International Journal of Innovative Computing, Information and Control
Volume **14**, Number **6**, December **2018**

 ISSN 1349-4198
pp. **2221–2243**

SECURE ROAMING AUTHENTICATION MECHANISM FOR WI-FI BASED NETWORKS

Tahadray Jean Tsitaitse[1], Yongquan Cai[1] and Shaldon Leparan Suntu[2]

[1]College of Computer Science and Technology
Beijing University of Technology
No. 100, Pingleyuan, Chaoyang District, Beijing 100124, P. R. China
fahasoavajean@hotmail.com; cyq@bjut.edu.cn

[2]Department of Information and Engineering
University of Science and Technology Beijing
No. 30, Xueyuan Road, Haidian District, Beijing 100083, P. R. China
suntusha@yahoo.com

Received January 2018; revised May 2018

Abstract. *A severe contest for seamless roaming between inter-domain Wireless Fidelity technologies is to build a trust model in a milieu of several WLAN service providers with varying charging or billing options and authentication mechanisms. This study implements a comprehensive single sign-on prototype for the unification of various WLAN service providers. Users choose the suitable single sign-on verification scheme from the authentication abilities existing on the WLAN service providers that prevent the exposure of their information from illegitimate users while roaming. A composite layer 2 and web-based authentication method intended to ensure secure transmission of cryptographic keys while maintaining the prevailing WLAN charging options. The study deployed RADIUS and liberty based protocols to control unauthorized access to the WLAN network resources. In this paper, RADIUS simulation performed shows how authentication, authorization and accounting standards can be used to allow only the legitimate client to access the network while averting unauthorized users. In addition, the performance of the confederated Wi-Fi networks was shown by performing an experiment for the negotiation based authentication protocol with policy engine and authentication framework via the web-based protocol. The proposed mechanism revealed low latencies results which are suitable to support seamless user experience.*

Keywords: Seamless user experience, Security association, Web authentication, Authentication delay, Policy engine, Service provider, Identity provider

1. **Introduction.** Wireless Fidelity (Wi-Fi) technology is the primary goal of surfing the Internet for both home and office users. As an outcome, it brings a major challenge for designing seamless handover authentication protocols in Wi-Fi-based networks, more so in certifying security and efficiency [1]. The key to success of WLAN (Wireless Local Area Network) expertise is to provide fast and secure handover of a user's session key during roaming process [2]. Wireless network users assume that the Internet Service Providers (SPs), apart from providing an efficient access to the Internet resources should also protect their identity during roaming process [3,4].

A Security Association (SA) is a coherent unidirectional connection that exists between two or more peers stipulating algorithms, parameters and rekeying materials required for providing security services. The SA configuration between two peers can be done manually or dynamically to provide authentication, integrity or confidentiality. These protocols

DOI: 10.24507/ijicic.14.06.2221

include [5], a Transport Layer Security (TLS) Handshake protocol used by the TLS [6], IP level and by datagram transport layer security [7], at the transport level. Even though several methods and protocols are possible, they often use the Diffie-Hellman technique for the exchange of security keys between the mobile node and the Access Point (AP) to guarantee perfect forward secrecy.

In the circumstance of IEEE 802.11 every time a station changes from one AP to other the authentication process must take place. Owing to the issues found in the original IEEE 802.11 security resolutions, IEEE 802.11i is being standardized. IEEE 802.11i makes use of IEEE 802.1X and Authentication Authorization and Accounting (AAA or Triple "A") [8] protocol like Remote Authentication Dial-In User Service (RADIUS) or Diameter [9]. The IEEE 802.1X authentication process enables the supplicant, the authenticator (AP) and the Authentication Server (AS) to provide a dedicated secure infrastructure for Wi-Fi Protected Access (WPA) 1 or 2 for an enterprise WLAN. Extensible authentication protocol [10,11] control access to the WLAN to minimize frequent masquerading attacks between the supplicant and the AP.

For WLANs, clients entail that authentication, authorization and accounting need to be sheltered against impulsive disclosure to providers unless permitted by the client. At the same period, the client may require seamless roaming to avoid unnecessary sign-on of credentials where it does not infringe the client's security policy. From the ISP perspective, stern network access control is essential to avoid larceny of services from malevolent attackers. Likewise, WLAN providers are usually concerned about giving Internet Protocol (IP) level access to clients prior to authentication to permit different validation and sanction selections. This approach of giving IP level access in absence of authentication triggers a vulnerability to larceny of services via IP or Medium Access Control (MAC) address spoofing.

