International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

ELTPA : EFFECTIVE LIGHTWEIGHT THIRD-PARTY AUTHENTICATION PROTOCOL FOR CLOUD INTEGRITY AND SECURITY

Kalluri Rama Krishna[1], C. V. Guru Rao[2]

[1] Research Scholar, Osmania University, Hyderabad India
[2] Professor & Dean, School of Computer Science & Artificial Intelligence, S. R. University, Warangal, India.
Corresponding Author Email: kallurirk@hotmail.com

Article Info
Volume 9, Issue 1
Page Number : 276-291

Publication Issue :
January-February-2022

Article History
Accepted : 20 Feb 2022
Published: 28 Feb 2022

ABSTRACT

With the increasing demand for adaptation, cost minimization, high availability, scalability of cloud computing is also increasing. Cloud security is emerged as a critical component of its continued growth and success. An anonymous authentication mechanism for Cloud users is presented in this work, and it is both safe and productive. This process entails establishing mutual authentication between the cloud server and the user before granting access to the cloud using Effective Lightweight Third-Party Authentication protocol. The cloud users and the targeted service provider can interact with one another after the successful mutual authentication through third-party authentication. Even though several cloud computing authentication systems are available, the ones offered are not as secure as the ones previously used. Furthermore, the ones that have been presented are more durable and can resist a broader range of security threats. The proposed framework ELTPA protocol is intended to propose cloud environment with secure and lightweight authentication that is both fast and easy to use. A variety of different adversaries readily breaches it. The AVISPA tool is a performance evaluation tool that may be used to assess the effectiveness of a suggested protocol. It demonstrates that it is capable of resisting well-known security threats.

Keywords : Adversary model, AVISPA tool, Cloud Authentication, Computation complexity. Privacy. Conditional tracking. Data integrity.

I. INTRODUCTION

The Cloud Computing refers to collection of devices that gather data and interact with one another across a network of connections. Many of these devices are linked to the Internet through a wireless connection. They must be able to keep and share the information that they acquire with others. Cloud computing has emerged as a viable option for dealing with the many computational and storage challenges that cloud applications are confronted with today. However, to protect the users of this platform from exploitation, a variety of security measures must be implemented. There are several vulnerabilities in the authentication

procedures used in the cloud environment that may be exploited. A novel adversary model, as well as a mutual authentication technique, are introduced in this work. Participants are made up of a collection of users, cloud service providers, and a third-party that has been thoroughly vetted. The users use smartphones and other Internet-connected devices to access the service. The data of the users is collected and stored by the cloud service providers.

Clients may now choose from various processing techniques and the advancements in network and computer technologies. An excellent example of this is cloud computing, enabling clients to access a network and computational resources without being bound to a single physical location. Security and privacy are two essential considerations that cloud computing companies should consider before launching their services to the public. In order to reduce the danger of exploitation, service providers should ensure that their systems have sufficient security to prevent unwanted access from occurring.

An attacker can change or intercept communications delivered before they reach their intended recipients. They may be able to carry out a variety of attacks because of this vulnerability. Cloud computing security is not a simple undertaking, and it might be compromised if a user is not verified anonymously, as is the case here. When it comes to cloud computing, several issues might arise. Because the user information is saved in the cloud, an attacker can change or discover the specifics of the system. A mutual authentication system may be used to establish a connection between the user and the service provider. This strategy is effective even when the service provider does not know the user's identity who is being served. Mutual authentication becomes more secure and resilient as a result of anonymity. Aside from that, it prohibits an attacker from keeping track of which users and services are cooperating. Cloud servers must also consider the privacy of their users, which is a significant security problem to address. A successful attacker would not reveal the user's private information to the rest of the world if he or she were successful. Some researchers have devised an anonymous authentication technique that may avoid the exploitation of spying and impersonation attacks. This scheme is intended to address the problem. The unlikability of this security notion is still another key issue to consider. A secure bilinear pairing authentication system is proposed in this study, which does not need the usage of SSL or mutual authentication to be implemented.

This effort aims to develop a mutual authentication system that will allow users and service providers to authenticate each other without needing to know each other's identities. The parts that follow are grouped in the manner shown below. These sections provide an overview of the different themes explored in the book. They also go through the numerous actions that must be taken to put the system in place. A mutual authentication system for the Cloud Computing is presented in this work, which is enhanced and lightweight in comparison to previous protocols [9]. An enhanced adversary model and protocol for secure authentication in an environment with the cloud is presented in Section 3 of this paper. It is stated in Section 4 that the findings and comments from this section are given.

II. RELATED WORK

This part will go through the many types of authentication systems that may be used in cloud settings. After this section, we shall summaries and compare the various approaches. When using the recommended solution, it is necessary to encrypt the password table, making it susceptible to an attack induced by the theft of a username. An authentication system that is both safe and readily manipulated has been presented, called multi-server authentication. However, it is not secure and needs a significant

amount of storage. With the introduction of Juang5, a multi-server authentication mechanism that uses nonces and passwords was developed. Within-company assaults, as shown by Ku et al. [1], are a simple way to exploit the suggested technique. In today's environment, the current authentication mechanisms are not safe enough to be used. In order to circumvent this problem, Amin et al. [2] have presented an expanded authentication technique that is not only safe but also of great complexity, as described below.

Generally speaking, public-key cryptography is used to provide authentication for cloud computing applications in most scenarios (PKI). In this mode, certifications are provided to a third party known to be trustworthy (TPCP). The high cost is a result of the process's inherent complexity. An IBC was presented as a means of lowering these costs. Li and colleagues presented a cloud-based authentication technique that is based on the Internet of Things. It should be noted that this system needs the regular and safe transmission of each user's identity information to prevent unwanted access. The suggested solutions were too complicated, and they could not offer a unified method for dealing with a variety of privacy concerns. Instead, they advocated for incorporating a mutual authentication and key agreement mechanism that is resistant to other assaults. Even though the suggested system can generate strong passwords, it cannot prevent the security risks caused by password guessing. It also lacks a revocation mechanism, which would enable consumers to cancel their subscriptions at any time [10].

A lightweight authentication technique has been presented to prevent some security vulnerabilities in the future. In this method, there are no erroneous mutual authentication procedures used. However, it is not appropriate for use in a secure cloud environment where users may remain anonymous. An attacker might quickly get a user's private keys if the user has several private keys shared by various cloud service providers, allowing the attacker to impersonate the service provider. It is a primary problem with these methods. The majority of the authentication techniques that have been developed do not provide secure forward secrecy as a feature. The majority of the time, the implementations of these systems fall short of providing enough anonymity. In 2017, they suggested a way of anonymous authentication for cloud computing, which was accepted. Based on the notion of Hierarchical Attribute Authorization, the approach is implemented. It may be used to authenticate users without requiring them to submit any personal information into the system. For user registration and cancellation, this scheme does not offer any functionality. As an alternative, it presents an anonymous authentication technique based on protecting personal information in the cloud environment [11].

