{10}\left(\frac{1}{K}\sum_{k=1}^{K} \|\boldsymbol{\theta}_k(n) - \boldsymbol{\theta}_0\|^2\right) \quad (3)$$

5. Put the decryption into action to decipher the encrypted text that was submitted.

This is only feasible if the same password is put into the key generator function to produce the key. Other than that, it is impossible. Once, the entered password is confirmed, use the password to produce the decryption key using the key generator feature.

Step 6: Save a copy of the file to your local device from the Adhoc Network.

Store the plaintext that has been decrypted in the memory of the user's computer.

Step 7: Ask the user whether he wishes to remove the encrypted file that was uploaded to the server.

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

If the user chooses the delete option and indicates that they do not desire to download any more files from the Adhoc Network, the encrypted file should be removed from the Adhoc Network storage location.

Step 8: Disconnect your device from the Adhoc Network.

Sign out of the user account, and then terminate the connection that is already established with the Adhoc Network. The process of downloading files, which is diagrammatically shown in Figure 4 as:

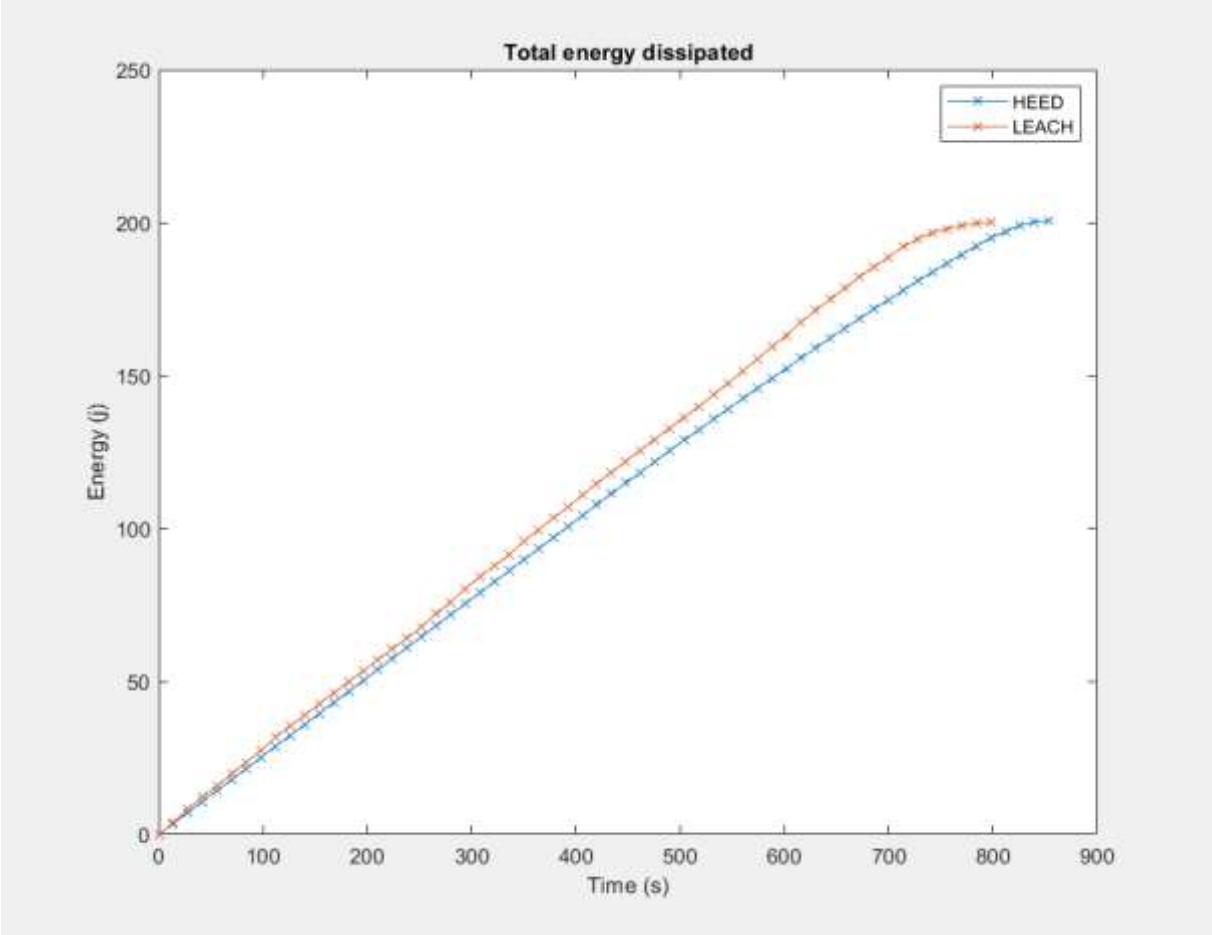

Figure 5: Energy Consumed

4. EXPERIMENTAL RESULTS

The examination of the experimental results was carried out by first generating seven different scenarios. Altering any one or multiple factors, such as region, number of DCs, UBs, VMs, image size of VMs, size of memory, and user request on- and off-peak time, were used to organize the various cases that were tested. In every one of these distinct circumstances, the values of the input parameters were altered. In every instance, we carried out the analysis a total of three times using an identical set of input parameters in order to guarantee the reliability of the findings. To put it another way, exactly the same. The sim file was run three times for the same scenario, and the same case was run several times for each of the algorithms that were being compared (ESCEL, Push-Pull, and DWLM). A more fruitful study of the suggested algorithm was produced as a consequence of this approach, which helped to improve the output.

Implementation Details

The Xilinx Zedboard embedded system board was chosen for the performance evaluation because it features a dual-core ARM Cortex A9 processor and 512 megabytes of random access memory (RAM).

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