Considering these problems, this study developed an inclusive security solution for Wi-Fi-based network services, as an intersection on prevailing typical authentication and authorization prototypes. This paper addresses three core objectives:

1) To unite WLAN providers with diverse authentication structures and under diverse inter-provider and user-provider trust-relations,
2) To safeguard user's authentication credentials from indisposed exposure and minimalizing the amount of user involvement during sign-on and,
3) To govern network access by cryptographic methods while maintaining the prevailing substitute authorization means presently used in WLANs.

To meet the first objective, unification of WLAN ISPs to provide a Single-Sign-On (SSO) authentication scheme in the milieu of multiple authentications through trusted ISP SSO is centred on the Security Assertion Markup Language (SAML) technology which is a substantial tool as long as web-based security is presented. Likewise, it is a malleable and interoperable method of realizing heterogeneous security. This method is achieved through creating an authentication flow context to be adopted by the ISPs. Its strategic module is the negotiation-based authentication framework. Users may need to know the possible available verification methods in a precise server and deliver a friendly environment to select a preferred choice amongst the existing alternatives. It is necessary to do it in a standard approach as to permit automatic handling of the data at the client portion.

To meet the second objective, an implementation of policy engine is considered on the side of the client to automatically select the authentication information to be transmitted to the Service Provider (SP) depending on the user well-defined policies SALM which is an eXtra Markup Language (XML) and considering the context of communication. The

policy engine can be combined with the client negotiation-based protocol to trigger the policy engine to control the information to be transmitted to the negotiation based authentication server depending on the abilities of the core AS, instead of requesting the user to manually provide the required information. In this scenario, the policy engine can be considered as an integral part of the adaptation framework of the authentication process. However, it can also be used self-reliant, as it provides an elementary Application Programming Interface (API) for authentication information access. This can be evoked not only by the web-based framework but also by another framework like Transmission Control Protocol (TCP)/IP layer of authentication. In addition, the policy engine supports provisional action as suggested by [12,13].

To meet the third objective, the development of a compound layer 2 (L2) and web-based authentication method should be pondered in order to safeguard cryptographically protected access to Wi-Fi networks. In this composite L2 method, the client first launches a session key of an L2 by means of unregistered account in an IEEE 802.1X authentication protocol. The client then inserts the L2 session key abridgement in web-based authentication. By integrating L2 and web-based authentication outcomes, this method averts service theft, eavesdropping, and message modification while being transmitted to the recipient.

To exemplify the use of authentication process adaptation and the work of the policy engine, cogitate the following scenario:

"A user switched on his Portable Digital Assistant (PDA) in his workplace and is automatically associated with his organization's Wi-Fi network. The organization Wi-Fi network deploys 802.1X authentication with Extensive Authentication Protocol (EAP) and the policy engine allows automatic compliance of the shared secret key between him and the organization Wi-Fi network. Then he gets out of the workplace building in possession of his PDA, thus roaming into a library WLAN network. The network broadcasts its identity and the authentication mechanism. This network deploys its verification via a web-based mechanism known by the user. The policy engine permits the user's credential to be submitted automatically to library authentication method, thus permitting him to get associated with the library WLAN network. The user gets out of the library and walks into a hotel; the PDA discovers the availability of Wi-Fi network. As previously, the Wi-Fi network broadcasts its service set identifier and verification capabilities. The engine can detect both the Liberty-based and RADIUS-based protocols. The policy engine presents a graphical user interface on the user side and queries him if he needs to link to the Wi-Fi network. If he concedes it, the policy engine sends his verification information to the AS of the Wi-Fi network SP that delivers network access for the hotel after selecting a preferred choice of authentication capability of the hotel AS (RADIUS-based or Liberty based). He then gets associated with the hotel Wi-Fi network and granted access to the internet services."

The sections ahead are organized as follows. Section 2 presents the literature review. Section 3 describes the proposed roaming model. Section 4 presents the proposed SAML web-based SSO authentication mechanism certification. Section 5 introduces the client-side's policy engine. Section 6 presents simulation of access to Intranet (Wi-Fi) network using RADIUS authentication protocol. Section 7 presents the proposed authentication framework. Section 8 analyzes the web-based and access control authentication security, and, finally, Section 9 concludes the work.