They developed a framework that would allow for the safe storage and retrieval of all sensitive information kept in a private cloud while maintaining the highest level of security. Put system through its paces against a variety of security threats. According to Babu et al.[3], the most severe problem in their protocol is allowing a malicious cloud server to impersonate a safe cloud server. This problem may be resolved by implementing a mutual authentication mechanism on the network. The suggested protocol is based on a set of processes that, when taken together, ensure the system meets security standards that have been established. Using the AVISPA tool, they conducted a rigorous cookie verification procedure. According to the authors of this work, an enhanced authentication method based on an ECC-based authentication system has been developed. It circumvents the constraints of the current protocol in a significant way 12.

Zargar concluded that their proposed protocol is more secure and efficient for implementing cloud ecosystem after conducting a performance and security analysis.

They proposed an extended secure authentication mechanism that is based on the key agreement for cloud environments. They put their suggested solution through its paces against various known threats and demonstrated its ability to withstand them. Kumar and his colleagues have devised a secure key exchange technique that may facilitate the interchange of RFID tags between cloud servers and mobile devices such as automobiles. They employed a method known as ECC to encrypt the data sent across the network. Their suggested technique for building an authentication system for the Cloud Computing devices performed admirably, and they received high praise for it. Because of their calculations and the completion of their recommended task, they could accomplish their goal [14].

In order to verify their solution, they used ProVerif to conduct a verification study. They demonstrated that it is capable of protecting against a variety of well-known assaults. It also had some security characteristics. Using the data from the Cloud server, Wazid et al and his colleagues have devised a lightweight approach of authenticating both fast and secure users. According to the authors, their suggested approach verifies the validity of end-users via the use of XOR and one-way hash algorithms. It was also shown by the authors of this research that their solution outperforms current authentication methods in terms of network and communication costs.

They have presented an upgraded key-based authentication protocol that tackles the security restrictions of a dispersed cloud server network by using asymmetric key authentication. They put it through its paces with the help of the ProVerif tool and the BAN logic model. Furthermore, the performance of the suggested protocol was shown to be much superior to that of the most recent authentication techniques. With the help of the AVISPA tool, they then conducted a detailed analysis of the many security elements of their planned project. They also examined the performance of the suggested work and said that it is much less expensive than the current alternatives. They conducted research in which they compared their suggested scheme to the one proposed by He et al.[4], which was shown to be ineffectual against most security assaults. They then created their key agreement and authentication technique to use with the system.

Their suggested security solution was presented and evaluated using the ProVerif program, which allowed them to demonstrate its resilience to various threats. The findings showed that their technique is safe but has a higher computational cost than the competition. Fan et al.[5] present a dependable RFID authentication technique that may be employed in a cloud-based system to verify the identity of users. Instead of using the hashing algorithm, their solution makes use of a rotation and permutation operation. During their research, they discovered that the suggested solution may minimize the storage and communication overhead of the tag and that it is also possible in cloud-based networks.

The authors of this research have proved that the architecture presented by Madhusudhan et al. [6] failed to ensure user anonymity [7] and might potentially disclose sensitive information. It was also shown by the researchers that its implementation is subject to a variety of assaults. Specifically, we demonstrate in this work that the proposed key agreement system for the Cloud Computing is susceptible to exploitation due to its lack of transparency and inability to establish an efficient key agreement, both of which are deficiencies. In response to their discovery of the flaws in the Braeken and Mall et al.[8] created a new protocol that allows secure communication between two devices. Many strategies for authenticating users have been developed; however, these systems are often subject to exploitation due to recent adversary capability advances. Using a mutual

authentication protocol as the basis for our adversary model, we provide it in this work for the first time.

2.1 Preliminaries and system model

This section discusses the modeling of the system, the security needs, and the bilinear pairing principles, all of which are essential considerations.

The Trusted Third-Party Communication Protocol (TPCP) communicates with service providers and users when the registration procedure is complete by sending authentication data to both parties. Once the information is collected, the service providers keep it on their servers and utilize their authentication procedures. The TPCP picks its key and then calculates its public key, which it subsequently distributes. After transmitting their identities and relevant information to the TPCP, the user and their service provider must identify themselves using a secure communication mechanism such as SSL. The primary goal of this framework is to provide a privacy-protecting system that would enable companies to verify their users while maintaining their anonymity in the process.
Before a user may commence a data transfer, it is critical that they first authenticate themselves and that the information being sent is secure. Both of these steps must be completed before the user can begin requesting data from the service provider. It is critical to keep every user and server's identities hidden to protect their personal information. Anonymity, reversibility, and traceability are all critical. The TPCP can identify the identity of users and SPs without the need to depend on other organizations.

2.2 Bilinear pairing

Let G_1, G_2, and G_T represent 3 multiplicative cyclic groups of order q, here q is a large prime. The bilinear map $e: G_1 \times G_2 \rightarrow G_T$ obeys 3 properties.

1 Bilinearity: The mapping $e: G_1 \times G_2 \rightarrow G_T$ is said to be bilinear if $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}, g_1 \in G_1 \& g_2 \in G_2$ and $\forall \quad a, b \in Z_q^*$, where $Z_q^* = [1, \dots, (q-1)]$

2 Nondegeneracy: $e(g_1, g_2) \neq 1_{G_T}$.

3 Computability: we have an productive method to smoothly calculate the bilinear map $e: G_1 \times G_2 \rightarrow G_T$. Let ψ be the isomorphism and represented as $\psi: G_2 \rightarrow G_1$.

III. THE PROPOSED ELTPA APPROACH

The ability to offer secure connections to the internet is essential for keeping consumers safe on the internet. This research aims to enhance the security of the authentication strategy for devices that make use of the cloud. The cloud environment is one in which the data gathered by a client node is transferred to a cloud server for storage. The data on the cloud servers may be accessed at any time by the user. In order to create a connection with the cloud server, the user registration procedure must be completed. After that, the server needs to be registered with a reputable third party in order for users to be able to contact it. Users must first create an account with the trust center to have access to the cloud server. After that, they authenticate with the trusted third-party service provider. The Do Lev-Yao model is used to describe the notion of the remote authentication protocol. Recent years have seen an increase in the capability of the adversary's military forces. The suggested framework is divided into four phases: user registration, authentication, cloud server registration, and password updating. Each step is described in detail below as shown in figure-1.

