Software Defined Network Function Virtualization Framework for Securing Cloud with Data Fusion and Machine Learning Techniques

Rajit Nair [1], Miguel Botto-Tobar[2], Premnarayan Arya[3]

[1]VIT Bhopal University, Bhopal, India
[2]Research Group in Artificial Intelligence and Information Technology, University of Guayaquil, Ecuador
[3] Department of Computer science and engineering,G.H. Raisoni Institute of Engineering and Business Management, Jalgaon, Maharashtra, India

Emails: rajit.nair@vitbhopal.ac.in; miguel.bottot@ug.edu.ec; premnarayan.arya@raisoni.net

Abstract

Computing in the cloud is one of the platforms that may be used to provide distributed computing resources. Supplying and managing cloud resources most effectively is referred to as resource management. A recent development in technology known as fog computing is an example of an expanded and dispersed infrastructure. This architecture maintains application processes between end devices and the network edge to provide more dependable and efficient services. These services include remote data storage, allowing customers to access their data from a distant location. Providing remote storage service is an advantageous function offered by cloud suppliers. On the other hand, the data stored in the cloud is geographically dispersed and kept in various data centers, significantly increasing the risk to users' privacy and security. One of the problems that might arise with privacy is when many data centers store the same information. Many cloud service providers check their customers' data using a Third-Party Auditor (TPA) to address concerns about client privacy and data integrity. Currently, most trusted TPAs only have one validator, making it impossible to expand the data integrity across several data centers. The various verifiers used by TPAs have been reduced in number in response to Man in the Cloud (MiTC) attacks. As a result, they cannot check and authenticate the integrity of data stored in several data centers. A unique Peer to Peer (P2P) authentication protocol with Certificate Authority (CA) and Data Storage Protocol is presented as a solution to the problem that has been outlined above to check for and go around any issues that may arise (DSP). The efficiency of the proposed protocol is demonstrated by the incorporation of TPAs and Certificate Authorities. The proposed protocol has been tested with a single user and a single storage server, as well as multiple storage servers in ownCloud with one backup server, two storage servers, three clients, and two TPAs. The NoSQL server in an organization's cloud is set up to save data to storage servers in the appropriate format. The Amanda backup server is used to back up the mirror copy of the stored data on the storage servers. Automated Validation of Internet Security Protocols with Data Fusion and Applications, or AVISPA for short, is a technology that may be used to verify data stored in the cloud. The findings make it abundantly evident that the suggested protocol is strong enough to guarantee the authenticity of data kept in several data centers.

Keywords: Third Party Auditor (TPA); multiple data centers.; attacks; Certificate Authority and TPA; Peer to Peer; data fusion.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

1. Introduction

The scope of the Internet is impressive beyond measure. The introduction of agility, simplicity of deployment, hosting, and maintenance of corporate applications were only some of the ways that cloud computing disrupted the IT operations and ICT organizations of all enterprises. It significantly reduced growth, operation, and capital investment expenditures, among other costs [1]. However, as more devices and computers were linked to one another, and the expansion of digital services led to significant network congestion, over-provisioning, and routing complexity, end-users encountered more excellent delays for time-sensitive applications. Cloud service providers cannot provide an end-user experience that is suitable in terms of immediacy, mobility, location, and context awareness of their services.

The development and administration of infrastructure and services in traditional networks is a dynamic process that requires the change of numerous different network defaults. This modification is often accomplished via the use of proprietary interfaces. Complex and Decentralised protocols such as OSPF[1, BGP, and EGP[2] are responsible for managing the process of a packet being sent from one location to another. Implementing complicated rules in typical IP networking infrastructures is challenging due to the absence of a standardized description of the global network state and suitable network abstractions. Furthermore, because the network is planned rather than coded, deploying new services is much more complicated and time-consuming [3, 4].

By removing control information from forwarding devices like switches and routers, "Software-Defined Networking" (SDN) represents a paradigm change and clean-slate design in the networking industry [5, 6]. SDN has been a massive game-changer in the administration of large-scale networks since it detached the control function from the devices used to transfer traffic (i.e., switches and routers). Before the advent of software-defined networking (SDN), every button ran its control plane software, which the switch manufacturer supplied. This program carried out several distributed algorithms to ascertain the topology of the network and the regulations governing its forwarding (e.g., the spanning tree protocol [7]).

This strategy had several drawbacks; the first was that the distributed control plane was more challenging to implement and needed compatibility from various suppliers that did not always agree. Second, since network administrators were required to adhere to the vendor's list of supported capabilities, the modification and innovation process was tricky. Third, for all of the components to operate in harmony with one another, it was necessary to establish a solid connection with a particular supplier. This meant there was a high cost of ownership for the equipment, and network managers were forced to undergo pricey training and certification to utilize the equipment appropriately. Nevertheless, SDN has made significant steps in solving several fundamental difficulties of the data plane forwarding devices, such as the lack of flexibility, programmability, dynamic policies, upgrades, and innovation. SDN has also tried solving obstacles that arise in multi-tenant data centers.

As a result, it made the market more accessible to new sellers and cut the obstacles to the entrance. In addition, the provision of network services and the enforcement of rules in a dynamic manner, which is manual in conventional networks and requires a significant amount of time and resources, become a comparatively controllable (programmable) autonomic job when SDN is enabled. As a result, SDN has made considerable headway in the business world and the academic community, and it has been used in both data centers and wide area networks (WANs) [8, 9].

Academic institutions are researching SDN extensively, while businesses and network operators are examining its potential. Some of the most successful corporations with scattered content and IT, such as Google Inc., are using SDN-based WAN to join their data centers in different parts of the world through an internal backbone network. Because of this, the network's performance was greatly enhanced, and the utilization of the connections rose from 30 to 40 percent to about 100 percent [10]. This remarkable accomplishment was made possible by SDN, which enabled greater control of network transmissions and the programming of network flows.

The expansion of software-defined networking (SDN) is anticipated to continue in the years to come, as seen by the expanding backing provided by key networking suppliers like Cisco [10], Huawei [11], Juniper [12], and Hewlett Packard [13]. SDN has also found use in current virtualized data centers and Internet of Things-based smart infrastructures [14], and it is expected that it will be the critical enabling technology for the applications of 5G networking [15]. Furthermore, the completely different approach that SDN network administration and configuration takes has essential consequences for network security.