2. Literature Review.

2.1. Authentication mechanism.

According to [14] authentication refers to the manner in which one party attests the identity of the requested identity. Also, [15] defined authentication as an identity that requires further proof of identity as a user or a computer. The validator is the entity that validates the requested identity by the applicant. The authors also discussed a variety of data transfer verification methods between the entities under-identification in a WLAN.

The authors of [16] built a network called CHOICE to offer the following goals: foremost, only legitimate users should access the network and its resources. Secondly, no one apart from the user and the authentication database should be outhoused to self-information, for instance, the login credentials. Thirdly, several categories of security should be configured to scramble data and authenticate only the legitimate users. Fourthly, a dynamic key management is crucial and finally, one single encryption should be discouraged. CHOICE deployed protocol for authorization and negotiation of services, which provides access, authorization, security, privacy, policy enforcement, accounting and quality of service.

According to [17] the authors based their notion on novel AAA architecture in WLAN hotspots areas for Internet access. The authors protracted the 802.11i standard to such network scenario through using forwarding abilities without degrading the security salient features in 802.11i technology. The method of adjusting 802.11i to this vibrant milieu is centered on providing a computer-generated infrastructure among the roaming clients.

Fast handoff is required to be done one hop ahead of a roaming mobile station to the targeted AP. Association and reassociation enable the roaming client to remain connected to one AP at a time [18]. If the client roams, the target AP request for buffer data transfers from the old AP. During the context information change, the Internet access point protocol ensures the confidentiality of context information by deploying the RADIUS to secure communication between the network access server (NAS) and the back-end AS.

The authors of [19] proposed different prevailing virtual operator based on AAA clarifications and presented an interpretation that is fully based on IP level. The authors attained their goal by congregating both the AAA process and data conveyance, at the IP level to provide a clarification, which was tremendously extensible. This method works across multiple interfaces and is compatible with wireless network cards from a variety of vendors. Service credits were dully apportioned to these intermediary nodes as enticements for delivering relay amenities.

2.2. Web pass-through mechanism.

Several organizations use pass-through software or web-based authentication to authenticate their clients into the network [20]. In this context, a uniform resource locator is required to redirect the user to a web application page to query for a valid combination of password or username from a web server or active directory domain. This form of authentication prevents frequent logging in when a user wants to associate to the network within the same administrative domain.

Security Assertion Markup Language (SAML) protocol discussed by [21] as a security measure for exchanging information between the web client, the service provider and the IDP. To illustrate this scenario, a profile of the SAML request authentication protocol is deployed, with a combination of the HTTP-Redirect, HTTP-POST and HTTP-Artifact bindings [22,23]. This protocol supports SSO.

Many WLAN providers hire web-based authentication in combination with IP packet filtering at an infrastructure access server centered on the MAC and IP addresses. Since address deceiving is easily accomplished by means of readily available arsenals, this way does not guarantee robust security for network providers. Malevolent users can screen the

wireless channel, get MAC and IP addresses of authentic users, and transmit packets with tricked addresses to execute theft of service or Denial-of-Service (DOS) attacks [24,25].

This study differs from aforementioned extant studies in that a user can select his own IDP by using only a standard based link-layer security, even though they assume a centralized AS entails proprietary security of the sublayer. This method makes it possible for a user to choose the most favored authentication mechanism and IDP among others, and avert unwilling security information exposure according to the user-define policy, which is not mentioned in their studies. This is mostly because the policy management functionality exists in both the network and the user, while they assumed a policy controller only at the network side.

Likewise, several studies revealed that to design a roaming network, RADIUS server is used to protect the data between the communicating nodes. In this study, RADIUS server is used to provide AAA services whereas SAML is deployed in the exchange of information between the IDP and the SP in a secure manner. In addition, a single sign-on mechanism is introduced to enable the user to supply the login credentials at home server and while roaming across will be authenticated to various Wi-Fi networks where roaming agreement exists without using several passwords but only redirected to the home server for the formation of the trust relationship between the IDPs.