The performance of Native Linux on Zedboard is compared with that of L4Linux on the L4Re microkernel running on Zedboard. In this context, "Native Linux" refers to Linux that was built for Zedboard using the Yocto build system, and it is distinguished by the fact that it operates directly on bare metal hardware without the use of virtualization. There are 90 registers in the PMU of the arm cortex A9 processor.

Performance Analysis utilizing the Suggested Method Seven performance counters that are able to be configured to measure particular events. The application was constructed with the help of the cross-compiler known as gcc-linaro-6.31.

Measurements of performance are made with the help of the hardware performance counters that are made available by the PMU. In a typical scenario, you will not be able to access these performance counters from within L4Linux if you are using a virtual environment. The performance measuring tool perf, which is available as part of the Linux kernel, makes use of PMU to obtain the performance results. The specifics of these changes are described in Section 4.2.1. Additional features are implemented in the Fiasco microkernel to avail these counters in a virtual environment. The performance of the virtual environment can be measured with perf on L4Linux, and the performance of the non-virtual environment can be measured with perf on Native Linux.

In this part of the presentation, our primary goal is to discuss the tests that were carried out to investigate the impact of varying levels of load on the performance of the optimal controller. The experiments were carried out with each load being at one of four different levels. The test setup in this section is very similar to the setup that was illustrated in the previous section. We are making use of the setting-1 of the Q and R matrices, in which the values of these matrices are determined by the expressions Q = [2 0; 0 50] and R = 2. K equals [1.9920 0.1423] when it comes to the value of the feedback gain matrix. The results of these experiments are outlined in Table 4.3 below.

The first entry details the results of the test that was conducted in setting 1 in the section before this one. The remaining entries all fall under distinct load categories, such as 85 req/10sec, 69 req/10sec, and 25 req/10sec, respectively. In addition to this, we conducted experiments in which no controller was active in order to determine the optimal cap value for each load level. We plotted the results of each experiment after applying the cost function to the measured values from each experiment. In order to determine whether or not the controller is able to set the cap to the optimal value that is appropriate for each load level, the optimal cap value that was obtained from these cost function curves is put to use.