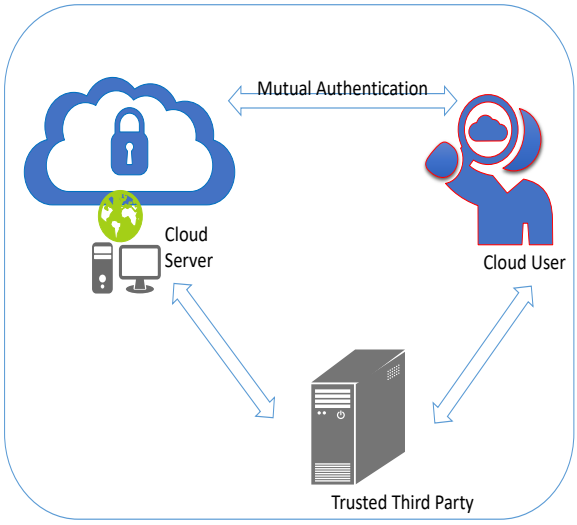

Figure 1: Architecture of the proposed approach

The adversary has the ability to get every communication that travels across the network as well. A user's smartcard and registration information may also be obtained by the adversary from the user. The attacker may simply seize a user's smartcard and utilise it to obtain access to their financial information. Also possible is the capturing of a session key that has become invalid. The mechanisms for anonymous mutual authentication are described in detail. Service providers must verify their users in order to prevent communication with unlawful users. The registration phase, system initialization, mutual authentication, and phishing are the four steps of this procedure, covering the registration phase, system initialization, mutual authentication, and phishing. When it comes to sending data, both parties should check the other party's integrity before proceeding.

sig $_{\_ j} = g_2^{\overline{r_j + S \cdot S_p p_j}}$ is the anonymous signature of information M in an anonymous mutual authentication between the user and the service provider. It is stated as follows: c_j is the pseudonymous certificate for information M. The short-life confidential private key r_j and the service provider confidential private key $SPprk_j$ are both used to compute sig_j and c_j, which are only known to the corresponding service provider and are not shared with anyone else. Because both keys are unknown, it is impossible to create an anonymous certificate and an anonymous signature using a forged anonymous certificate. Aside from that, the short-lived private keys are changed regularly. As a result, even if an intruder knows the short-lived confidential private key r_j, the intruder will not issue the current anonymous certificate unless the intruder also knows the service provider's secret private key $SPprk_j$. In the same way, the anonymous signature is determined by the equation using $usig_i = g_2^{\overline{s_j + 4\mu_i + H(F)}}$. On the other hand, the user signature cannot be forged if we are unfamiliar with the user confidential private key upr $_i$ and the short-life confidential private key s_j, both of which are used in the process of forging. False attacks and impersonator assaults are thus prohibited under this approach.

3.1 Conditional privacy preservation

When it comes to protecting the genuine identities of users and service providers, anonymous certificates and signatures are widely employed to do so. The TPCP may determine a user's genuine identity by mapping an anonymous certificate to the user's computer.

3.2 Anonymity

It is computationally tough to identify the genuine user who sent the message when using an anonymous signature $_i = g_2^{\frac{s_j + u\mu p_i + H(F)}{2}}$ and certificate cu_i in conjunction with a digital signature. As a result, the intruder cannot determine who sent the message from $usig_i$ and cu_j.

3.3 Unlikability

Calculations for the signature utilizing $\_ _i = g_2^{\frac{1}{s_j + 4pr_i + H(F)}}$ and the certificate cu_j are performed using short-life secret private keys that are chosen at random. So each change to the short-life keys results in the generation of a new anonymous signature and certificate for each communication that takes place. As

a result, without the usage of TPCP, it is impossible to determine if two connections were initiated by the same person or not.

3.4 Non-repudiation

Once the user has received the notification from the service provider, they will be unable to retract their response. Because when the user gets a message from the service provider, it may use the c_j function to determine the efficacy of the service provider and the sig_j function to verify the identity of M. When a disagreement arises, the user may present the msg to TPCP. The TPCP may follow the real identity of the service provider from the message and then eventually disclose the service provider's privacy and remove it from the cloud using the information from the message.

IV. SECURITY ANALYSIS

In this section, security and privacy analysis of our proposed scheme is described.

4.1 User registration

The user registration procedure that specifics the process are covered in the following sections. When user $i(\text{U}_\text{i})$ initially connects to the network, it selects a unique identification (UID_i), a pseudo-identity $(PUID_i)$, and a password to identify itself (P_i). Afterward, it selects a random value (UR_i) and, using the hash function (H), calculates the value of A_i by Equation 1 using the random value (UR_i). Bio_irefers to the user's biometric information.

$$\begin{aligned} PBio_i &= P_i \oplus H(Bio_i) \\ UA_i &= H(PBio_i \parallel UR_i) \end{aligned}$$

Then U_i sends a registration message to the TPCP, containing the $(UID_i, PUID_i)$ identifiers. When a UID_i is received, the TPCP first determines whether or not it is genuine. If the test is passed, TPCP picks a random number TR and uses Equation 2 to compute TTP_1 and TTP_2. TPCP then transmits (TTP_1, TTP_2, ID_{TTP}) to U_i, followed by a return.

$$\begin{aligned} TTP_1 &= H(UA_i \| ID_{TTP} \| TR) \\ TTP_2 &= H(UID_i \parallel TR) \end{aligned}$$

Finally, U_i calculates and stores (A_i, B_i, C_i, D_{TTP}) in its smart card using Equation 3.

$$\begin{aligned} A_i &= TTP_1 \oplus UA_i \\ B_i &= TTP_2 \oplus H(UID_i \parallel UA_i) \\ C_i &= UR_i \oplus H(UID_i \parallel P_i) \end{aligned}$$

4.2 Cloud service provider registration

The registration procedure for cloud service providers specifics the process which are addressed in the following formula. The cloud service provider should also be registered with TPCP, if not already. Consequently, service provider j(SP_j) logs into the network and picks an identifier $(SPID_j)$and a pseudo-identity (PSPID $_j$), and then transmits the (SPID $_j, PSPID_j)$ and the randomly determined value (SPR_j) to TPCP for registration. When the data is received, TPCP uses Equation 4 to compute $STTP_1$ and $STTP_2$. Afterward, TPCP delivers the following data to SP_j: $(ID_{TTP}, STTP_1, STTP_2)$

$$\begin{aligned} STTP_1 &= H(PSPID_j \| ID_{YTP} \| TR) \\ STTP_2 &= H(SPID_j \parallel TR) \end{aligned}$$

When received, SP_j stores $(ID_{TTP}, STTP_1, STTP_2, SPID_j, PSPID_j)$.

