AMAP: ADAPTIVE MULTILEVEL AUTHENTICATION PROTOCOL ON CLOUD ENVIRONMENT

[1]BHARATI AINAPURE, [2]DEVEN SHAH , [3]A. ANANDA RAO

[1]Reseach Scholar, JNTUA, Computer Science & Engg., Anantpur, India

[2]Profssor, TCET, Department of Information & Technology, Mumbai, India

[3]Profssor, JNTUA, Department of Computer Science & Engg., Anantpur, India

E-mail: [1]ainapuressa@gmail.com, [2]sir.deven@gmail.com, [3]akpogu@gmail.com

ABSTRACT

Cloud computing is an emerging technology that allows users to access the computational data through virtual machines on a cloud. Since the technology is based on the sharing of resources, lack of security is a major issue. This paper proposes a new authentication protocol, with an intention to provide secure access to computational data through virtual machines. The proposed protocol works on mutual and multi-level authentication between the user and the server in a cloud environment. This multi-level authentication protocol provides security, considering multiple parameters like OTP, session password, and so on. The protocol includes two phases: Registration and Authentication. At first, the cloud user and the server are registered under Authorization Centre (AC), which authenticates the user and the server using four different messages. The verification of the user is on the basis of hashing function and EC, following a six level authentication process to allocate the virtual machines to access the computational data in the cloud. This protocol provides resistance against Server spoofing attack, stolen verifier attack, Password guessing attack, Impersonation attack and replay attack. Thus, the protocol allows the cloud user to gain a secured access offering robustness with the utilization of Elliptic Curve Cryptography (ECC) and hashing function. The experimental results show that the proposed protocol could provide 75.58% genuine user details, 78.49% attacker details, and 77.03% accuracy, in the comparative analysis made with the approach of Vanga Odelu et al. This comparison shows that it had better performance in providing authentication than the considered existing technique.

Keywords: *Authentication, OTP, Session password, ECC, Hashing, Registration, Protocol, Cloud.*

1. INTRODUCTION

In IT field, cloud computing has become a rapid developing technology from a guaranteed business perception [1]. It refers to the integration of hardware and software that provides various services to the clients through the Internet. Some kinds of services that cloud computing offers to the end users are software services, platform services, and infrastructure services [2]. The concept virtualization provides resources to simulate physical devices and, thereby, offering various services. But, in cloud computing, virtualization is one of the challenges during the organization of a cloud computing system. The cloud can be categorized into three, namely, private, public and hybrid cloud, based on the data it has [3]. This technology satisfies multiple end users by enhancing the demands of users to access the resources available via the Internet [4]. Even though it is advantageous, it offers several issues related to security and reliability [5]. Security has become a critical problem affecting the growth of this technology [6]. Hence, it is important to design techniques for authentication, so as to provide security [7]. Authentication is the two party identity management scheme, in which participating parties need to prove the trustworthy relation with each other. Authentication identifies the legitimate users. In computer world authentication is very simple, as giving the identity to the physical local equipment to gain the access. In case of cloud providing the identity is little bit difficult, because once the company decides to go with the cloud, then the company will going to lose the control over the data, whatever they wanted to store on cloud. This is termed as lack of control. The cloud providers may spatially have different servers to provide services to users. But to get the services from cloud, the users want the smooth and continue security from cloud providers. So cloud providers normally adopt the cryptographic techniques to provide security to the users. Authentication is one of the cryptography methods to prove the identity between the user and cloud provider. It guarantees the secured initial phase of communication between the user and cloud provider. Many classical authentication mechanisms like private key cryptography, public key cryptography, and single sign on, password based protection are available in theory and are practice to provide security to the cloud users. These classical mechanisms work well in private cloud environment where users of the cloud are within the organization. But public cloud has different scenario where multiple users are accessing the cloud resources over the internet. In such situation it is very difficult to provide security for the resources over the cloud. One of the solutions to this is to create an authentication protocol. Various authentication protocols are developed to have control over the attackers from using cloud resources so as to solve security issues in the cloud [8]. Depending on the service that supports security, the server generates a secret key as soon as a user requests for a service to the server.

Some of the attacks like Denial of Service (DOS) attacks, malware injection attack, side channel attack and authentication attack, lead to several security issues in the cloud [9]. The protocol utilizes various security parameters like OTP, Session Password, and so on, for the authentication. Apart from accessing the services in cloud computing, the users also update the services by modifying, deleting, inserting, etc. However, most of the authentication protocols presented in the state-of-the-art considered only static data files and the dynamic update is insecure in most of the authentication applications used [12-20].

Key Contribution:

This paper proposes an authentication protocol, AMAP that works on mutual and multi-level authentication between the user and the server in the cloud environment to reduce cache-based side channel attacks. This multi-level authentication protocol provides security considering multiple parameters like OTP, session password, number of cache access, and so on. The protocol includes two phases: Registration, Authentication. At first, the cloud user and the server are registered under Authorization Centre (AC), which authenticates the user and the server using four different messages. The verification of the user is on the basis of hashing function and ECC following a six level authentication process. Data confidentiality, data integrity, multi-level authentication, and mutual authentication are the properties used that offer security to the proposed protocol. The proposed novel authentication protocol is to designed with respect to cloud environment to lessen attacks such as password guessing, Denial of service etc., and allocate virtual machines to users with the utilization of various security parameters, such as OTP, session password, hashing function, ECC, etc.