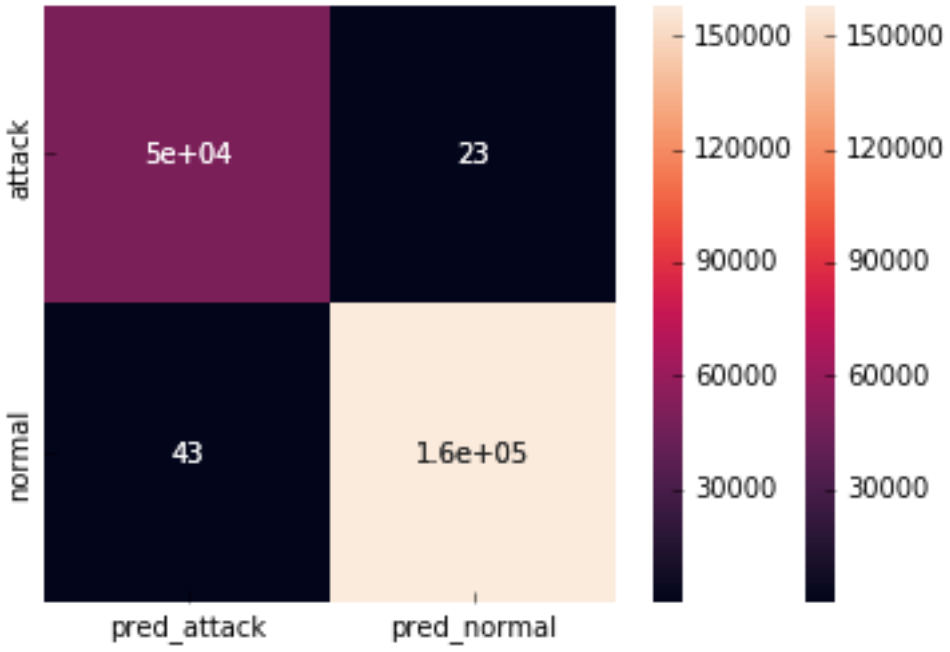

Figure 6: Confusion matrix

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

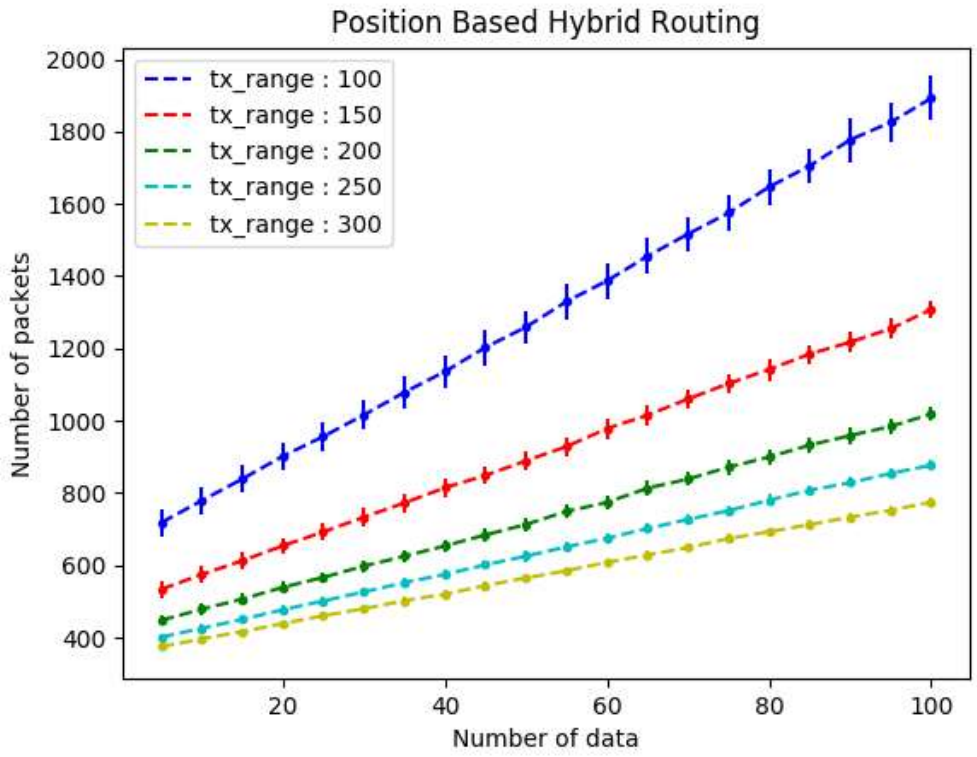

Figure 7: Position-based routing

Both the CM arm and test sum workloads exclusively include CPU calculations and do not include any system call activities. Other workloads, such as test files, block read, char read, and char write, are examples of programs that contain system calls and make use of read/write system calls. As a result, this assists in determining the performance difference that exists between workloads that entail CPU calculations and workloads that involve OS calls. Real-time applications are referred to as h264enc and h264dec respectively. Listed below are more facts about each individual task.

• CoreMark also known as CM arm, is a benchmarking program that measures the performance of the CPU. The sole activity involved in this task is calculation; there are no system calls. Enabling Hardware Performance Counters on a Microkernel-based Routing Protocol.

• test sum is a program that calculates the total of N different integers. This workload solely involves calculations performed by the CPU.

• test fileOp is an example of a program that performs read/write operations on files. It is made up of system calls like read, write, and fprintf, among others.

The 'read' function is used to read the file in 64KB chunks whereas the 'block read' job extracts blocks of characters from an input file.

• ‘read’ function is used by char read, which then reads each character from an input file one at a time. char read100 reads up to 100 characters one at a time from /dev/zero in character-by-character increments. The char read64k function reads up to 64KB worth of characters one at a time from the /dev/zero device.

• The char write function appends data to a file one character at a time. using the 'write' function with the char write100 parameter. Up to 100 characters may be written to /dev/null one at a time by using the char write100 function. char write64k is capable of writing 64KB worth of characters to /dev/null, one character at a time.

• h264enc/h264dec is OpenH264 video encoder/decoder.

When carrying out profiling with the perf tool, three distinct workloads with the names of CM arm, buff read, and char read64k are used. CoreMark is a benchmarking program that measures how well a