4.3 Authentication

The authentication procedure that specifics the process that are addressed in the following sections. User $i(U_i)$puts his smart card into the card reader and enters his username $(UID_i,)$.and password (P_i) into the card reader's keyboard. The smart card then produces a new $PUID_i$, termed $PUID_i^{\text{new}}$ and picks a random integer SC_u, and uses Equation 5 to compute the data shown

below. After that, M_u =Data $_1$, Data $_2$, Data $_3$, Data $_4$, $PUID_i$) is delivered to SP_j as a function of the input data.

$$\begin{aligned} Ub_i &= H(UID_i \parallel PBio_i) \oplus C_i \\ UHP_i &= H(PBio_i \parallel Ub_i) \\ A_i^* &= UHP_i \oplus A_i \\ B_i^* &= H(UID_i \parallel UHP_i) \oplus B_i \\ Data_1 &= SC_u \oplus A_i \\ Data_2 &= UID_i \oplus H(SC_u \| PUID_i \| ID_{TTP}) \\ Data_3 &= B_i^* \oplus H(SC_u \parallel UID_i) \oplus H(UID_i \parallel UHP_i) \\ Data_4 &= H\left(SC_u \| PUID_i \| PUID_i^{\text{new}} \| ID_{TTP} \| Data_3\right) \end{aligned}$$

SP_j generates a new $PSPID_j$, denoted as $PSPID_j^{\text{new}}$, and chooses a random number SP_s and calculates the following data using Equation 6. After that, M_{sp1} = (Data $_1$, Data $_2$, Data $_3$, Data $_4$, Data $_5$, Data $_6$, Data $_7$, Data $_8$, PSPID $_j$, PUID $_i$) is sent to TPCP.

$$\begin{aligned} \text{Data}_5 &= STTP_1 \oplus SP_s \\ \text{Data}_6 &= SPID_j \oplus H\left(SP_s \| PSPID_j \| ID_{TTP}\right) \\ \text{Data}_7 &= STTP_1 PSPID_j^{\text{new}} \oplus H\left(SP_s \parallel SPID_j\right) \\ \text{Data}_8 &= H\left(SPID_j \| PSPID_j \| PSPID_j^{\text{new}} \| SP_s \| Data_7\right) \end{aligned}$$

TPCP checks the validity of UID_i and $Data_4$ by computing SC_u, UID_i, and $PUID_i$. After that, it checks the validity of SP_j and $Data_7$ by computing $SP_s, SPID_j$, and $PSPID_j$ (new). The session is stopped when any validation fails. If the verification of user and cloud service provider is passed, TPCP generates a random number R_{TTP} and computes the following responses using Equation 7. After that, M_{TTP} = $(\text{Resp}_1, \text{Resp}_2, \text{Resp}_3, \text{Resp}_4, \text{Resp}_5, \text{Resp}_6)$ is sent to SP_j.

$$\begin{aligned} SK_{TTP} &= H(R_{TTP} \oplus SP_s \oplus SC_u \\ \text{Resp}_1 &= H\left(TR \| ID_{TTP} \| PSPID_j(\text{ new })\right) \oplus H\left(SP_s \parallel PSPID_j^{\text{new}}\right) \\ \text{Resp}_2 &= H\left(PSPID_j \| SP_s \| PSPID_j^{\text{new}}\right) \oplus \left(SC_u \oplus R_{TTP}\right) \\ \text{Resp}_3 &= H\left(SK_{TTP} \| \text{Resp}_1 \| \text{Resp}_2 \parallel \text{H}\left(SPID_j \parallel TR\right)\right) \\ \text{Resp}_4 &= H\left(TR \| ID_{TTP} \| PUID_i^{\text{new}}\right) \oplus H\left(SC_u \parallel PUID_i^{\text{new}}\right) \\ \text{Resp}_5 &= H\left(PUID_i \| SC_u \| PUID_i^{\text{new}}\right) \oplus \left(SP_s \oplus R_{TTP}\right) \\ \text{Resp}_6 &= H\left(SK_{TTP} \| \text{Resp}_4 \| \text{Resp}_5 \parallel \text{H}(UID_i \parallel TR)\right) \end{aligned}$$

SP_j checks the validity of Resp_3 by computing SC_u, R_{TTP}, and SK_{TTP}. If the validation result is positive, then SP_j computes $STTP_1^{\text{new}}$ using Equation 8 and replaces $STTP_1$ and $PSPID_j$ with $STTP_1^{\text{new}}$ and $PSPID_j^{\text{new}}$, respectively. Finally, M_{sp2} = $(\text{Resp}_4, \text{Resp}_5, \text{Resp}_6)$ is sent to U_i

$$STTP_1^{\text{new}} = \text{Resp}_1 \oplus H\left(SP_s \parallel PSPID_j^{\text{new}}\right)$$

The smart card checks the validity of Resp_6 by computing R_{TTP}, SP_s, and SK_{TTP}. If the validation result is positive, then it computes TTP_1^{new} using Equation 9 and replaces TTP_1 and $PUID_i$ with TTP_1^{new} and $PUID_i^{\text{new}}$, respectively.

$$TTP_1^{\text{new}} = UHP_i \oplus Resp_4 \oplus H\left(SC_u \parallel PUID_i^{\text{new}}\right)$$

4.4 Password update

The method of updating a password that specific steps that are outlined in the next section. When U_i wishes to update the user ID, password, and biometrics, U_i must follow the procedures outlined. However, to change the password, U_i must first compute the new M_u, which is marked as M_u^{new}, and then communicate it to TPCP as $M_{update} = M_u^{new}$.. When a request is received, TPCP verifies the UID_i and $Data_4$ fields. If the test is passed, TPCP computes new Resp $_4$, designated as Resp $_4^{new}$, by Equation 7, and Resp _7 by Equation 7. (10).

$$\text{Resp}_7 = H\left(UID_i \| \text{Resp}_4^{\text{new}} \| SC_u \| UID_i \| PUID_i^{\text{new}}\right)$$

It is simple for adversary A to obtain the authentication parameter by re-registering with the legal user Ui's identity IDi, which is a smooth process. Because the authentication parameter is static, on the other hand, it is possible to take advantage of it without difficulty. He-authentication Another advantage of Sadra technique is that it can prevent the user from accessing sensitive information on the server, which is another advantage.

V. RESULTS AND DISCUSSIONS

Here, the proposed anonymous authentication methods are evaluated in terms of performance analysis and total computational cost. This section makes discussion on simulation results of the AVISPA tool. We also compare the time cost and communication cost of the proposed protocol with its counterparts.