The organization of the paper is as follows: Section 2 describes the existing techniques developed for authentication stating the challenges and problems. Section 3 provides the cloud setup. The proposed authentication protocol for the cloud to securely allocate virtual machines to user is explained in under section 4. Section 5 demonstrates the experimental results of the proposed method and section 6 concludes the paper.

2. RELATED WORK

This subsection deliberates the literature associated with the authentication protocols and techniques used to mitigate the few authentication related attacks. Here, the research papers deal with the protocols for securing cloud privacy issues.

Hong Liu et al. [12], developed a protocol, Shared Authority based Privacy-preserving Authentication protocol (SAPA) to solve the privacy problem for cloud storage. Some of the features of SAPA were, i) Anonymous access request matching mechanism had provided authority in shared access by considering the security and privacy features, ii) It had access control based on attributes so that the user could access only in their own data fields, iii) data sharing was possible among multiple users, as the cloud server utilized proxy re-encryption mechanism. Moreover, a model, called Universal Composability (UC), was designed to show that SAPA had design correctness in the theoretical analysis. This suggested that the protocol can be used for various multi-user collaborative cloud applications. However, SAPA adopts an identity token based authentication, and there is no interoperable capability between the tokens.

Sarah Abughazalah et al. [13], developed a protocol with an assumption that the data were prone to privacy invasion and attacks, as the servers in the cloud might be insecure. It utilized Xie et al. protocol i.e. cloud-based Radio Frequency Identification (RFID) authentication, such that the cloud data were preserved, and cannot be compromised. This protocol had attained mutual authentication between all the elements like, cloud server, a reader and a tag, which were involved in the communication. The protocol was analyzed both formally and informally with the utilization of a privacy model and CasperFDR. The major limitation of this protocol is that it is susceptible to location tracking of attack, and impersonation attack.

Ta-Chih et al. [14], had designed a smart card based authentication scheme combined with an access control function to preserve users' data and information. The scheme was based on the objectives as follows: Confidential data transmission: It considered the confidentiality issue during user login or during the transmission of data to/from the cloud environment. Smart card authentication mechanism: The protocol designed a smart card authentication scheme between the cloud server and user's equipment so that authorized users could login to the multimedia cloud environment. Combined multimedia cloud access procedure: This access control mechanism ensured proper data access by the corresponding user. A home group privacy and content preservation mechanism: Even though the multimedia cloud was suitable for family use, privacy and control in media content were essential. Here, a group-role based access control scheme was used combined with the authentication mechanism to ensure privacy and content control protect mechanism. However, the technique has various disadvantages as follows: i) User management issue, ii) Failure to consider security in channel issue, iii) Failure in providing solution for the lost smart card phase, iii) The verification process requires large consumption of cloud resources.

Marwan Darwish et al. [15], presented a cloud-based authentication protocol that was aware of both internal and external DoS attackers to protect the cloud resource from attackers. It used a multilevel adaptive technique to state the efforts of the participants in the protocol. This could identify the valid requests of a user keeping them at first in the authentication process queue. The design was made such that the cloud servers were aware of the threats due to DoS attacks. Even though the protocol provides authentication by detecting the risks at an early stage, it did not consider security in side-channel problems.

Wei Liu et al. [16], designed a Yoking-Proof-based Authentication Protocol (YPAP) for authenticating the devices in the cloud environment. Mutual authentication was provided between a smart phone and two wearable devices using a physical unclonable function and lightweight cryptographic operators. Mutual authentication along with the yoking-proofs establishment performs simultaneous verification. It also performed Rubin logic-based security, formal analysis to ensure the theoretical design correctness in YPAP. Thus, YPAP was known to be flexible for lightweight wearable devices in various IoT applications. The drawback is that the verification process is complex.

Safiriyu Eludiora., et al. [17], proposed a layered protocol called U_IDM (User identity management) to secure all stakeholders in cloud computing. This protocol is developed to provide security based on answering some questions being asked by stakeholders and developers based on authentication, authorization, encryption, key management, etc. Here AAA i.e. authentication, authorization and accounting are considered in the development of algorithms. Authors check the attributes those are given by the stakeholders, character by character to provide security. Even though the authors proposed the layer wise security but much of performance overhead is incurred in the development of this protocol.

Nimmy K., et al [18] proposed mutual authentication scheme to share the secret key between client and server. This scheme also uses steganography as an additional encryption scheme. The secret key is divided in two parts and part of the key are kept with server and client combined to form one complete key. Mutual authentication is achieved by sharing steganography and a secret key among both. It also includes out of band authentication to provide additional security. Even though this protocol provides resistance against attacks such as replay attack, denial of service attack and man in the middle attack, but it is unable to handle an offline password guessing attack.

C. Vorugunti., et al. [19] proposed low cost steganography authentication scheme. The proposed scheme is divided into four stages:

Registration stage, Login stage, Mutual authentication stage and Password change stage considering the server, client and communication networks are trustworthy. Author in this paper tried to take off the resource consuming by encryption, decryption and stegano operations from client side and server side load. Even though many attacks like replay attack, man in the middle attack, etc. are reduced, but due many levels of message passing between client and server reduced the performance of the proposed work.