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

computer's central processing unit (CPU) functions. The job is known as "buff read" and reads characters from the input file one block at a time. The 'char read64k' command reads each character from an input file one at a time. The CM arm task is unique in that it solely consists of calculations and does not make any system calls. All of the other workloads, on the other hand, do make system calls; hence, this helps to determine the performance gap between CPU- and OS-intensive workloads. Figures 7, 8, and 9 correspondingly show the outcomes of running 'perf report' with the callgraph capability enabled for the various workloads tested on L4Linux and native Linux.

The functions are arranged in the results presented depending on the amount of time it takes to execute each one; the functions shown at the top need the most amount of time to execute. When the callgraph option is activated, it provides information about the caller as well as the callee, and it displays the overhead using the parameters 'Children' and 'Self' to determine who is responsible for what. The 'Self' column displays the amount of overhead that is exclusive to that function, and the total amount of overhead for all of the 'Self' functions adds up to 100%. The functions that are called by the parent functions are shown in the column labeled "Children." The total number of child functions is more than 100% due to the fact that each of them represents the self-overhead of its own offspring. The number reflects the proportion of the total samples gathered in the function that corresponds to it. The 'Command' column identifies the procedure from which the samples are obtained. The privilege level at which samples are collected is shown in the 'Symbols' column of the table. "[.]" denotes user-level symbols, which display the icons that were generated by the user's program. '[k]' signifies kernel level symbol from [kernel. kallsyms]. In the results of the workload profiling performed by L4Linux, the symbols from the guest kernel that are executed in userspace are denoted by the notation '[k]'. The function l4x vcpu entry c is the entry function to L4Linux. This is the point at which the execution of each event, such as an interrupt, a system call, or a page fault, will begin. The functions irq exit, __handle domain, and handle IRQ are among others that are used for interrupt handling.