The computational cost of the suggested anonymous authentication technique for short-life anonymous signature and certificate methods is examined in this section. Computational pricing refers to the amount of time it takes for entities to validate a single/n signature and a single/n certificate to be created. It is computed to authenticate the entity and ensure that the information is accurate and complete. Many contemporary approaches, and CPA are evaluated in terms of computational cost to our method. In all of the ways, the BLS scheme is regarded as the foundation of the anonymous authentication method presented. Let $T_{pa\dot{b}}$ represent the time required for executing a pairing operation, T_{hash} represents the time required for performing a hash operation, and T_m represents the time required for performing a one-point multiplication operation. $T_{\text{exp}-1}$ and T_{exp-2} are the time units used to express exponential operation time in G_1 and G_2 (exp-2)

It can be shown in Table 1 that the anonymous authentication technique of the proposed scheme is less expensive in terms of computational price when compared to the different existing methods used during the verification of signature and certificate process. Because the anonymous authentication strategy requires just $2T_{pajr}$ and $3T_{ep-1}$ operations to examine a single anonymous message and signature, it is a cost-effective authentication method. As a result, as compared to the BLS, the Song's scheme, the CAS, the Khan's scheme, and the CPAS schemes, the newly suggested anonymous authentication technique can verify a more significant number of anonymous signatures and certificates. It has been noted that the T_{pair} and T_{hash} functions are the most time-consuming functions in the certificate and signature validation method. T_{pair}, T_{mud} , and T_{hash} are computed in our simulations and are equivalent to 1.6 milliseconds (ms), 0.001 milliseconds (ms), and 2.7 milliseconds (ms), respectively. 0.6" " ms is needed to perform $T_{\text{exp}-1}$ and $T_{\text{exp}-2}$ on a computer.

In this work, the PBC library performs operations such as exponential and multiplication, among others. It is also used in the calculation of the computational cost. It is necessary to study the outcomes from over 100 simulations in order to get the average conclusion. Table 1 also includes an explanation of the costs associated with certificate and signature verification.

As seen in Fig. 2, the cost of certifying a certificate and a signature is calculated. It demonstrates that our suggested approach for verifying a signature needs just two pairs of operations and two exponential operations to complete.

The computational time needed to validate a 100 user signature and certificate has grown dramatically due to the growing number of users. Our suggested strategy, on the other hand, is more cost-effective when compared to the current ways.

5.1 Total computational cost

Computing the computational cost of an authentication technique involves considering the amount of time it takes for a certificate to be generated and for verification to occur.

$$t_{TCC} = t_{gen} + t_{veri}$$

here, t_{gen} denotes the time required to generate one shortlife signature and certificate by the transferring entity, and t_{veri}] denotes the time required to check one signature and certificate by the verifier. The cost reductions associated with the suggested strategy for verification, which has been calculated. The TCC of the suggested system is lower than the TCC of the

current approaches. There has been a considerable reduction in the amount of time required to create certificates and signatures. Furthermore, our suggested approach is high-speed, taking just 570 milliseconds. The time necessary to verify an anonymous signature and certificate is shorter than the time required to verify the schemes already in place. Although our suggested technique can complete the verification of 100 signatures and certificates in as little as 710 milliseconds, the current schemes may take as long as 1080 milliseconds. The entire computational expenses of 100 certificates and signatures are completed in less than 1670 milliseconds using our suggested technique.

5.2 Simulation results of the AVISPA tool

The AVISPA program is used to determine whether validating an Internet security protocol is accurate and reliable. It is the most extensively used tool for this particular purpose in the world. There is no other tool that can compete with AVISPA in terms of performance and robustness. The suggested technique is provided in the form of an experiment, which uses the ON-the-fly Model Checker and the CL-Atse tool to demonstrate its effectiveness and efficiency. The two tools are used to examine cryptographic protocols, and they are complementary. The validation processes of the proposed protocol are shown in the figures that accompany this document. According to the table below, the recommended technique is safe to use with both instruments in question as shown in Table 1.

5.3 Computation cost

When it comes to managing passwords, we only compare the performance of the protocols that have been disclosed. Some protocols only give a password update phase after a user has updated their password, whereas others allow it at any time. The Xor operations are more efficient than the hash function in terms of computing costs as shown in Table 2 and figure-2.
According to this, assuming that the total of the XOR operations' calculation costs is equal to one hundred thousand, the suggested system has a lower overhead than the existing approach. We depict the time required to implement the SHA-2 protocol and its alternatives as shown in Table 3 and figure-3. Most of the one-way hash functions that we execute are performed using the SHA-2 approach. The cost-to-time ratio of the suggested strategy is the greatest, and the communication costs are the lowest. It outperforms the majority of the other options in terms of performance as shown in Table 4 and figure-4.

Table 1: Protocol AVISPA tool

Protocol	Li et al.	Amin et al.	Xue et al.	Wazid et al.	Yu et al.	Sadra	Proposed ELTPA protocol
CL-AtSe	Safe	Unsafe	Safe	Unsafe	Safe	Unsafe	Safe
OFMC	Unsafe	Safe	Unsafe	Safe	Unsafe	Safe	Safe

Table 2: Computation costs Comparative summary

Protocol	Li et al.	Amin et al.	Xue et al.	Wazid et al.	Yu et al.	Sadra	Proposed ELTPA protocol
TPA	25	16	18	8	12	16	8
Cloud Provider	8	4	6	8	6	6	4
Cloud Client	8	12	12	18	12	14	8

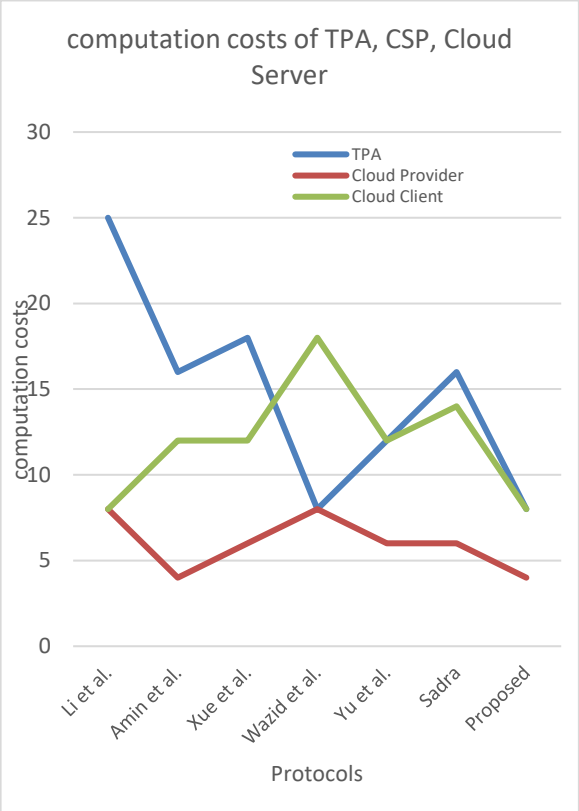

Figure 2: Computation costs of TPA, CSP, Cloud Server with recent approaches.