3. SYSTEM MODEL

This section presents the system model for the cloud as architecture which is shown in figure 1. The objective of this system model is to offer a trusted service by launching virtual machine to access the computational data. This cloud model consists of three main components; Physical servers P^M , an Authentication Center (AC), and User U

Physical Server: It is one in which 'n' number of multiple virtual machines are created to share the resources among multiple users. Let $P^M = \{P_1^M, P_2^M, \ldots, P_n^M\}$ denotes a set of physical machines, where, n is the total number of physical machines present in the cloud. Each physical server consists of several virtual machines $V^M = \{V_1^M, V_2^M, \ldots, V_p^M\}; 1 \le j \le p$, where, p is the number of virtual machines available on a server.

The Authorization Center (AC): authorizes the user and the server before a service is provided.

User: Group of people who are allowed to access computational data in a cloud environment after an authentication.

Let $U = \{U_1, U_2, \ldots, U_m\};\ 1 \le k \le m$ represents different users who access the cloud, where m is the number of users.

Once AC authorizes a user, it provides the access to computational data requested by the user by launching virtual machine on AC such that an attacker cannot obtain sensitive information regarding the user.

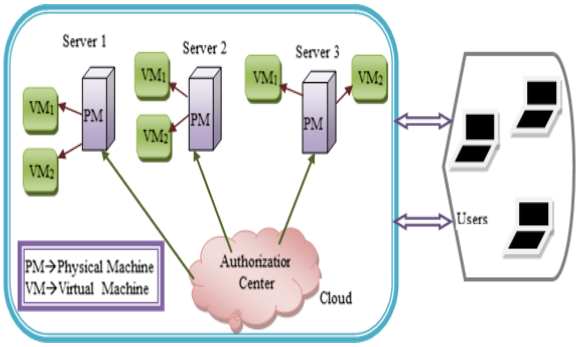


Figure 1. Cloud data storage model

4. PROPOSED AMAP BASED SECURITY

The proposed protocol that reduces authentication attacks for the security in the cloud is explained in this section. The protocol works in two phases, 1. Registration phase and 2. Authentication phase. Figure 2 illustrates the block diagram of the proposed authentication protocol.

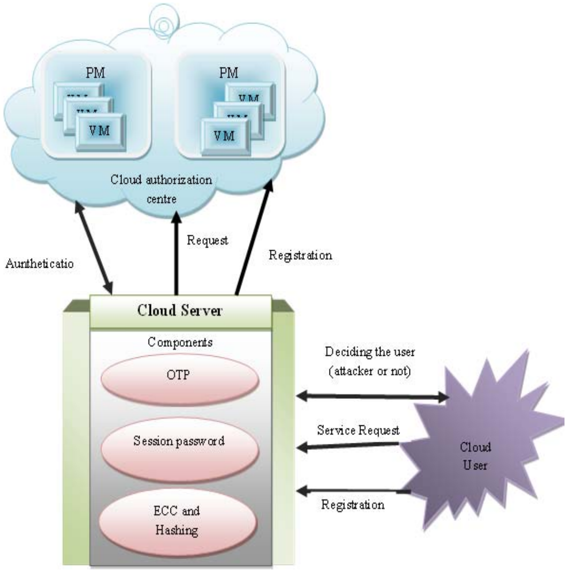


Figure 2. Block diagram of proposed multi-level authentication protocol

Different symbols that are used in this work are listed in Table 1 along with its description as shown below.

Table 1. Notations with description

Symbol	Description
S_{ID}	Server ID
S_{PW}	Server Password
S_{ePW}	Session Password
K_{AC}	Authorization Center Key
K_S	Server Key
K_U	User Key
U_{ID}	User ID
U_{PW}	User Password
$P(K)$	Public Key
$\bullet$	Embedding Operator
Θ	Extraction Operator

The following sections elaborate the two phases of the protocol in providing authentication for the security against attackers.

4.1 Registration

The first step in the protocol is registration of the user and the server. Only the registered user and server are considered as authenticated, where the AC permits the server to serve the resource required for the user. In registration, the server and the AC share the identity so as to register the cloud server in AC through a secured channel. The steps involved in the user and the server registration are as follows: Each server has its own ID and password, represented as, S_{ID} and S_{PW}, which are stored in AC for the authorization. AC generates a session password S_{ePW} by applying a hash function as given below. Here the hashing function is used to turn the message or text into a fixed string of digits to provide the security. When hashing is used, it makes the attacker nearly impossible to derive the original test from the string. This work uses a one way hashing function to create digital signatures which in turn identify and authenticate the sender and messages.

$$S_{ePW} = h[K_{AC} \| r \| S_{PW}] \qquad (1)$$

Where, $h[.]$ is the hash function, K_{AC} is the encryption key of AC, r is a random number and S_{PW} is the server password.

Then, AC generates the server key by hashing its own key K_{AC} along with the server ID as follows,

$$K_S = h[K_{AC} \| S_{ID}] \qquad (2)$$

The session password and the secret key generated in AC are submitted to the server, which stores the server key K_S. Then, the server generates an OTP based on the device number DN of the user and check if the session password matches. OTP-based mechanism utilized in the proposed protocol can easily overcome the DOS attacks, even though the users access their system in different environments. Then, AC compares S^*_{ePW} with S_{ePW} and if both are equivalent, i.e. $S^*_{ePW} = S_{ePW}$, the server is registered.