These implications may be broken down into three categories: Despite its many benefits and high level of complexity, the new networking architecture presents several issues that put the environment in which it is implemented at risk. These challenges jeopardize its security, management, and resilience. The safety afforded to

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

the software-defined network deployment is denoted by the phrase "Security of SDN," which refers to the tenacity and fortitude of software-defined networking (SDN). The central control plane of an SDN architecture is one of its inherent design flaws, which may make it vulnerable to having a single point of failure. The research communities in academia and industry have explored the many attack vectors and vulnerabilities present in deployed settings, which has helped advance the argument for SDN. Finally, SDN's logically consolidated perspective and programmability simplify the development and execution of network-wide security regulations. This aspect of security is referred to as "Security by SDN."

Using software-defined networking (SDN), which gives operators the capacity to operate a network from a logically centralized place, we describe novel approaches for increasing security in front-line networks. To do this, we begin by reevaluating the corporate SDN deployment strategy. After that, we integrate SDN into industrial environments while providing cloud computing support. Our research findings demonstrate how SDN-based security solutions may be adapted to address deployment issues while considering each network's particular qualities and constraints. This thesis tackles difficulties present in today's front-line networks and, without our SDN solutions, would otherwise stay unsolved. As a result of this, the problems are handled.

First, we look at how rethinking the implementation of SDN in the organization might help solve current issues with scalability and situational awareness. Because of the intricacy of the network, scalability and situational awareness become complex challenges. Because of this intricacy, there are occasions in which operators cannot see traffic on the web, making it challenging to have a comprehensive and global picture of the network. If network operators had a greater awareness of the network activity coming from end systems, they would be better able to prevent hazards such as the propagation of malware from a system that has been hacked. Since hosts immediately route the data without transiting security enforcement and monitoring devices, network operators in conventional methods are often unaware of the intra-subnet activity.

This is because old systems do not utilize host-based intrusion detection systems. In the case of a malware outbreak, containment strategies call for turning down essential network services and maybe even disconnecting the whole network to stop the infection from spreading [16]. In the SDN paradigm, owing to the global perspective, it is possible to identify and thwart DDoS assaults in the early phases of their development. SDN architecture is more suitable for deploying ML algorithms than implementing NIDS in the conventional network model. The switches provide the statistics to the coprocessors.

This helps to solve the problems of network intrusion and the detection of sophisticated attacks. To enforce rules on these flows and do ML-based analytics on the flow data, the centralized controller in the data center makes an interface available to apps in the form of a "northbound API." ML-based systems may mine a massive amount of time series data to derive insights, which can then identify network intrusions and anticipate future network assaults [17]. The dataset and the process of training the machine with labeled data are the core factors that determine the efficiency and practical feasibility of any ML-based NIDS. As technology advanced, it brought multi-core and hardware-accelerated CPUs (such as scalable Intel Xeon and Phi) and many-core coprocessors (such as GPGPUs and Tensor units). This opened up the platform for ML-based analytics and deep computational networks [18][19].

Consequently, the controller-based system offers an environment well suited for deploying machine learning algorithms for anomaly and intrusion detection. In addition, based on historical and real-time data analytics, SDN provides the programmable model via API, automating provisioning, services chaining, dynamic security choices, and traffic rules at run time [20]. This model can automate provisioning, service chaining, vibrant security choices, and traffic rules. Because SDN is built on top of both of these technologies, this is feasible. We discovered that the existing machine learning (ML)-based classifiers improve the accuracy of intrusion detection systems (IDS). However, they do so at the price of increasing processing power and memory needs, which renders them unsuitable for use in real-time applications. Consequently, by conducting this research, we could address some of the most urgent issues about NIDS in SDN systems.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