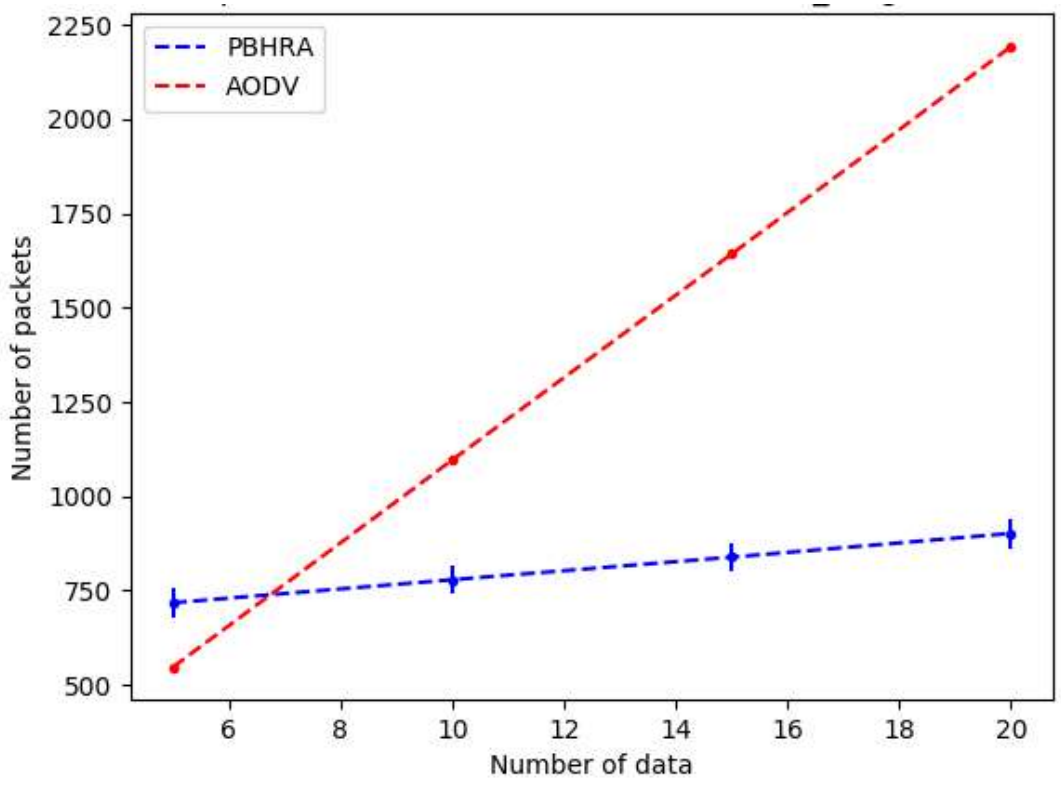

Figure 8: User Uploads comparison

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

The user can download the file by clicking on "Download Data" and then enter a password for the process of decryption. If the password that was entered is invalid, then an error notice should be shown, and the password should be rejected. If the password that was entered is legitimate, then a key should be generated. Get the file by downloading it from the Adhoc Network. The user can erase the encrypted file that was uploaded by choosing the delete option, as seen in Figure 9.