To verify whether the user is a registered user or not, the generated OTP is sent to the user. The server generates a key by adopting the user ID stored in the server as,

$$K_U = h[K_S \| U_{ID}] \qquad (3)$$

Where, U_{ID} is the user ID.

The user stores its private key K_U and forwards the OTP to the server. The user is identified as registered if the server finds $OTP^* = OTP$. Figure 3 illustrates the registration phase where the user and the cloud server are registered.

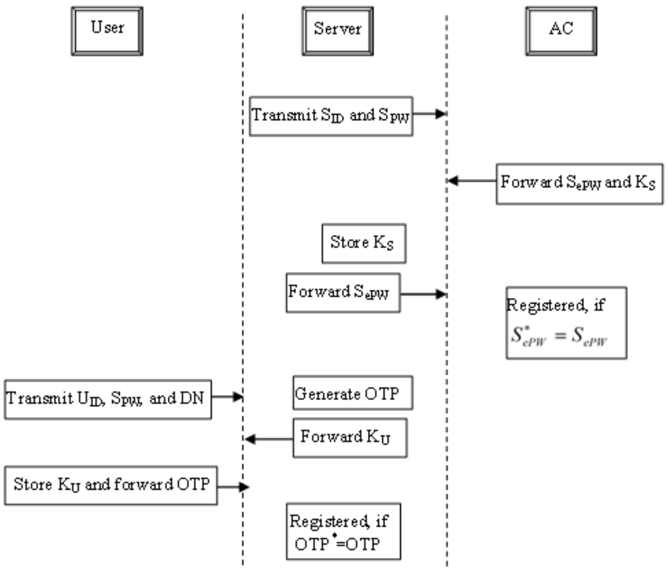

User
Server
AC
Transmit S_{ID} and S_{PW}
Forward S_{ePW} and K_S
Store K_S
Forward S_{ePW}
Registered, if $S^*_{ePW} = S_{ePW}$
Transmit U_{ID}, S_{PW}, and DN
Generate OTP
Forward K_U
Store K_U and forward OTP
Registered, if OTP^*=OTP

Figure 3. Sequence Registration Phase

4.2 Multi-level Authentication

The second phase is the authentication phase, which performs mutual and adaptive verification using six levels. Once it registers both the user and the server, it executes authentication based on four different messages using various functions via the communication channel. The first two levels of verification utilize the hash function. Initially, the user forwards a message to the server by concatenating the user ID with the hashed user password, as given below,

$$X_1 = [U_{ID} \,||\, h(U_{PW})] \tag{4}$$

Where, U_{ID} is the user ID and U_{PW} is the user password.

Then, the server computers X_1^* by hashing U_{PW} based on the length of U_{PW} obtained from the user as in the following equation,

$$X_1^* = [U_{ID} \,||\, h^*(U_{PW})] \tag{5}$$

Once the server finds $X_1 = X_1^*$, it is considered as the first level of verification.

The server by hashing the server password and then concatenating with the IDs of server and user, creates a message as,

$$X_2 = [S_{ID} \,||\, U_{ID} \,||\, h(S_{PW})] \tag{6}$$

To calculate X_2^*, AC utilizes the stored S_{PW} that is obtained based on its length and applies the hashing function, i.e. $h^*(S_{PW})$, as given below,

$$X_2^* = [S_{ID} \,||\, U_{ID} \,||\, h^*(S_{PW})] \tag{7}$$

When $X_2 = X_2^*$, it is assumed that the server has cleared the second level of authentication.

The third and the fourth level of authentication are based on stegno function. Let Y_1 be a message computed in AC by embedding the server key with the server ID, as follows,

$$Y_1 = [S_{ID} \bullet K_S^*] \tag{8}$$

Where, $\bullet$ is the embedding operator.

The message is then transmitted to the server, where it evaluates the server ID by extracting Y_1 and the server key.

$$S_{ID}^* = Y_1 \Theta K_S \tag{9}$$

Where, K_S is the server key and Θ is the operator representing extraction.

If the server find $S_{ID} = S_{ID}^*$, it is the authentication level three. Then, the server embeds the user ID with the user key to compute the message Y_2 as,

$$Y_2 = [U_{ID} \bullet K_U] \tag{10}$$

The above message is then forwarded to the user, where it performs the extraction on Y_2 and K_U.

$$U_{ID}^* = Y_2 \Theta K_U \tag{11}$$

When the evaluated ID matches with that in user, i.e. $U_{ID} = U_{ID}^*$, it forms the fourth level of verification.

The final two verification levels follow an XOR-based authentication. It adopts an encryption technique, called ECC, for privacy preservation. Main benefits of elliptic curves rather than cryptographic algorithms based on finite fields, such as RSA or DSA include a smaller size of key for security equivalence, the possibility to implement without crypto processor, and the faster execution in some cases when using a crypto processor.

The user computes a message W by encrypting the user password using ECC and then applies XOR operator over the hashed keys, as given in equation (12),

$$W = ECC[U_{PW}] \oplus h(K_U) \oplus h(P(K)) \tag{12}$$

Where, $P(K)$ is the public key of the user and $ECC[U_{PW}]$ is the ECC applied user password.