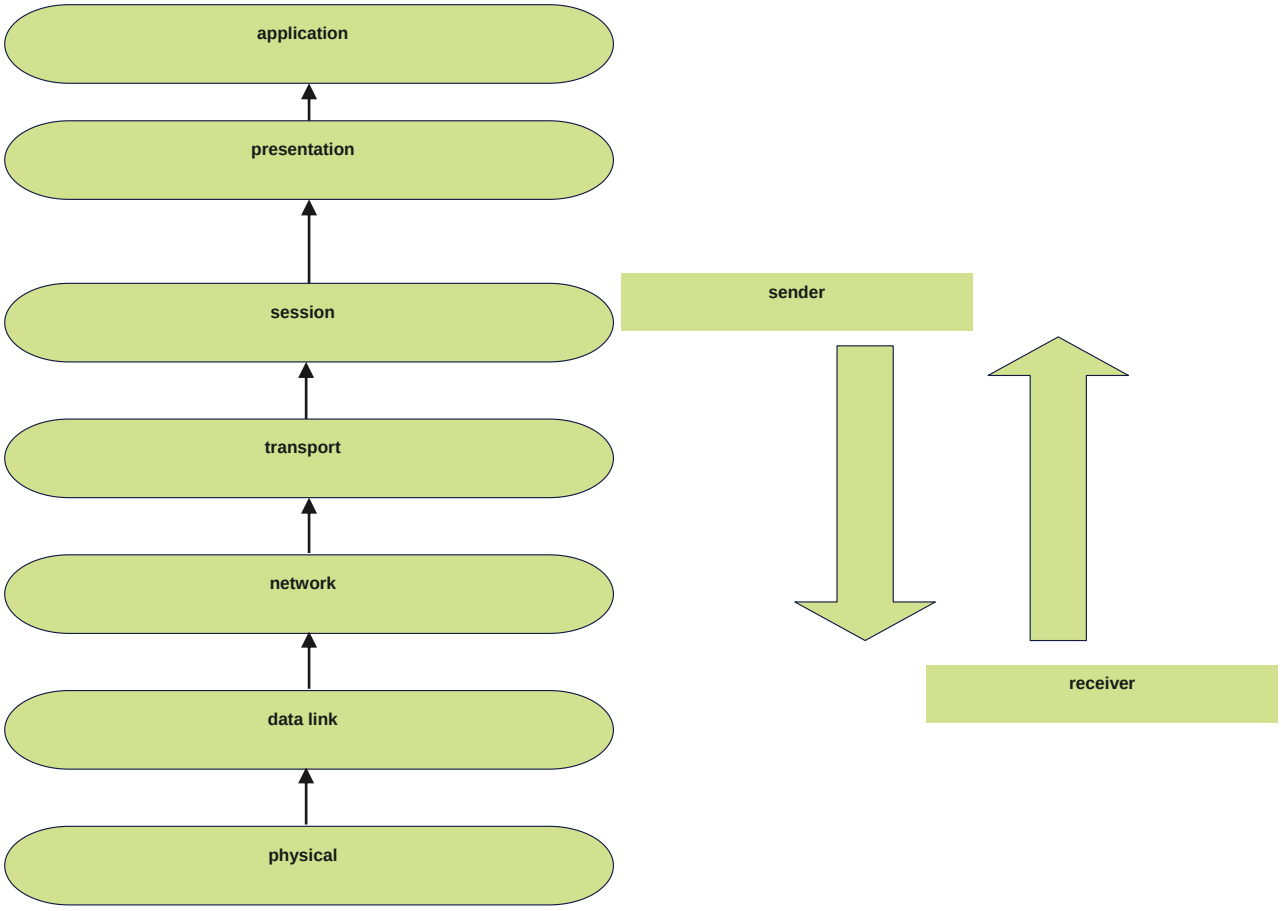

Figure 1: General layers in Wireless Network

Recently, there has been a rise in the number of cyberattacks that are automated and carried out by groups of cybercriminals. The attackers have the necessary capabilities to compromise any infrastructure. Present-day attackers employ numerous tactics to take off their target, comprising seven kill chain steps. This often starts with a reconnaissance phase, during which information is acquired, and possible target systems are identified. The techniques they use will determine how long this phase lasts. After that, the computer network will be scanned, depending on the nature of the engagement, either externally, internally, or both, to conduct a more in-depth examination of it and locate any known vulnerabilities. If vulnerabilities are discovered, there is a possibility that an effort may be made to exploit them, and eventually, access may be achieved. In addition, a hacker could potentially try to get into systems that do not have a known vulnerability but are merely open to the internet. The lack of concern for data safety was not the driving force for the first move to the cloud. However, this has the potential to become an essential driver of development for enterprises that use distributed computing. Because of this, we were inspired to create a robust security architecture to safeguard the storage units housed in the cloud environment.

• To design an innovative authentication system for users to use with one another to protect cloud storage

• To provide a robust security framework for cloud and fog storage that utilizes attribute-based encryption as well as multi-factor authentication

• To design a bio-inspired computer system using the cuckoo search algorithm to provide an effective and reliable security framework.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

The primary emphasis of this research is the development of comprehensive security frameworks and protocols to offer an additional layer of protection to cloud storage. In this setting, this dissertation provides a unique security framework. In this dissertation, there is also a discussion of a unique approach that has been developed to protect fog-end devices. In addition, the management of cloud resources is performed with the help of a robust Cuckoo search algorithm. The following is a model of the stated scope of this thesis: to safeguard the data storage by imparting a cryptographic algorithm; to guarantee the reliability and resilience of the storage devices, to design a practical framework for fog devices; to plan the allocation of resources correctly.

This research work focuses primarily on Cloud data management mechanisms for an innovative Peer-to-Peer protocol with Certificate Authority (CA), Ciphertext–Policy Attribute-Based Encryption Scheme and Multi-factor Authentication (CP-ABE-MA), and Cuckoo Search Algorithm (CSA). This protocol is proposed and implemented to supplement the existing security countermeasures. The Signal protocol used by the Open Whisper system served as the basis for constructing the P2P protocol. The P2P protocol encrypts data using an authentication key generated by AES256 operating in Code Block Chaining mode and authenticates users with HMAC - SHA256. Recreating the data from the session using the Authentication key is impossible, which is needed to verify the data's authenticity. The clients are guarded by a File key produced via a Sobole sequence and are subject to changeability if the cloud storage server changes. The purpose of the integrity validation phase of the P2P protocol is to verify the verification phase of the Signal protocol, which includes two primary phases: i) key distribution and verification and ii) validation of the protocol's integrity. In the P2P protocol, TPAs are the ones to produce authentication keys and then distribute them to CA so that they may check the data's integrity. The TPA examines the data's integrity while verifying the CA's return findings in this step. TPA uses the client file key once again to confirm the client's file's authenticity.

2 Related Work

The concept of cloud computing can be separated into three service models, each of which is determined by the different types of services provided by the cloud. (a) Software as a Service, also called SaaS, is a model for distributing software in which applications are hosted by a vendor or service provider and made accessible to customers through a network, most commonly the internet. This model is also called "cloud computing" [21].

SaaS is becoming increasingly widespread for distributing software as underlying technologies that allow web services and service-oriented architecture (SOA) continue to expand, as well as new ways of software development that have emerged, such as Ajax. Software as a service, often known as SaaS, is a software delivery paradigm strongly tied to the application service provider (ASP) model and the on-demand computing model. IDC recognizes two delivery techniques for software as a service that are very different from one another (SaaS). The hosted application management (hosted AM) paradigm is comparable to the application service provider (ASP) model because a provider hosts commercially available software for customers and distributes it via the internet. In the paradigm of software accessible on demand, the service provider allows their customers access over a network to a single copy of an application designed specifically for distribution through SaaS. This access is granted to the client through the application [22].

This allows the client to design and test new apps in addition to running the applications they already have. Software as a Service, often known as SaaS, is a paradigm for distributing software in which users can access hosted software applications via the internet. Platform as a Service, called PaaS, is a spinoff of software as a service (SaaS) designed to compete with SaaS. PaaS gives developers various chances and advantages in a single package [23]. PaaS enables users to alter and update various operating system properties regularly. This capability was not before available. During software development projects, it is feasible for teams of developers located in different geographic locations to collaborate. Getting services from diverse sources outside a single country's boundaries is possible. Using infrastructure services from a single vendor instead of maintaining various hardware facilities that frequently perform redundant duties or suffer from incompatibility issues may reduce the initial and ongoing expenditures associated with the business operation. This is because using infrastructure services from a single vendor is more efficient than maintaining various hardware facilities. Another strategy for cutting expenses and lowering total expenditures is consolidating operations related to programming production. (c) Infrastructure as a Service (IaaS) The customer is provided with the opportunity to utilize processing, storage, networks, and any software that they choose to run on the cloud infrastructure together with the operating system that they want to use. This option is known as "infrastructure as a service." However, the user controls networking components such as the host firewall, storage, operating systems, and installed applications. The client does not have control over the infrastructure that the cloud is built on top of [24]. An organization can "outsource" the hardware and software necessary to support its operations using a service delivery method known as "Infrastructure as a Service," or IaaS.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

[25] in Graphic Password, Authentication is a safe authentication method utilizing graphical passwords presented in this study to upgrade conventional authentication mechanisms and let users securely access cloud services.