Table 3: Comparison of Time cost with recent approaches.

Protocol	Li et al.	Amin et al.	Xue et al.	Wazid et al.	Yu et al.	Sadra	Proposed ELTPA protocol
Time Cost	0.065	0.075	0.09	0.085	0.085	0.092	0.081

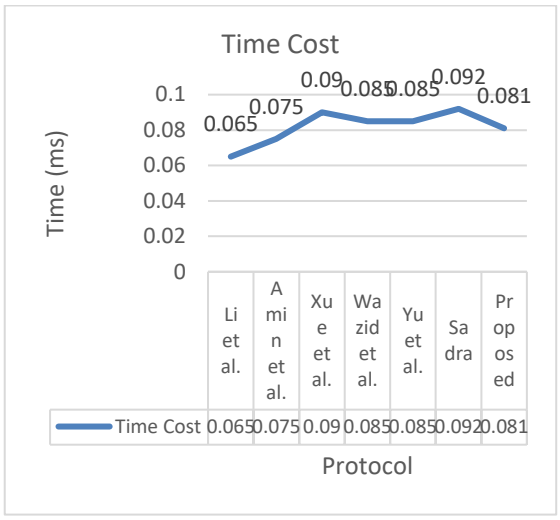

Figure 3: Time Cost with recent approaches.

Table 4: Communication cost with recent approaches

Protocol	Li et al.	Amin et al.	Xue et al.	Wazid et al.	Yu et al.	Sadra	Proposed ELTPA protocol
communication cost (bits)	6600	5700	5800	5100	6500	5000	4800

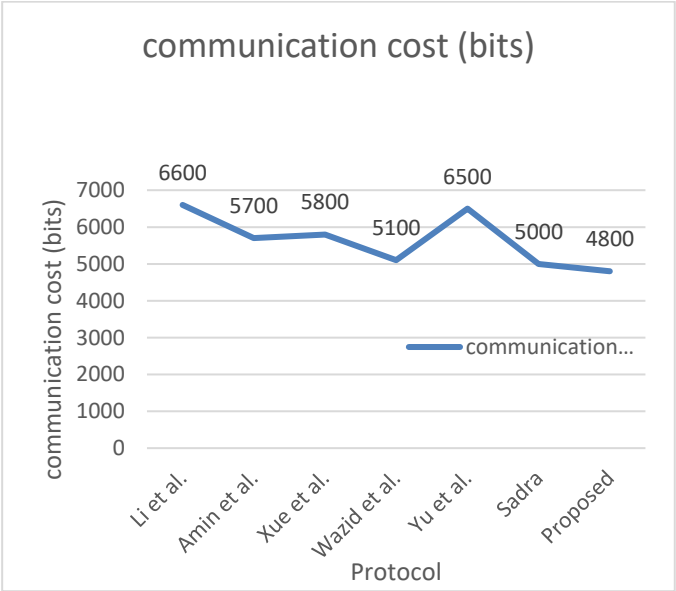

Figure 4: Communication cost with recent approaches.

VI. SECURITY ANALYSIS

The security analysis of the proposed protocol is a crucial stage in determining the appropriate security measures for the system to be implemented. A comparison of the different attack resistance systems and the recommended protocols is provided in the analysis. The suggested protocol satisfies all of the security criteria of the many methods that have been offered. Some of the functions, on the other hand, need security enhancements.

If the attacker steals the user's smart cart and according to the new adversary model, he/she can get access to the stored data in the last session of the smart card, he/she can calculate $Ub_i = H(UID_i \parallel PBio_i) \oplus C_i, UHP_i = H(PBio_i \parallel Ub_i)$. Then he/she can use $B_i \oplus H(UID_i \parallel UHP_i) = Data_3 \oplus PUID_i \oplus H(SC_u \parallel UID_i)$, $UID_i = Data_2 \oplus H(SC_u \| PUID_i \| ID_{TTP})$, $A_i = \text{Resp}_4 \oplus UHP_i \oplus H(SC_u \parallel PUID_i)$, and $SC_u = Data_1 \oplus A_i \oplus UHP_i$. It is impossible for the attacker to guess the UID_i and $PBio_i$, because A_i disappeared when the last session was over, and the attacker cannot compute SC_u.

6.1 Resistance to insider attack

In the proposed protocol, the user (U_i) sends a registration message containing $(UID_i, PUID_i)$ to the TPCP, which are not relative to the password. Therefore, the insider attack is avoided in the proposed authentication scheme. The ability to withstand a desynchronizing assault Users' data must be changed on their behalf, not by third parties if they want to have their information updated. Additionally, before updating the password, TPCP should verify the user's details with the user. An attacker is prevented from generating a message in a session if the session is resistant to forgery attacks. It is impossible for the attacker to forge a message in a session because he/she cannot elude the secret key TR in TPCP. The details of the resistance to forgery attack are discussed as follows.

1 In the user message M_u to the service provider, Data $_1$ and $Data_3$ have SC_u.

2 In the service provider message M_{sp1} to TPCP, Data $_5$ and Data $_7$ have SP_s. Furthermore, the service provider has the secret key of the user in M_u.

3 In the TPCP message M_{TTP} to the service provider, (Resp $_1$ to Resp $_6$) have TR and R_{TTP}.

4 In the service provider message M_{sp2} to the user, Resp $_5$ and Resp $_6$ have SP_s.

The suggested protocol prevents the attacker from knowing which messages have been transmitted by the same user simultaneously. It also has some security measures that are simple to verify. Users and service providers are authenticated via the Resp3 and Resp6 protocols, both implemented in the Java programming language.

VII. CONCLUSION

By conducting an evaluation, AVISPA determined that the ELTPA protocol authentication mechanism for the cloud environment met all requirements. The results of the test revealed that it is secure against a variety of various forms of assaults. Many authentication techniques for emerging computing paradigms such as edge/cloud computing were designed without considering the device's mobility. For example, in specific systems, such as the Internet of Vehicles, the user can only authenticate at one or more edge/fog nodes before proceeding. In cloud computing, an anonymous authentication mechanism is suggested to be utilized to secure information between users. This approach is more secure than the other authentication methods currently available. It is proposed in this study that a conditional authentication mechanism be employed in cloud computing to detect the genuine

identity of the phishing entities, which is currently unavailable. It has the capability of detecting and rescinding the credentials of hacked persons from the cloud. The goal of this study is to build an unknown batch authentication mechanism capable of dealing with high numbers of users. It will simplify the authentication process for large-scale networks, which would be beneficial.