The user forwards this message to the server, where it computes W_1 as,

$$W_1 = W \oplus h(P(K)) \tag{13}$$

Where, $h(P(K))$ is the hashed user public key. Then, the server evaluates $ECC(U_{PW})^*$ to check if it matches with $ECC(U_{PW})$, to verify whether the user is a registered user and thus, creating the fifth level of authentication.

$$ECC(U_{PW})^* = W_1 \oplus h(K_U) \tag{14}$$

To execute the final authentication level, the server transmits a message, which is computed using ECC applied S_{PW}, hashed server key and hashed public key, to the AC as given below,

$$V = ECC[S_{PW}] \oplus h(K_S) \oplus h(P(K)) \tag{15}$$

$$V_1 = V \oplus h(P(K)) \tag{16}$$

The verification is done here by computing $ECC[S_{PW}]^*$ to check if it matches with $ECC[S_{PW}]$ using equation (17).

$$ECC[S_{PW}]^* = V_1 \oplus h(K_S) \qquad (17)$$

The mutual authentication phase performed in six levels of verification is depicted in figure 4 to allocate virtual machine in a cloud environment to access the data.

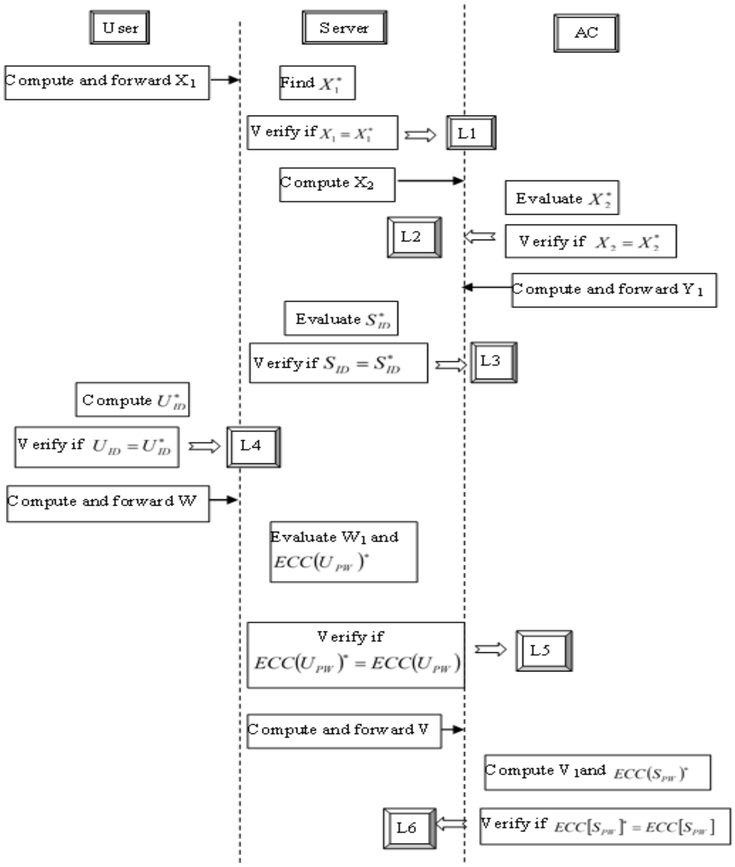


Figure 4. Flow of Authentication Phase

5. RESULTS AND DISCUSSION

This section presents the results of the protocol providing cloud security to offer virtual machines to user. Moreover, the experimental setup and the performance of the proposed approach, evaluated in a comparative analysis are discussed in the following subsections.

5.1 Experimental set up

The simulation of the proposed technique is executed in a system operated with Windows 10 having the following configurations: Intel processor of CPU 2.16 GHz, memory of 2GB and 64-bit OS. AC and cloud servers are simulated using cloudsim tool, while, the cloud users and the authentication of cloud users are programmed using JAVA and interfaced with cloudsim. A random model considering a specific number of attackers is also simulated. Depending on the multiple parameters considered, the behavior of the attackers will be simulated.

Setup 1: The cloud setup 1 consists of five PMs that consist of 12 VMs through which the users can access the cloud data.

Setup 2: The cloud setup 2 is designed with 10 servers and 24 VMs for the cloud data access via the internet.

5.2 Method Employed for Comparison

The level of efficiency of an algorithm can be checked with that of an existing algorithm to estimate how far the method is better than the previous. The proposed authentication approach is compared with a multi-server authentication approach, Vanga Odelu et al. [11]. In [11], an authentication protocol using biometrics-based smart card and ECC was developed for the security. This method is taken here as the existing approach for the comparison with the proposed multi-level authentication protocol.

5.3 Performance Comparison

The performance of the proposed adaptive authentication protocol is explained in this section with the simulation results obtained for the cloud setup. These are discussed based on analyses of simulation, as deliberated below.

5.3.1 Evaluation metrics

The proposed AMAP protocol for authentication considers three parameters, such as number of genuine/authenticated users, number of attackers, and accuracy, to evaluate its performance, as defined below,

Number of genuine users: From an assumed percentage of attackers in the network, the number of genuine users accessing the cloud over a simulation time can be defined as follows,

$$N_G = \frac{N_g}{T_G}$$

Where, N_g is the number of genuine users identified over a time and T_G is the total number of genuine users in the cloud.