Shoulder surfing is an assault that may be used to break it. The suggested 3D Password [26] is a combination and sequence of several user interactions inside a 3D environment.

[27] in their paper entitled "protected biometric authentication," investigated the authentication that Das first developed. They stated that Das's technique was vulnerable to various assaults and suggested a modification. A. His article "Biometric Authentication" suggests an upgrade that would solve the security issues caused by DOS and Server Spoofing. The method was shown to be more secure and efficient after security assessments, and performance tests were conducted. The fact that different devices and infrastructures are required is a significant obstacle.

[28] developed a cloud-based RFID authentication strategy in their work on RFID-based authentication. This technique allows readers to access the cloud anonymously via wired or wireless VPN connections. An encrypted hash table is used so the cloud cannot access the client's secrets, including readers and tags. It is envisaged that the first RFID authentication mechanism will be implemented to protect the privacy of RFID readers and tags from an untrusted database keeper. [29] in their paper, Eid Authentication presented a solution to this problem for cloud applications by using the STORK framework to secure cloud authentication using eidos. This would narrow the gap that now exists. The STORK framework is designed to enable various national Eid solutions and will be the Eid framework of choice across Europe shortly. Table 1 reviews the constraints of the various known techniques for authenticating users using passwords.

The deployment of computer resources almost exclusively via cloud computing has become the standard owing to the flexibility and dependability of this model. Based on a case study, an effort is made to investigate the concept of security monitoring and tracking particular user needs. As a result, several security technologies that are realistically relevant for handling the requirements are uncovered, and selection criteria are developed to choose the most effective solutions.

An analysis of the tools and a rating of those tools is provided below, with priority given to those tools that best satisfy the case study's specific needs. The work presented here extends the concept of cloud security monitoring and offers a logical and practical approach to problem-solving a security-related issue [30].

3 **Proposed Work**

Computing in the cloud is quickly becoming the primary differentiator between success and failure for businesses of all sizes. It offers a virtual environment for development, storage, and networking, along with the ability to dynamically allocate and reallocate resources as necessary. It meets the user's requirements for on-demand services. It makes the concept of sharable resources "as a service" easier to implement. The cloud provides businesses with data centers, allowing them to transport their data worldwide. Cloud computing does away with the need for local nodes to be responsible for the upkeep of their data, and it also allows for the personalization of web-based services. Cloud service providers are responsible for the computer resources and data that are managed automatically via the software. When information is created at a quick pace and publicly shared via new and agile collaboration channels, however, we are no longer able to exercise control over the news. Hence The safety of one's data has emerged as a primary worry. It has been mentioned that concerns regarding data safety are the primary factors for cloud computing.

The following are some categories that may describe the many security problems that exist in a cloud computing environment: 1.

1. The safeguarding of information on the part of the service provider
2. Data safety when stored on a server or in a cloud data center (CDC).
3. SQL injection attacks are one of the most critical problems when dealing with software as a service (SaaS). An attacker uses a technique known as a SQL injection attack to accomplish their goal of introducing malicious code alongside the usual SQL codes. Attackers can get knowledge of sensitive information from protected databases using this method. This is a significant worry about the cloud storage provided by CSUs that cannot be trusted.
4. Cross Site Scripting, often known as XSS, is still another significant kind of assault. The adversary inserts harmful scripts into the website's content in this attack. If any user clicks on them, the

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

sensitive information will be instantly sent to the computer used by the attacker. In the realm of cloud computing, this is something that may occur if an adversary were to compromise the cloud service interface. Cloud applications should demand web interfaces for the services they provide.

5. Attacks on the Domain Name Service (DNS) led to the secure web pages being redirected to non-trusted users in a situation where any fast domain might turn to any of those CSUs.

6. Attackers are also known to hijack sensitive information from any secure domain by taking advantage of the time lag required to reuse any IP address. As a result of the fact that cloud domain addresses are constantly being updated for every CSU, this exploit engages in harmful operations inside cloud storage.

7. In Denial-of-Service assaults, also known as DoS attacks, the attackers make many requests, which results in the actual service being inaccessible to the users who can be trusted. For example, you might temporarily or permanently stop or suspend the services of a host that is linked to the internet.

In a Distributed Denial of Service or DDoS assault, the destination server is flooded with many packets that the target server cannot process. This is done to prevent the vital services operating on the server from being interrupted. A distributed denial of service, sometimes known as a DDoS, is an assault in which the attack source is not just one, but more than one, and frequently thousands of, individual IP addresses. The safety of users' data is essential to a service's overall quality. The information has to have security for safe data storage and access.

1.1 Proposed Work

When thinking about the safety of cloud data, the primary focus should be on protecting data when it is resting in the cloud. 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 cloud computing has grown owing to the versatility and broad network access that is provided by it. On the other hand, dependability is essential in offering a setting that is free from danger and safe for the user's personal information and data.

The Advanced Encryption Standard (AES) is used throughout this work and is encrypted before uploading sensitive information to the cloud. Instead of storing the original data, the cloud database stores the encrypted data that has been held there.

The computer's memory is cleared of the original data. The data will be encrypted and made accessible to the user after requesting to utilize it. 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 immediately visible in the user interface. When this occurs, it means that new features have been submitted. 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 cloud 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 customers provide is not stored in a single place or on a single piece of equipment; instead, it is stored in several reliable nodes spread out over the network. This is done to ensure that client's needs may be satisfied no matter where those customers may be situated. This program allows many users to swiftly and concurrently access its features from various places. It also makes it possible for this access to take place at the same time.

(1) The fusing of the degree signal. Through the use of signal-based fusion, signals coming from a variety of sensors are fused in order to generate a new signal that has a high signal-to-noise ratio.
(2) The merging of individual pixels. The fusion of images based on pixels is accomplished one pixel at a time. This results in the generation of a fused image that contains data from a group of pixels in source photos. This helps to improve picture management activities such as segmentation in order to boost the output of each individual pixel.
(3) A functional level equivalent to fusion. The extraction of feature-level items that are recognised across many data sources is an integral part of functional fusion. The extraction of notable properties, which may include pixel size, edges, or textures, based on the surrounding environment. The input frames are merged together to provide these same properties.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

(4) In order to achieve fusion on a decision level, it is necessary to integrate the results produced by a number of different algorithms before arriving at a final choice that is fused at a higher level of abstraction. The information included in each input photo is extracted using its own unique processing. After the information has been gathered, it is then coupled with decision laws in an effort to enhance commonly used definitions.