VIII. REFERENCES

[1] Ku W-C, Chuang H-M, Chiang M-H, Chang K-T, "Weaknesses of a multi-server password authenticated key agreement scheme," in Proceedings of 2005 national computer symposium, 2005, pp. 1-5.

[2] Amin R, Kumar N, Biswas G, Iqbal R, Chang V. A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment. Future Gen Comp Syst. 2018;78:1005-1019.

[3] Babu, S. Dilli, and Rajendra Pamula. "An Effective Block-Chain Based Authentication Technique for Cloud Based IoT." International Conference on Advances in Computing and Data Sciences. Springer, Singapore, 2020.

[4] He D, Zeadally S, Kumar N, Wu W. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures. IEEE Transac Inform Foren Sec. 2016;11(9):2052-2064.

[5] Fan K, Luo Q, Zhang K, Yang Y. Cloud-based lightweight secure RFID mutual authentication protocol in IoT. Inform Sci. 2019:1-11.

[6] Madhusudhan R, Nayak CS. A robust authentication scheme for telecare medical information systems. Multimed Tools Appl. 2019; 78(11):15255-15273.

[7] Arasan, Anakath, et al. "Computationally efficient and secure anonymous authentication scheme for cloud users." Personal and Ubiquitous Computing (2021): 1-11.

[8] Mall P, Bhuiyan MZA, Amin R. A lightweight secure communication protocol for IoT devices using physically unclonable function. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer; 2019:26-35.

[9] Ayub, Muhammad Faizan, et al. "Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology." Digital Communications and Networks 7.2 (2021): 235-244.

[10] Li L-H, Lin L-C, Hwang M-S. A remote password authentication scheme for multiserver architecture using neural networks. IEEE Trans Neural Netw. 2001;12(6):1498-1504.

[11] Wazid M, Das AK, Bhat V, Vasilakos AV. LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment. J Net Comp App. 2020;150:1-19.

[12] Xue K, Hong P, Ma C. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. J Comp Sys Sci. 2014;80(1):195-206.

[13] Yu Y, Hu L, Chu J. A secure authentication and key agreement scheme for iot-based cloud computing environment. Symmetry. 2020; 12(1):1-16.

[14] Zargar, Sadra, Ali Shahidinejad, and Mostafa Ghobaei-Arani. "A lightweight authentication protocol for IoT-based cloud environment." International Journal of Communication Systems 34.11 (2021): e4849.

[15] J.Nageswara Rao ,Veeraiah D , Dr Joel Sunny Deol G , Dr. Rajendra Kumar Ganiya, SA , Suneetha Bulla , Assefa Alene, Energetic And Valuable Path Compendium Routing Using Frustration Free Communication Dimension Extension Algorithm In Manet, Wireless Communications and Mobile Computing, Science Citation Index Expanded (SCIE)-accepted-2022

[16] J. Nageswara Rao ,Ranga Swamy Sirisati, C. Srinivasa Kumar, A. Gautami Latha, Kanusu Srinivasa Rao ,B. J. D. Kalyani , A framework for effective utilization of cloud resource and optimal scheduling strategy with complex cloud resource using whale genetic optimization, Soft Computing

https://doi.org/10.1007/s00500-021-06642-z,Science Citation Index Expanded (SCIE)-accepted-2022.

[17] J.Nageswara Rao, Rajendra Kumar G, Veeraiah Duggineni, Suneetha Bulla, , J. Sunny Deol . G,Efficiency Evaluation of HRF mechanism on EDoS attacks in Cloud Computing Services, International Journal of Ad Hoc and Ubiquitous Computing, DOI: 10.1504/IJAHUC.2022.10041784, Science Citation Index Expanded (SCIE),2022.

[18] J.Nageswara Rao, Babu Rao Markapudi, Kavitha Chaduvula,Indira DNVSLS3 , Joel Sunny Deol Gosu, An improved deep convolutional neural network for classification of breast cancer images using artificial fish school algorithm, Soft Computing, DOI: 10.1007/s00500-021-06684-3, Science Citation Index Expanded (SCIE)-accepted-2022.

[19] J. Nageswara Rao, P. Satyanarayana, T. Mahalakshmi, P. Rama Koteswara Rao, AdlinSheeba, JampaniRaviand, "Enhancement of Energy Efficiency and Network Lifetime Using Modified MPCT Algorithm in Wireless Sensor Networks", Journal of Interconnection Networks (2022)

[20] J Nageswara Rao, S Sai Kumar, AnumalaReethika Reddy, B Sivarama Krishna, Ajmeera Kiran, "Privacy Preserving with Modified Grey Wolf Optimization Over Big Data Using Optimal K Anonymization Approach", Journal of Interconnection Networks, Pages 2141039 (2022)

[21] J.Nageswara Rao, BhupalNaik, G Sai Lakshmi, V Ramakrishna Sajja, D Venkatesulu,"Driver's Seat Belt Detection Using CNN", Turkish Journal of Computer and Mathematics Education,Vol.12 No.5 (2021), 776-785

[22] J Nageswara Rao, Dr R Satya Prasad, "An Enhanced Novel Dynamic Data Processing (ENDDP) Algorithm for Predicting Heart Disease in Machine Learning", International Journal of Scientific Research in Computer ScienceEngineering, and Information Technology (IJSRCSEIT), ISSN, Pages 2456-3307 (2021)

[23] J Nageswara Rao, Dr R Satya Prasad, "An Ensemble Deep Dynamic Algorithm (EDDA) to Predict the Heart Disease", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN, Pages 2394-4099 (2021)

[24] J Nageswara Rao,Dr KattaSubba Rao, ChMadhuBabu, GovinduSurla,"SOFTWARE DEFECT PREDICTION TO IMPROVE SOFTWARE QUALITY USING MACHINE LEARNING APPROACH", Turkish Journal of Physiotherapy and Rehabilitation, Volume- 32, Issue- 3, Pages 6916-6922 (2021)

[25] J Nageswara Rao,Avantika Tiwari, SundeepSaradhiKanthety, DNVSLS Indira, "AN ENHANCED USAGE PATTERN HYBRID METHOD FOR MINING HUI SETS FROM LARGE DATASETS", Turkish Journal of Physiotherapy and Rehabilitation, Volume- 32, Issue-3, Pages 6505-6509 (2021)

[26] J Nageswara Rao,ChintalapudiSowndaryaLahari, B Sivarama Krishna,PERSONALIZED MEDICINE PREDICTION USING DEEP LEARNING APPROACH", Turkish Journal of Physiotherapy and Rehabilitation, Volume- 32, Issue-3, Pages 6492-6496 (2021)