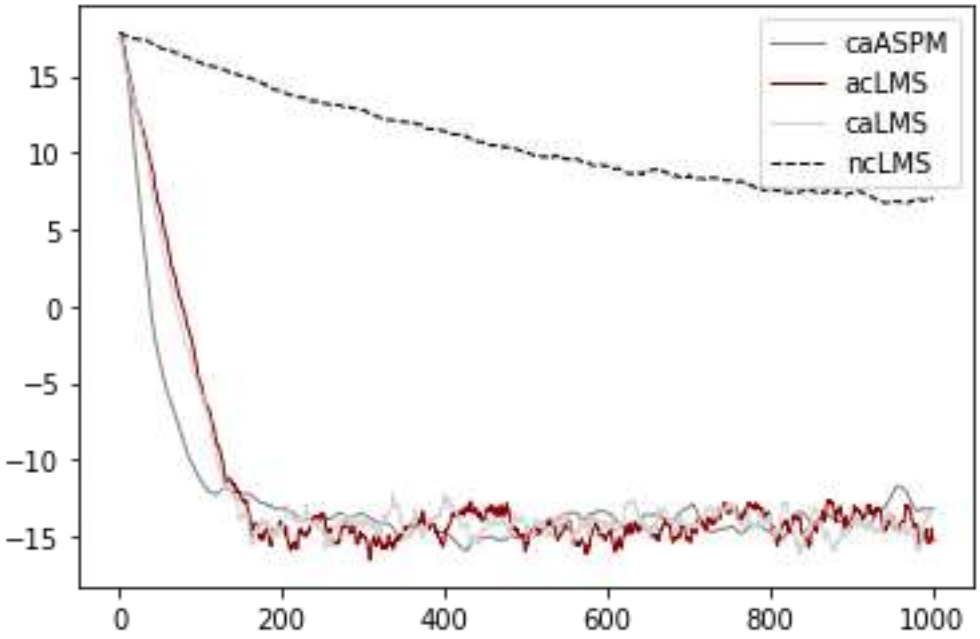

Figure 9: Download File and Decryption

Among the user application samples, the functions core state transition and crcu8 have the highest and second highest overhead, respectively, as shown in Figure 9 and Figure 10 respectively. This can be determined by looking at the overhead of the self-column. The fact that the results obtained from the profiling tool in L4Linux and native Linux are identical demonstrates that the proposed implementation accurately profiles the system it runs on.

The results of executing buff read with the 'perf record' and 'perf report' commands on L4Linux with the proposed implementation and on native Linux respectively. The 'buff read' workload will read a file in sections that are 64 KB in size.

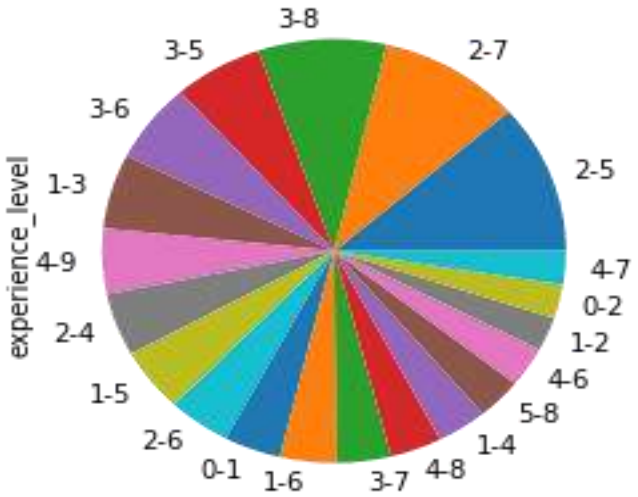

Figure 10: Owner Viewing Confidential File

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

The setting-1 was discussed in the previous section in further detail. We found that the ideal cap value was supposed to be 70-110%, while the average cap value that was set by the controller was 106.47%. Setting 2 now has a load that is 85 req/10sec, which is an increase from the previous setting. Figure 10 graph makes it clear that the value of the cost function is at its lowest in the range of 70-110% cap. This is something that can be deduced from the graph. Figure 10 is a graph that demonstrates the cap values that are established by the controller when the system is subjected to a load of 85 req/10sec. The cap is currently set at an average value of 112.42% by the controller. At the third configuration level, the demand on the program is decreased to 65 req/10sec