3.1.1 Algorithm based on the AES Fusion

The fusion hypothesis builds a fusion judgement by incorporating masses of evidence from n different categories of proof. The discernment framework for the fusion problem that is now being considered by n'exclusive and exhaustive hypothesis must be the number of evidence sources equal to n2, with the stipulation that "all is" All of the subsets of è t are collectively referred to as è tione, and each one is given the designation 2 è tione. In Shafer's approach [11], the basic belief assignment (bba) is represented by a function m that ranges from 2 to, with power ranging from one to [0,1].

$$m(\phi) = 0 \text{ and } \sum_{A \subset z'} m(A) = 1 \quad (1)$$

$$m(\phi) = 0 \quad (2)$$

Multiple distinct AES fusion systems make use of a distributed intrusion detection system (IDS) in order to monitor and analyse incoming network traffic. While monitoring incoming network data, the AES fusion will sound the alert if it detects anything that may indicate an attack. It is possible to give either positive alerts or negative cautions. Alarms that prevent an invasion or assault are known as positive notifications, whereas notifications that warn of an invasion or attack are known as negative notifications. Warnings about AES fusion are being played up to attract widespread attention. The Jesang formula is what is used in order to make the transformation from alert to mass [5]. If we find out that the assault only happens with H and that it does not occur with -H, then we have, in line with the hypothesis, that the attack only occurs with H [5],

$$m(H) = \frac{P}{P+N+C} \quad (3)$$

$$m(-H) = \frac{N}{P+N+C} \quad (4)$$

$$m(H \text{ or } -H) = \frac{C}{P+N+C} \quad (5)$$

The Advanced Encryption Standard (AES) encryption algorithm is a symmetric technique. It is recommended that the length of plaintext be 128 bits, whereas the critical size 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 size of the key.

Table 1: Relationship of Nr times and critical length

Key length	128	192	256
Nr times	10	12	14

1. The 128-bit plaintext input is broken up into 16 bytes, 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 plaintext block present in each wheel transform step.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

3. Initial plaintexts block M consists of the following: s00 s01 s02 s03 s10 s11 s13 s20 s21 s12 s23 s30 s31 s13 s33
4. The following are the stages involved in AES encryption:

We played a secret key plus operator game 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.

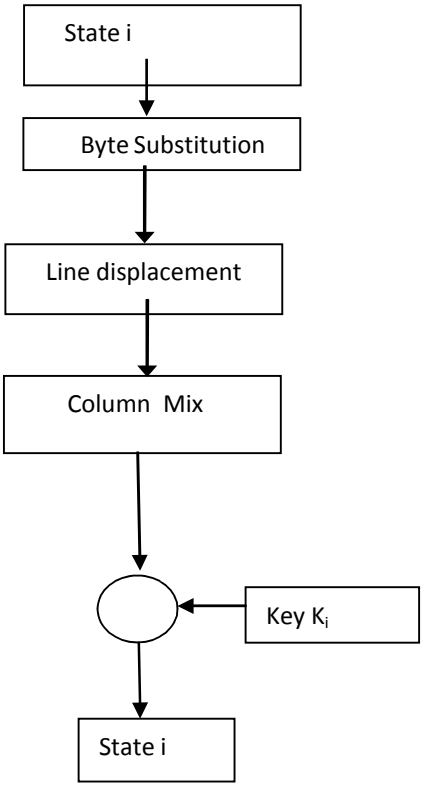

Figure 2: Encryption process

3.1 The design of a cloud storage system with AES algorithm with Data Fusion

The purpose of this system is the development of secure cloud storage services.

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

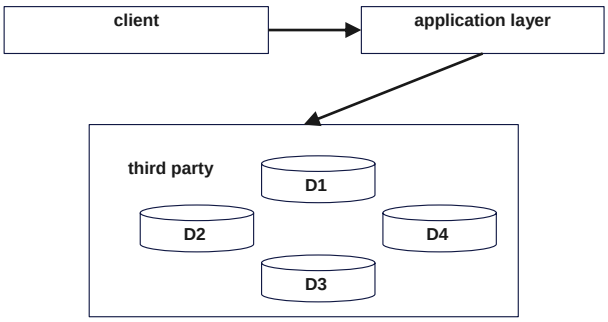

Figure 3: Cloud Storage System

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

Algorithm of Fusion AES

1. Implementation of the Advanced Encryption Standard based Data Fusion
2. In the modules that handled file uploading and downloading, encryption and decryption were employed, respectively.
3. The process of encryption
4. A byte transformation is defined by the AES as an S-box matrix 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 using the row displacement operator.
6. AES used a constant polynomial for the column mixed, simplifying the calculation. 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).

The process of decryption
1. Inverse byte substitution: This technique, quite similar to the byte substitution technique, searches each byte through the table.
2. Inverse row displacement: This procedure 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 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.
A connection should be established with the cloud if the user has been authenticated. In such cases, display the authentication error.
2. Instruct the user to choose an upload file before sending it to the cloud.
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 a cloud 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 using the provided option if the user deletes it.
8. Cut off your connection to the cloud.

This section will walk you through the many processes involved in uploading files: Step 1: Request the user's login information and then accept it.
The technique we have given tries to stop attacks that might be launched against the user data. Authentication is the first step in accomplishing the same goal. The system will accept the user's submission of their username and password. After these two things have been confirmed, the user will have access to their data. After the user's name and password have been entered, you should verify the authenticity of the information. The system will only create a connection with the cloud if the username and password 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 cloud 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 cloud. In this section, you will choose the file

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

that will be uploaded. The user can pick any text file stored in their system's memory. After selecting the file that is going to be uploaded,

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

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

Step 4: Write down this password and produce a key using the password you wrote. This is a crucial 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 essential technique that employs the same key for decrypting the material as it does for encrypting it. Using a critical generator function, this key is produced using the password. We strongly suggest you use PBKDF2 (Password-Based Key Generation Function 2). The increased amount of processing makes it much more challenging to break a password. This technique is referred to as essential 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 a Brute-force assault might compromise the password. This is something that should be kept in mind. Because of this, it is strongly suggested that the user use 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, 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 cloud 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.

Step 6: Place the file in a cloud storage location.