Number of attackers: Similarly, the number of attackers in the cloud can be estimated using the representation given below,

$$N_A = \frac{N_a}{T_A}$$

where, N_a is the number of attackers identified over a time and T_A is the total number of attackers in the cloud.

Accuracy: The well-known parameter to evaluate the degree of performance is accuracy, which defines the closeness of a value measured to a standard value as,

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

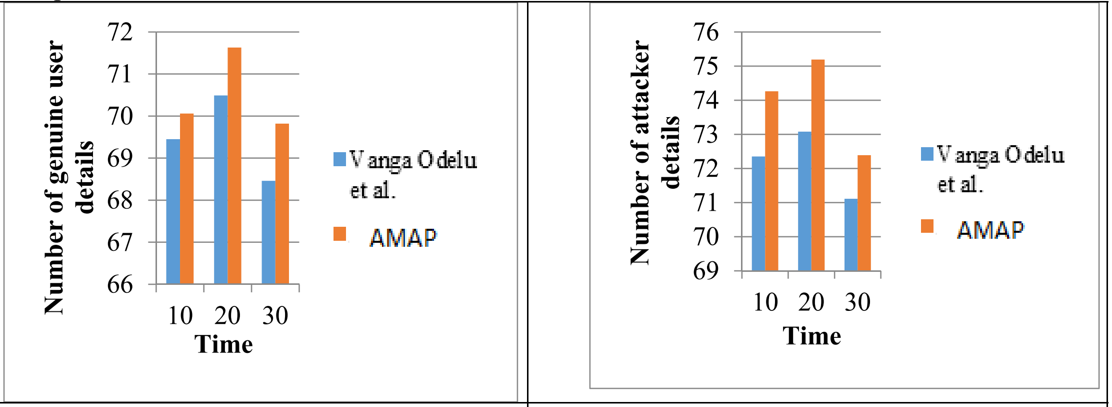
where, TP is True Positive, TN is True Negative, FP is False Positive, and FN is False Negative.

5.3.2 Simulation analysis

In this analysis, the simulation results of the proposed protocol, which are carried out in the two cloud setups are discussed. The results are evaluated based on the three parameters in the proposed as well as the existing biometric-based multi-server protocol.

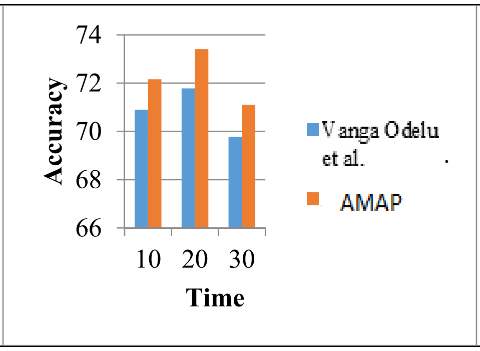
A. For cloud setup 1

Figure 6 presents the estimated details regarding the number of genuine users, attackers, and accuracy for the cloud setup 1. Figure 6.a shows the comparative analysis based on the genuine users details in proposed AMAP and in existing Vanga Odelu et al. protocols for the time instants 10, 20, and 30 sec. The number of genuine user details identified in Vanga Odelu et al. is 69.45%, and 68.46%; and 70.06% and 69.82% in the proposed protocol, at time 10 and 30 sec, respectively. The maximum increment is obtained at time 20 sec, with 70.49% in Vanga Odelu et al. and 71.63% in AMAP, which is 0.0159% more than in the existing protocol. Figure 6.b illustrates the number of attacker details estimated in the comparative analysis, where maximum attacker details are identified at time 20 sec. When Vanga Odelu et al. showed the maximum 73.08% result, AMAP could provide 75.19% result. As the time is kept to its maximum, the details regarding the number of attackers provided is 71.11% and 72.39%, in Vanga Odelu et al. and AMAP. In figure 6.c, the accuracy analysis result is illustrated, where the maximum accuracy of 73.41% is found in AMAP, at time 20 sec, while the existing protocol could attain only 71.78%.