7. Conclusion

Our efforts began with a study of one of the most important issues in the context of the execution performance of apps that were operating inside the Routing Protocol Hosts. We identified a difficulty with performance isolation as well as unexpected performance, both of which are addressed in the literature on Routing Protocols. The performance of each application that is hosted in a distinct Routing Protocol is significantly impacted as a result of the partition of resources among various Routing Protocols, as was shown by a number of assessment studies. In this particular setting, we identified two distinct categories of issues that need to be resolved:
• in finding resource allotment for each Routing Protocol in such a way that application execution performance is maximized at a minimal cost. • in finding resource allotment for each Routing Protocol in such a way that each application gets its guaranteed quality of service.

It needs to be clarified, and it is a fixed connection, that the amount of resource shared in a Routing Protocol has corresponded in any way to the performance with which an application is executed. Because the virtualized environment has a number of different sources of dynamics, the difficulty of the issue is increased. As a result of this, we came to the realization that it is necessary to compute the resource shares of the Routing Protocols in a dynamic manner.

Feedback control has found widespread application in the continuous monitoring and tuning of system parameters in a variety of electrical and mechanical systems, including those used to control aircraft, thermostats, and many others. The use of feedback control as a means to optimize the parameters of computer systems has been the subject of a significant amount of study as of late. We concluded that the feedback control would be useful for solving our issue. As a result, we suggested making use of a self-tuning technique so that dynamic resource allocations could be adjusted for specific Routing Protocols. The most innovative aspect of our work is the analysis, design, and implementation of an optimal control mechanism for dynamically tuning the CPU share of a Routing Protocol. This ensures that the application performance is optimized while the associated costs are kept to a minimum. In order to determine whether or not feedback control has any practical applications, we began by developing a straightforward feedback control system. This system computes CPU shares in such a way that every application operating within a distinct Routing Protocol receives the desired quality of service.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Abhishek et al. (2012)," Adhoc Network Data Security while using Third Party", International Journal of Scientific & Engineering Research, Vol. 3.
[2] Adnan, M.A. Razzaque (2013)," A comparative study of particle swarm optimization and Cuckoo search techniques through problem – specific distance function", International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia.
[3] Akanksha, (2014)," Encryption of text characters using ASCII values", International Journal of Engineering Research & Technology, Vol.02 (3), pp.232-235.
[4] Ali et al. (2016)," Security and Privacy of Sensitive Data in Adhoc Network Computing: A Survey of Recent Developments", David C. Wyld et al. (Eds): NETCOM, NCS, WiMoNe, CSEIT, pp. 131–150.
[5] Al-Saffar (2015)," Identity Based Approach for Adhoc Network Data Integrity in Multi-Adhoc Network Environment", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, pp.505-509.