The uploaded information is encrypted, and the cipher 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 cloud 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 cloud, the user is offered the option to remove the file from their local device. The user can forego this action and keep the file in its original state by using the second available option. We strongly suggest that the original file be discarded in its entirety. Because of this, the plain text file saved on the system will not be accessed unauthorizedly 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 cipher text file was successfully transferred to the cloud and that the user does not have any other files that need to be uploaded, the connection to the cloud must be severed.

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

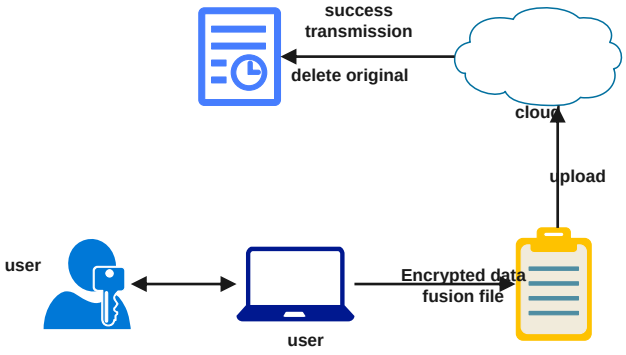

Figure 4: File upload

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

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.
Step 2: Ask the user to choose the file they want to download.
The user's whole collection of files stored in the cloud up to this point is shown. It is up to the user to choose one of the available files from the list.
Step 3: The user should be prompted to provide a password before decryption.
In this part of the process, the user will be prompted to enter the password 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 that matches the one used to encrypt the file, the cipher text file that the user uploaded 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 using the same key.
5. Put the decryption into action to decipher the submitted encrypted text.
This is only feasible if the same password is put into the critical generator function to produce the key. Other than that, it is impossible. Once the entered password is confirmed, use the password to make the decryption key using the key generator feature.
Step 6: Save a copy of the file to your local device from the cloud.
Store the plaintext decrypted in the user's computer's memory.
Step 7: Ask the user whether he wishes to remove the encrypted file uploaded to the server.
If the user chooses the delete option and indicates that they do not desire to download more files from the cloud, the encrypted file should be removed from the cloud storage location.
Step 8: Disconnect your device from the cloud.
Sign out of the user account and terminate the already established connection with the cloud. The process of downloading files, which is diagrammatically shown in Figure 4 as:

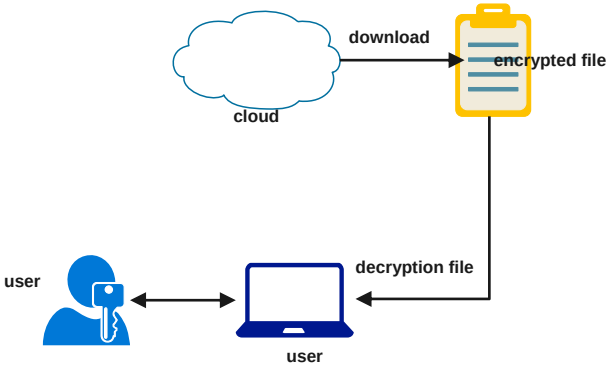

Figure 5: File download

4 Experimental Results and Analysis

Implementation var password = "Lock it up saf3," var plaintext = "pssst... don't tell anyne!," and var ciphertext = "Aes." Ctr.encrypt(plaintext, password, 256); var origtext = Aes.Ctr.decrypt(ciphertext, password, 256); Ctr.decrypt(ciphertext, password, 256);

Implementation Details

In this part, we will examine some essential aspects of the implementation. The Client App, the Encryption/Decryption Service, and the Storage Service are the three parts that comprise the larger whole, the entire project.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

Client App: A Brief Introduction Client App is a java web starting program. Figure 5 provides a visual representation of the Client Login Form. Web Startup is superior to applets because it solves numerous compatibility issues with browsers' Java plug and various JVM versions, while applets only solve a few of these issues. On the other hand, web pages no longer include Web Start apps as a page component. They are different apps that operate in their separate frames. To become a new user, the client or user must first register by clicking the "Register" button on the Login Form. After that, the client or user must log in with their unique user.

Step 1 Client App

At this point, the user will be prompted to provide their username and password before the system can accept them. After these two things have been confirmed, the user will have access to their data. After the user's name and password have been entered, you should verify the authenticity of the information. The system will only create a connection with the cloud if the username and password 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, as seen in Figures 6 and 7, respectively.

Figure 5: Client App Login Form

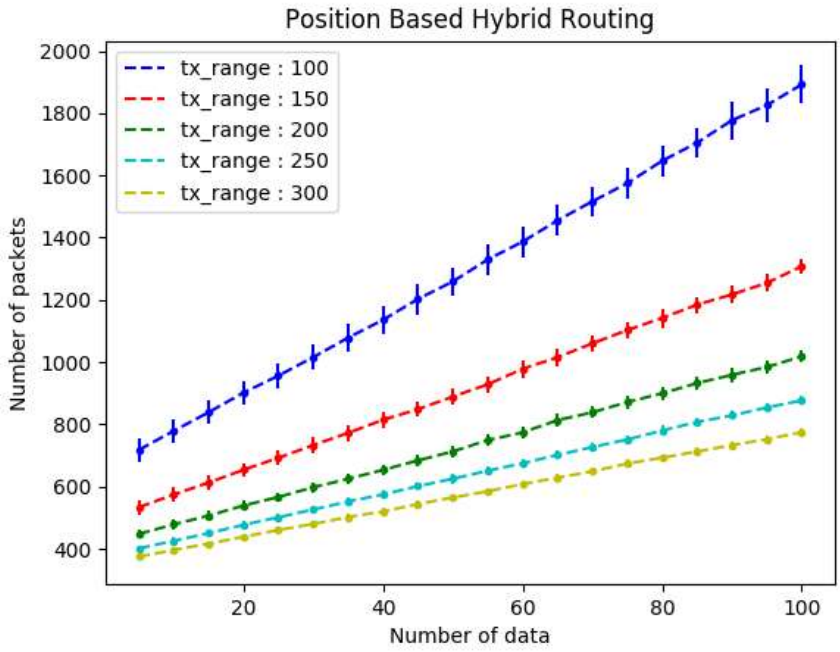

Figure 6: Position-based routing

Step 2 Encryption/Decryption Service

For example, the accounting department's head finalizes the "YDT Summary" report for a small-scale business. They then want to upload the document to cloud storage. The user clicks on the "Upload Data" button, then click's on "Upload File" and selects the file uploaded from its device/machine. The user now selects if they want to make the file Encryption which will be only accessible to itself, and the encrypted file will be stored in a cloud database. If the user uploads the file to the cloud without encryption, the original data will be held in the cloud. After uploading an encryption user can delete the original file from the user's machine so that only encrypted data go into the cloud. While uploading the file, it shows appropriate messages wherever necessary, as shown in Figure 8.