(a) Genuine user analysis

(b) Attacker analysis

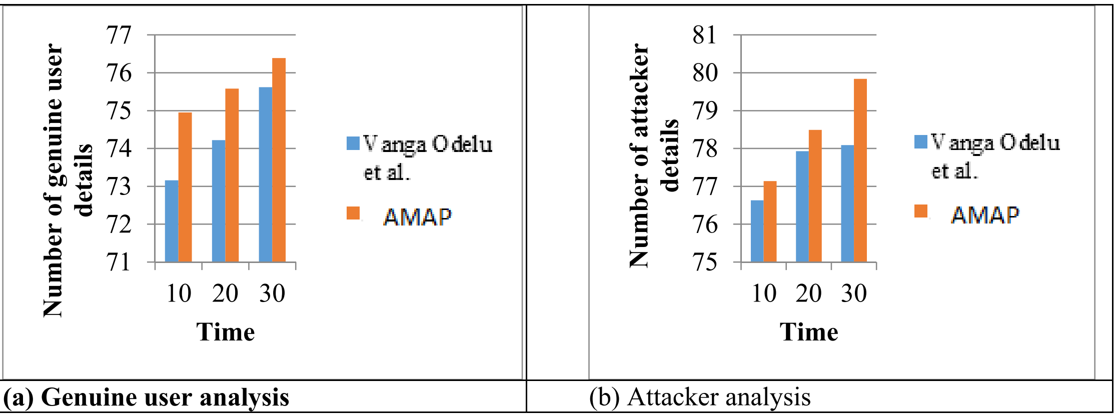


(c) Accuracy

Figure 6. Simulation results for cloud setup 1

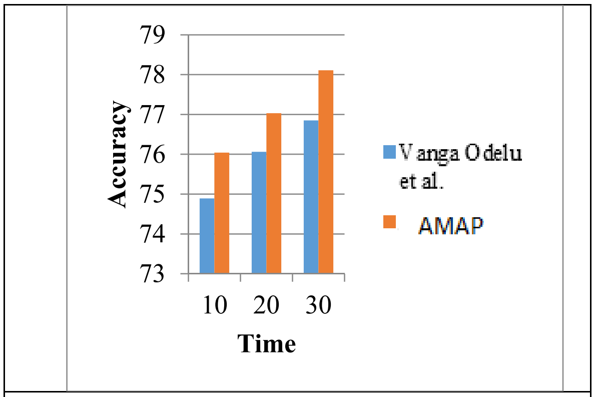
B. For cloud setup 2

The simulation results for the second cloud setup are demonstrated in this section, as in figure 7. Figure 7.a shows the analysis result based on the number of genuine user details, which shows maximum values of 75.62%, and 76.39%, in Vanga Odelu et al. and AMAP, at time limit of 30 sec. In figure 7.b, the details regarding the identified number of attackers at varying time intervals are shown. When Vanga Odelu et al. identified the maximum of 78.09% attacker details at a time instant 30 sec, AMAP could estimate 79.84% attackers. Figure 7.c presents the accuracy analysis graph of the two approaches. Here, the maximum accuracy estimated is 76.85% in Vanga Odelu et al., whereas in AMAP, it is 78.11%. This states that the proposed AMAP approach has 0.016% accuracy more than in the existing authentication protocol.



(a) Genuine user analysis

(b) Attacker analysis



(c) Accuracy

Figure 7. Simulation results for cloud setup 2

5.3.3 Discussion

This section discusses the comparative analysis results, which is obtained for the two cloud setups based on the performance evaluation metrics. Table 3 presents the performance comparative results showing the best results obtained to evaluate the performance of the proposed approach.

Table 3. Performance Analysis

		Vanga Odelu et al.			AMAP		
		T=10	T=20	T=30	T=10	T=20	T=30
Cloud setup 1	Genuine user analysis	69.45	70.49	68.46	70.06	71.63	69.82
	Attacker analysis	72.35	73.08	71.11	74.26	75.19	72.39
	Accuracy	70.9	71.78	69.78	72.16	73.41	71.1
Cloud setup 2	Genuine user analysis	73.16	74.22	75.62	74.95	75.58	76.39
	Attacker analysis	76.63	77.93	78.09	77.14	78.49	79.84
	Accuracy	74.89	76.06	76.85	76.04	77.03	78.11

From the overall performance comparison analysis, the proposed protocol seems to have better performance regarding genuine user details, attacker details, and accuracy, than that of the existing protocol at all the time intervals. However, at time T=20 sec, maximum results are obtained, with 71.63% genuine user details, 75.19% attacker details, and 73.41% accuracy, for the cloud setup 1; and 75.58% genuine user details, 78.49% attacker details, and 77.03% accuracy, for the setup 2. Hence, it can be suggested that the proposed authentication approach offers better result ensuring security.

6. FUNCTIONALITIES COMPARISON WITH EXISTING SYSTEMS:

According to table 2, AMAP protocol provides the mutual authentication by the way of getting confirmation from three parties involved. Also, AMAP protocol requires identity-verification mutually during the authentication. Server spoofing attack resistance is possible with the proposed AMAP protocol as the server wants to prove its identity to authorization center. Stolen verifier attack resistance, Password guessing attack resistance and Provides Session Key (SK)-security are possible because the hashing function and ECC are proved robust against these attacks. The proposed AMAP protocol utilized these mechanisms to provide the proof against these attacks. Impersonation attack resistance and replay attack can be easily achievable through the mutual verification process which is utilized in the proposed AMAP protocol. OTP-based mechanism utilized in the proposed AMAP protocol can easily overcome the DOS attacks even though the users access their system in different environments.

From the table 2, it is observed that the proposed AMAP protocol provides all the considered features, ensuring the security. Thus, it is observed that the proposed authentication protocol outperforms the existing technology in providing security with various functionality features.