[27] J Nageswara Rao,AnumalaReethika Reddy, NV Naik, "AN IMPROVED K-MEANS ADAPTIVE CLUSTERING METHOD ON LARGE DATASETS", Turkish Journal of Physiotherapy and Rehabilitation, Volume- 32, Issue-3, Pages 6497-6504 (2021)

[28] J Nageswara Rao, "CARDIOVASCULAR DISEASE PREDICTION USING MACHINE LEARNING TECHNIQUES", Turkish Journal of Physiotherapy and Rehabilitation, Volume- 32, Issue-3, Pages 6875-6880 (2021)

[29] J. Nageswara Rao, Dr.RambabuBusi, Dr. G Rajendra Kumar, U. Surya Kameswari, Contentimage Retrieval Based on using open Computer Vision and Deep Learning Techniques", International Journal of Advanced Science and Technology,Volume29Issue03Pages5926 - 593 9, (2020)

[30] J. Nageswara Rao, and D. Veeraiah "An Efficient Data Duplication System based on Hadoop Distributed File System", 2020 International Conference on Inventive Computation Technologies

(ICICT), 2020, pp. 197-200, doi:10.1109/ICICT48043.2020.9112567, Scopus/Web of Science.

[31] J. Nageswara Rao,RadhaMothukuriSuneetha Bulla, "Analysis of Unsupervised Dicretization Methods Impact on C4.5 Classification", International Journal of Advance d Science and Technology, Volume-29, Issue-5, Pages 802 – 815 (2020)

[32] J. Nageswara Rao, B. ShyamalaBhanu Prakash Doppala, M. Gargi, A. Nalini, "Prognosis of Cardiovascular Disease Using Machine Learning Algorithms", International Journal of Future Generation Communication and Networking, Volume- 13, Isssue-3, Pages 709 – 716 (2020)

[33] J. Nageswara Rao,KalamSwathi, M. Gargi, KhadriLalitha Vani Sri, B. Shyamala, "Human Activities Recognition Using OpenCV and Deep Learning Techniques", International Journal of Future Generation Communication and Networking, Volume-13, Issue- No. 3, Pages 717 – 724 (2020)

[34] J. Nageswara Rao, D. Veeraiah, "A Review on Coronavirus (COVID-19) Impact on the Public", International Journal of Future Generation Communication and Networking, Volume-13, Issue-3, Pages 314 – 318 (2020)

[35] J Nageswara Rao, Y DurgaMalleswari, K Teja Krishna, CH Vishnu Sai, Y Ramya Sri, "Twitter Sentiment Analysis for Different Business Applications", Journal of Advanced Research in Dynamical and Control Systems,Vol. 12, Issue-02, (2020)

[36] J.Nageswara Rao, H.SudhakarRambabuBusi, G Rajendra Kumar, "A New Analysis on Assessment of Sentiments Using EEG Signals and BCI", Journal of Advanced Research in Dynamical and Control Systems, Volume-12, Issue 2, Pages 1044-1047 (2020)

[37] J Nageswara Rao, BSivarama Krishna, Bhanu Prakash Doppala, S Phani Praveen, G Joel Sunny Deol, B Shyamala, "Advanced Adaptive Pattern Approach to Mine High Utility Item Sets from Large Transaction Databases", International Journal of Advanced Science and Technology,Vol. 29, No. 5, (2020), pp. 9435-9440

[38] J Nageswara Rao, KhadriLalithaVaniSri, B Shyamala, M Gargi, KudaravalliDeepika, "A Modern Optimized Fuzzy C-Means Clustering Using Machine Learning for Data Clustering",International Journal of Advanced Science and Technology, Vol. 29, No. 5, (2020), pp. 9417-9428

[39] J. Nageswara Rao, K Ruth Ramya, B Manjula Josephine, VenkataVara Prasad Padyala, KhadriLalithaVaniSri, "An Efficient and Secured Biometric Authentication for IOT Using Face Recognition", Journal of Critical Reviews, Volume-7, Issue-18, Pages 1016-1028 (2020)

[40] J.Nageswara Rao,KhadriLalithaVaniSri, B. Shyamala,M.Gargi, KudaravalliDeepika, "A Modern Optimized Fuzzy C-Means Clustering Using Machine Learning For Data Clustering", International Journal of Advanced Science and Technology,Volume 29, Issue-5, Pages 9417-9428 (2020)

[41] J. Nageswara Rao,D. Veeraiah"Use of Clustering Sentiments for Opinion Mining: An Experimental Analysis", Conference-Advances in Intelligent Systems and Computing 933, Pages 625-632 (2020)

[42] J Nageswara Rao, Mr V KanthaRao, Mr VenkataNareshMandhala, SGLS Ratna, Y Nagateja, K Hoshitha "Stock Market Prediction and Analysis using Machine Learning Algorithm-Random Forest Classifier (RFC)",International Journal of Advanced Science and Technology,Vol. 29, No. 7, (2020), pp. 1095 – 1103

[43] J. Nageswara Rao, "A Review on Data Mining & Big Data, Machine Learning Techniques", International Journal of Recent Technology and Engineering, Volume-7, Issue-6S, Pages914-916, (2019)

[44] J.NageswaraRao ,S.Govindu, K.SundeepSaradhi, A.Sudhakar, Ch.SrinivasaRao, "Advanced Ensemble ACGCTechnique using Image Segmentation Model", International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Issue-6S2, Pages 796-799 (2019)

[45] J.Nageswara Rao,Dr.M.Babu Reddy Dr.P.Ashok Reddy, "Design of Internet of Things (IoT) Sensors and Cloud Computing for Health Care Applications", Journal of Advanced Research in Dynamical and Control Systems – JARDCS, Volume 10, Issue-10, Pages 239-244 (2018)

[46] J Nageswara Rao, Mr Aryan Chandrapal Singh, "A Novel Encryption System Using Layered Cellular Automata", International Journal of Engineering Research and Applications, Vol. 2, Issue 6, November- December 2012, pp.912-917

[47] J Nageswara Rao, Mrs P Balaramudu M Tech, "Fingerprint Identification and Verification System using Minutiae Matching" (2012)

Cite this article as :

Kalluri Rama Krishna, C. V. Guru Rao, " ELTPA : EFFECTIVE LIGHTWEIGHT THIRD-PARTY AUTHENTICATION PROTOCOL FOR CLOUD INTEGRITY AND SECURITY, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 9, Issue 1, pp.276-291, January-February-2022.
Journal URL : https://ijsrset.com/IJSRSET22921