It now needs the list of people who will be able to access the file; for this, it clicks on the "Access List" button, followed by the "Add Access" button, and search for the person who will be able to access the data and click on "DONE," Figure 9.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

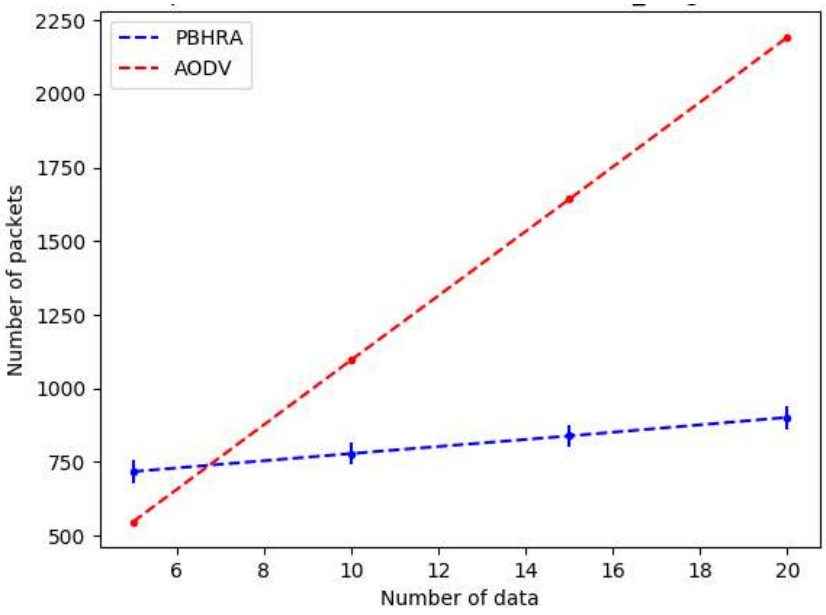

Figure 6: User Uploads comparison

```
Train Epoch: 800 [2000/15391 (13%)]     Loss: 0.014689
Train Epoch: 800 [3000/15391 (19%)]     Loss: 0.011826
Train Epoch: 800 [4000/15391 (26%)]     Loss: 0.008019
Train Epoch: 800 [5000/15391 (32%)]     Loss: 0.011443
Train Epoch: 800 [6000/15391 (39%)]     Loss: 0.012573
Train Epoch: 800 [7000/15391 (45%)]     Loss: 0.020904
Train Epoch: 800 [8000/15391 (52%)]     Loss: 0.014647
Train Epoch: 800 [9000/15391 (58%)]     Loss: 0.012772
Train Epoch: 800 [10000/15391 (65%)]    Loss: 0.013663
Train Epoch: 800 [11000/15391 (71%)]    Loss: 0.010102
Train Epoch: 800 [12000/15391 (78%)]    Loss: 0.010029
Train Epoch: 800 [13000/15391 (84%)]    Loss: 0.013865
Train Epoch: 800 [14000/15391 (91%)]    Loss: 0.011785
Train Epoch: 800 [15000/15391 (97%)]    Loss: 0.018701

Train accuracy: 72.7308167110649

Train set: Average loss: 0.5302693553702541

Test set: Average loss: 0.529815946435883

Test accuracy: 71.73006774361647
Train Accuracy 72.7438113183029
Test Accuracy 72.17300677436165
index is: 770
Number of train sensors 48.236732
Number of test sensors 48.163227
Train recon loss 0.5203007079478122
Test recon loss 0.5324413171860567
```