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022

[6] Anuja.S.Joshi et al. (2017),” Cuckoo Search Optimization- a Review”, International Conference on Advancements in Aeromechanical Materials for Manufacturing, pp.7261-7269.
[7] Arasu, S. et al.((2013), “Privacy-Preserving Public Auditing In Adhoc Network Using HMAC Algorithm.”, International Journal of Recent Technology and Engineering, Vol.2,pp.149-159.
[8] Ardagna et al (2015),” From security to assurance in the 143 Adhoc Network: A survey” ACM Computational Survey, Vol 48-1, pp 1- 50.
[9] Arjuna et al. (2016),” Adhoc Network Data Security with Modified RSA Algorithm”, International Journal of Engineering Research & Technology, Vol.5 (5), pp.205-208.
[10] Arora et al. (2012),” Adhoc Network Computing Security Issues in Infrastructure as a Service”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 1, ISSN: 2277 128X.
[11] Bachhav et al.(2015),” Secure Multi-Adhoc Network data sharing using Key Aggregate Cryptosystem for scalable data sharing”, International Journal of Computer Science and Information Technologies, Vol. 6 (5), pp.4479-4482.
[12] Bahrami M, Singhal M (2015),”The role of Adhoc Network computing architecture in big data”, Information Granularity, Big Data, and Computational Intelligence, Cham, Switzerland: Springer International Publishing, pp.275-295.
[13] Bhagat, Sahu (2013),” Adhoc Network Data Security while using Third Party Auditor”, International Journal of Computer Applications, Vol. 70– No.16, pp.9-14.
[14] Behl A (2012),” An analysis of Adhoc Network computing security issues”, World Congress on Information and Communication Technologies (WICT).
[15] Bryan F., et al (2017),” Expanded 128-bit Data Encryption Standard”, International Journal of Computer Science and Mobile Computing, Vol. 6, Issue. 8, pp. 133 – 142.
[16] C. Cachin, I. Keidar, and A. Shraer, “Trusting the Adhoc Network,” SIGACT News, vol. 40, no. 2, pp. 81–86, 2009.
[17] Charmee V. Desai (2014),” Survey on Data Integrity Checking Techniques in Adhoc Network Data Storage”, International 144 Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4,pp.292-295.
[18] Chatterjee et al., (2012),” Symmetric key Cryptography using two-way updated -Generalized Vernam Cipher method: TTSJA algorithm”, International Journal of computer applications, Vol.42, pp.39- 42.
[19] Chen (2012),”Data security and privacy protection issues in Adhoc Network computing”, International Conference on computer science and Electronics Engineering.
[20] Chin-Ming Hsu (2003),” A group digital signature technique for authentication “, Proceedings of IEEE 37th Annual 2003 International Conference.
[21] Chiroma et al (2017),” Bio-inspired computation: Recent development on the modifications of the cuckoo search algorithm”, Applied Soft Computing, Vol. 61, pp.149–173.
[22] Civicioglu ,Besdok (2011),” A conceptual comparison of the Cuckoo-search, particle swarm optimization, differential evolution and artificial bee colony algorithms”, Journal of Artificial Intelligence Review,Vol 39,pp 315–346.
[23] Cong Wang et al. (2013),” Privacy Preserving Public Auditing for Secure Adhoc Network Storage”, Computers, IEEE Transactions, Vol. 62(2), pp.362–375.
[24] Dinh HT, Lee C, Niyato D, Wang P (2013),” A survey of mobile Adhoc Network computing: architecture, applications, and approaches”, Wireless Communication Mobile Computing, Vol.13 (18) pp.1587-1611.
[25] Geeta, Varma, (2016)” Cuckoo Search Optimization and its Applications: A Review”, International Journal of Advanced Research in Computer and Communication EngineeringVol.5 (11), pp.556-562. 145.
[26] Gohil, G. B., Pathak, R.K. and Patel, A. A., (2013) "Security in Computing", International Journal of Computer Science and Mobile Computing, Vol- 2, Issue-3, pg.52 – 56.
[27] Goyal and sidhu (2014),” Third Party Auditor: An Integrity Checking Technique for Client Data Security in Adhoc Network Computing”, International Journal of Computer Science and Information Technologies, Vol. 5(3), pp.4526-4530.
[28] Grundy J., Almorsy, M. and Ibrahim, A. S., (2011) "Collaboration-Based Adhoc Network Computing Security Management Framework", 4th International Conference on Adhoc Network Computing, IEEE, pp. 364- 371.
[29] Hao (2011),” A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability”, IEEE Transactions On Knowledge and Data Engineering, Vol. 23 (9), pp. 1432 – 1437.
[30] Haw et al.(2019),” Implementation of RSA Algorithm to Secure Data in Adhoc Network Computing”, International Journal of Innovative Science, Engineering & Technology, Vol. 6 (4),pp.61-68.

Doi: https://doi.org/10.54216/IJWAC.050203
Received: March 28, 2022 Accepted: November 25, 2022