Table 2. Functionality Analysis

Features	He-Wang [20]	Vanga Odelu et al. [18]	AMPA protocol
Provides mutual authentication	Yes	Yes	Yes
Requires identity-verification table	No	Yes	Yes
Server spoofing attack resistance	Yes	Yes	Yes
Stolen verifier attack resistance	Yes	Yes	Yes
Password guessing attack resistance	Yes	Yes	Yes
Provides Session Key (SK)-security	No	Yes	Yes
Impersonation attack resistance	No	Yes	Yes
Reply attack resistance	No	Yes	Yes
Man-in-the-middle attack resistance	Yes	Yes	Yes
Provision for revocation and re-registration	No	Yes	Yes
DoS attack resistance	No	Yes	Yes
Dictionary attack	No	No	Yes
Key logger attack	No	No	Yes

6. CONCLUSION

The proposed protocol provides the mutual authentication by the way of getting confirmation from three parties involved. Also, the protocol requires identity-verification mutually during the authentication. Server spoofing attack resistance is possible with the proposed protocol as the server wants to prove its identity to the authorization center. Stolen verifier attack resistance, Password guessing attack resistance and Provides Session Key (SK)-security. OTP-based mechanism utilized in the proposed protocol can easily overcome the DOS attacks. To preserve privacy, encryption using ECC is applied over the considered four messages. ECC together with hashing improves the robustness of the protocol. Authentication is performed here on the basis of six levels of verification. The performance of the proposed protocol is compared with that of Vanga Odelu et al., considering the number of genuine user details, attacker details, and accuracy, as three parameters. The proposed approach could attain a maximum of 75.58% genuine user details, 78.49% attacker details, and 77.03% accuracy.

REFERENCES:

[1] Slawomir Grzonkowski, Peter M. Corcoran, Thomas Coughlin, "Security Analysis of Authentication Protocols for Next-Generation Mobile and CE Cloud Services ", in proceedings of International Conference on Consumer Electronics, pp. 83-87, 2011.

[2] HardeepKaur, ManjitKaur, "KAMAN Protocol for Preventing Virtual Side Channel Attacks in Cloud Environment", TELKOMNIKA Indonesian Journal of Electrical Engineering, vol. 15, no. 1, pp. 184-190, 2015.

[3] Zhang Q., Cheng L., & Boutaba R., "Cloud computing: state-of-the-art and research

challenges", Journal of internet services and applications, vol. 1, no.1, pp. 7-18, 2010.

[4] Sameera Abdulrahman Almulla, Chan Yeob Yeun, "Cloud Computing Security Management ", in proceedings of International conference on Engineering Systems Management and Its Applications (ICESMA), pp. 1-7, 2010.

[5] XU Xiao-long, TU Qun, BESSIS Nik, YANG Geng, WANG Xin-heng, "SATVPC: Secure-agent-based trustworthy virtual private cloud model in open computing environments", J. Cent. South Univ., vol. 21, no.8, pp. 3186−3196, 2014.

[6] L.M., Kaufman, "Data Security in the World of Cloud Computing", Security & Privacy, vol.7, no.4, pp.61-64, 2009.

[7] Charalampos Doukas, Ilias Maglogiannis, "Managing Wearable Sensor Data through Cloud Computing", in proceedings of International conference on Cloud Computing Technology and Science, pp. 440-445, 2011.

[8] Hardt, D., "The OAuth 2.0 authorization framework", ISSN: 2070-1721, 2012.

[9] Shikha Singh1, Binay Kumar Pandey, RatneshSrivastava, Neharawat, Poonamrawat, Awantika, "Cloud Computing Attacks: A Discussion With Solutions", Open Journal Of Mobile Computing And Cloud Computing, vol. 1, no. 1, pp. 1-10, 2014.

[10] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds,” in Proceedings of the 16th ACM conference on Computer and communications security ACM., pp. 199-212, 2009.

[11] Vanga Odelu, Ashok Kumar Das, Adrijit Goswami, "A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards", IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1953-1966, Sept. 2015.

[12] Hong Liu, HuanshengNing, QingxuXiong, and Laurence T. Yang, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 1, pp. 241-51, 2014.

[13] Sarah Abughazalah, KonstantinosMarkantonakis, Keith Mayes, "Secure Improved Cloud-Based RFID Authentication Protocol", in proceedings of International Workshop on Data privacy management, pp. 147-164, 2015.

[14] Ta-Chih Yang, Nai-Wei Lo, Horng-TwuLiaw, Wei Chen Wu, "A secure smart card authentication and authorization framework using in multimedia cloud", Multimedia Tools and Applications, pp. 1-23, 2016.

[15] Marwan Darwish, AbdelkaderOuda, Luiz Fernando Capretz, "A cloud-based secure authentication (CSA) protocol suite for defence against Denial of Service (DoS) attacks", Journal of information security and applications, vol. 20, pp. 90-98, 2015.

[16] Wei Liu, Hong Liu, Yueliang Wan, Huafeng Kong, HuanshengNing, "The yoking-proof-based authentication protocol for cloud-assisted wearable devices", Journal of PersUbiquitComput, vol. 20, no. 3, pp. 469-479, 2016.

[17] Safiriyu Eludiora, Olatunde Abiona, Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime, Lawrence Kehinde, “ A User Identity Management Protocol for Cloud Computing Paradigm”, Int. J. Communications, Network and System Sciences, 2011, 4, 152-163.

[18] Nimmy K., M.Sethumadhavan “Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography”, ICADIWT (*Applications of digital information and webTechnologies*), IEEEfifth international conference pp.101-106, 2014.

[19] C. Voruganti, M. Sarvabhatla and G. Murugan, "A Secure Mutual Authentication Protocol for Cloud Computing Using Secret Sharing and Steganography," 2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, 2014, pp. 1-8.

[20] D. He and D. Wang, "Robust Biometrics-Based Authentication Scheme for Multiserver Environment," in IEEE Systems Journal, vol. 9, no. 3, pp. 816-823, Sept. 2015.