Figure 7: User Adds Access to Confidential Files

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

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

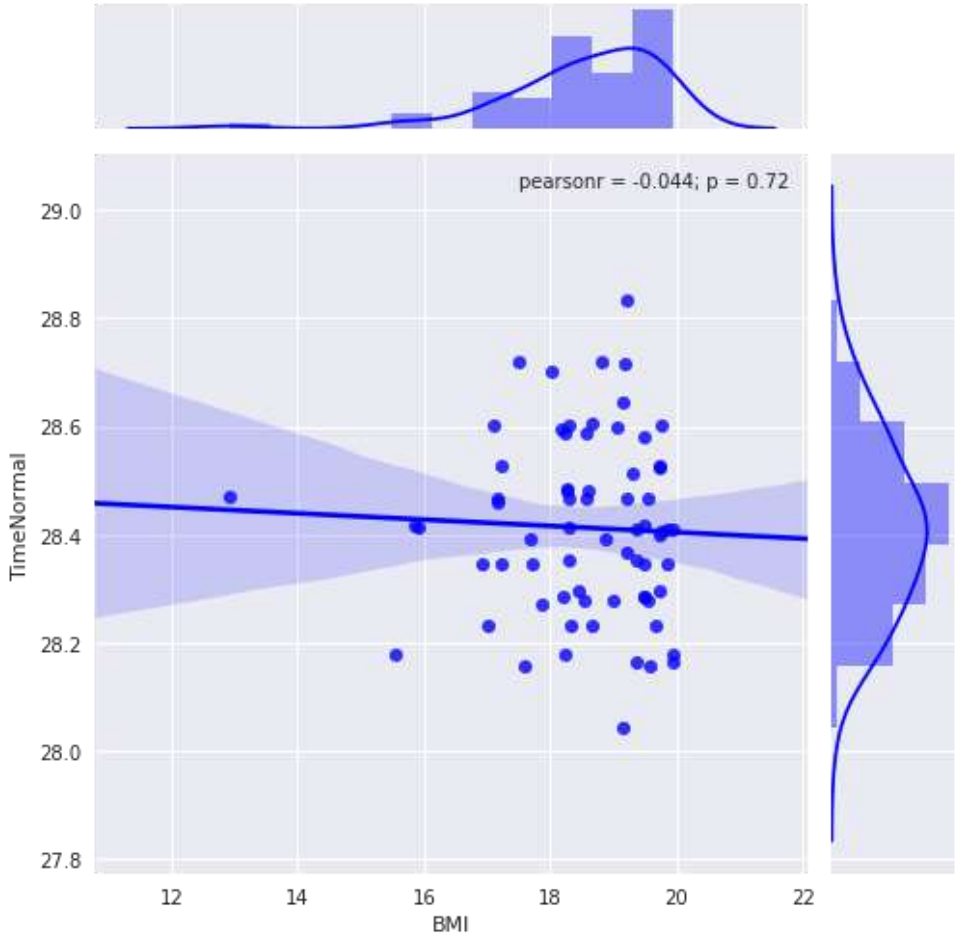

Figure 8: Download File and Decryption

Step 3 Storage Service

Click on "Save File as shown in Figure 9

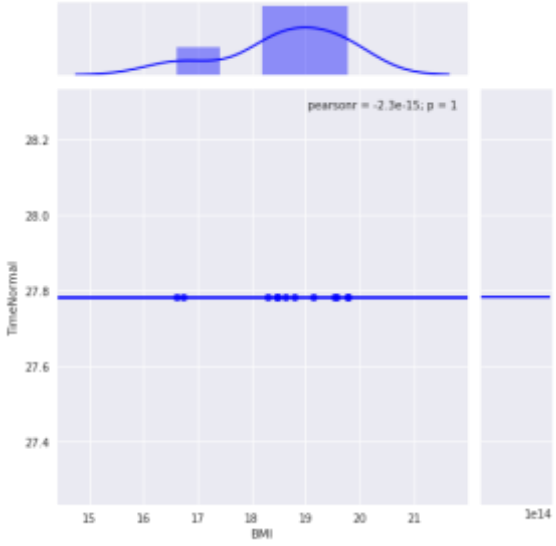

Figure 9: Owner Viewing Confidential File.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

5. Conclusion

The Cloud Service User Security Tool with Oracle Database 12c (CSUS), which was built to offer security on the user side, encrypts sensitive data before storing it in the cloud, allowing only authorized users to access the data. Data that has been encrypted is kept in the Virtual Machine of the cloud service provider. Encryption, when used in conjunction with Oracle Database 12c, helps ensure stored data's safety. According to the findings, the newly developed algorithm could accomplish its tasks in a shorter amount of time than the traditional RSA and Data Encryption Standard (DES) methods. This shows that the suggested efficient RSA with the CSA method is superior to the other strategies in terms of its overall performance. In addition, the efficient RSA with the developed CSA offers a higher throughput even though it extends the length of the algorithm's private key. In the future, the suggested method will undergo additional improvement by using different hybrid optimization-based algorithms to maximize the efficiency with which the key is encrypted. The improved throughput offered by the efficient RSA with CSA is achieved despite an increase in the total length of the algorithm's private key. In the future, the suggested method will undergo additional improvement by using different hybrid optimization-based algorithms to maximize the efficiency with which the key is encrypted. The work that will be done in the future may expand the study that is intended to work toward reducing the overhead of network traffic. The levels method and a particular decryption algorithm have been implemented in this research effort to increase communication security between users and cloud computing environments' servers. This research work addresses an issue with cloud computing's security. Utilizing a practical RSA cryptosystem elevates the protection of data storage. The secret key generation and data encryption are carried out with the assistance of the RSA cryptosystem. This is done to safeguard the data against the unauthorized access of a third-party auditor. The optimization of the secret key is carried out with the assistance of CSA to prevent a brute-force attack. According to the analysis of performance parameters, the system that has been provided is capable of achieving greater efficiency as a viable option for ensuring secure communication in the cloud. The scope of this study is limited to the cloud environment by itself. This study investigates the security concerns associated with the cloud environment, namely those about data integrity. This study is focused entirely on establishing the integrity of data stored in the cloud by using the services of a third-party auditor.

Funding: "This research received no external funding."

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

References

[1] Abhishek et al. (2012)," Cloud Data Security while using Third Party", International Journal of Scientific & Engineering Research, Vol. 3.

[2] Wang, S., Celebi, M. E., Zhang, Y. D., Yu, X., Lu, S., Yao, X., ... & Tyukin, I. (2021). Advances in data preprocessing for biomedical data fusion: an overview of the methods, challenges, and prospects. *Information Fusion*, *76*, 376-421.

[3] Kashinath, S. A., Mostafa, S. A., Mustapha, A., Mahdin, H., Lim, D., Mahmoud, M. A., ... & Yang, T. J. (2021). Review of data fusion methods for real-time and multi-sensor traffic flow analysis. *IEEE Access*, *9*, 51258-51276.

[4] Ali et al. (2016)," Security and Privacy of Sensitive Data in Cloud 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 Cloud Data Integrity in Multi-Cloud Environment", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, pp.505-509.

[6] Li, Q., Huang, Y., Zhang, J., & Min, S. (2021). A fast determination of insecticide deltamethrin by spectral data fusion of UV–vis and NIR based on extreme learning machine. *Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy*, *247*, 119119.

[7] Arasu, S. et al.((2013), "Privacy-Preserving Public Auditing In Cloud 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 cloud: A survey" ACM Computational Survey, Vol 48-1, pp 1- 50.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021

[9] Arjuna et al. (2016),” Cloud Data Security with Modified RSA Algorithm”, International Journal of Engineering Research & Technology, Vol.5 (5), pp.205-208.
[10] Arora et al. (2012),” Cloud 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-Cloud 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 cloud computing architecture in big data”, Information Granularity, Big Data, and Computational Intelligence, Cham, Switzerland: Springer International Publishing, pp.275-295.
[13] Bhagat, Sahu (2013),” Cloud 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 cloud computing security issues”, World Congress on Information and Communication Technologies (WICT).
[15] Deng, Y., Xiao, J., & Zhou, S. Z. (2021). ToF and stereo data fusion using dynamic search range stereo matching. *IEEE Transactions on Multimedia*, *24*, 2739-2751.
[16] C. Cachin, I. Keidar, and A. Shraer, “Trusting the cloud,” SIGACT News, vol. 40, no. 2, pp. 81–86, 2009.
[17] Charmee V. Desai (2014),” Survey on Data Integrity Checking Techniques in Cloud 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 cloud 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 Cloud Storage”, Computers, IEEE Transactions, Vol. 62(2), pp.362–375.
[24] Dinh HT, Lee C, Niyato D, Wang P (2013),” A survey of mobile cloud 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 Cloud 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 Cloud Computing Security Management Framework", 4th International Conference on Cloud 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 Cloud Computing”, International Journal of Innovative Science, Engineering & Technology, Vol. 6 (4),pp.61-68.

Doi : https://doi.org/10.54216/FPA.030204
Received: February 17, 2021 Accepted: May 25, 2021