To recap, existing web-based authentication models do not deliver adequate security against the theft of service, dynamic selection of dissimilar authentication structures, or a user's policy-based disclosure of private data while in a nomadic process. This study confederates several IDPs and SPs with different authentication methods and charging options as well as satisfying the security concerns required for the privacy of identity of user's information.

3. The Proposed Roaming Model.

One objective of this study is to confederate several WLAN SP and identity provider (IDP) with dissimilar authentication mechanisms. The authenticated IDP acts as a trusted party for the SP. Here, there is no direct contractual or trust relationship in between the user and the network being visited; however, there is trust between the user and the IDP and between the IDP and the SP. Because there is a trust relationship between the user and IDP through authentication trust and between the IDP and SP through roaming/federation agreement policy, the SP trusts the user. The trusted authenticated IDP will then be used to gain access to the targeted network. The roaming agreements will lay down under what circumstances the targeted network sanctions an authentication statement from the already verified SP, how the authentication credentials-cum-accounting data are exchanged and what monetary arrangement is in place for the guest users.

In Figure 1, the user wants to establish a connection with SP $\boldsymbol{A}$, and in this case, the user does not trust SP $\boldsymbol{A}$. Due to this, the user has a trust relationship between IDP $\boldsymbol{A}$ via trust authentication. There is also a trust relation between IDP $\boldsymbol{A}$ and SP $\boldsymbol{A}$ due to roaming agreement. In this scenario, IDP $\boldsymbol{A}$ forwards the authentication request to SP $\boldsymbol{A}$. Then SP $\boldsymbol{A}$ confirms whether the user is valid and replies IDP $\boldsymbol{A}$. Then IDP $\boldsymbol{A}$ replies the user. At this point, a transitive trust relationship is created between SP $\boldsymbol{A}$ and the user. This idea of transitive trust relationship property of equality is borrowed from mathematics which states that if $x = y$ and $y = z$ then $x = z$.

If a user roams from SP $\boldsymbol{A}$ to SP $\boldsymbol{B}$, a lot of work needs to be done to enable roaming of users between inter-domain technologies. WLAN SPs do not trust each other nor have knowledge about their existence. Therefore, IDPs play a crucial role to enable roaming of users across several WLANs within different domains. In Figure 1, the user wishes to roam from SP $\boldsymbol{A}$ to SP $\boldsymbol{C}$, and these networks are in different domains. In this case,

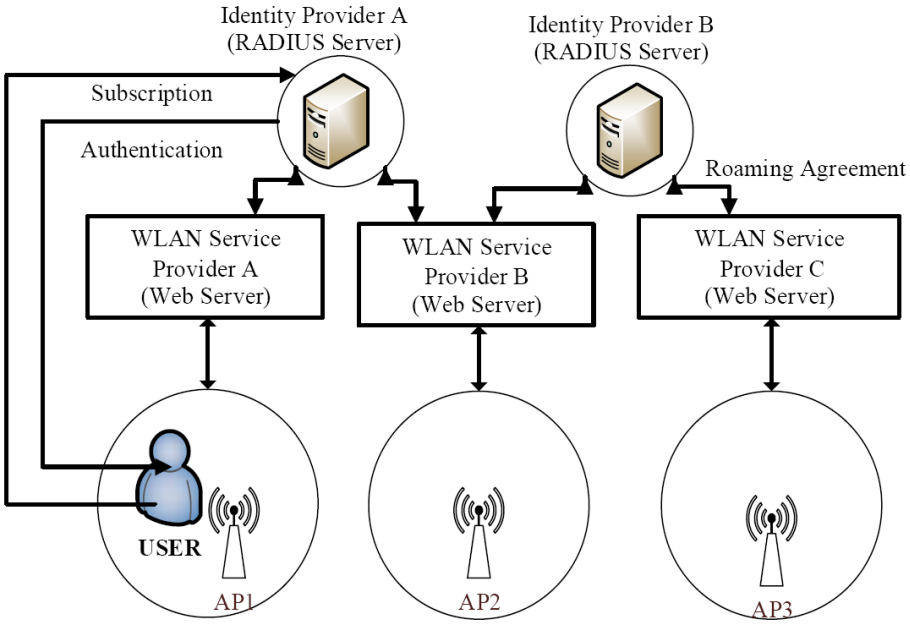


FIGURE 1. Proposed roaming model

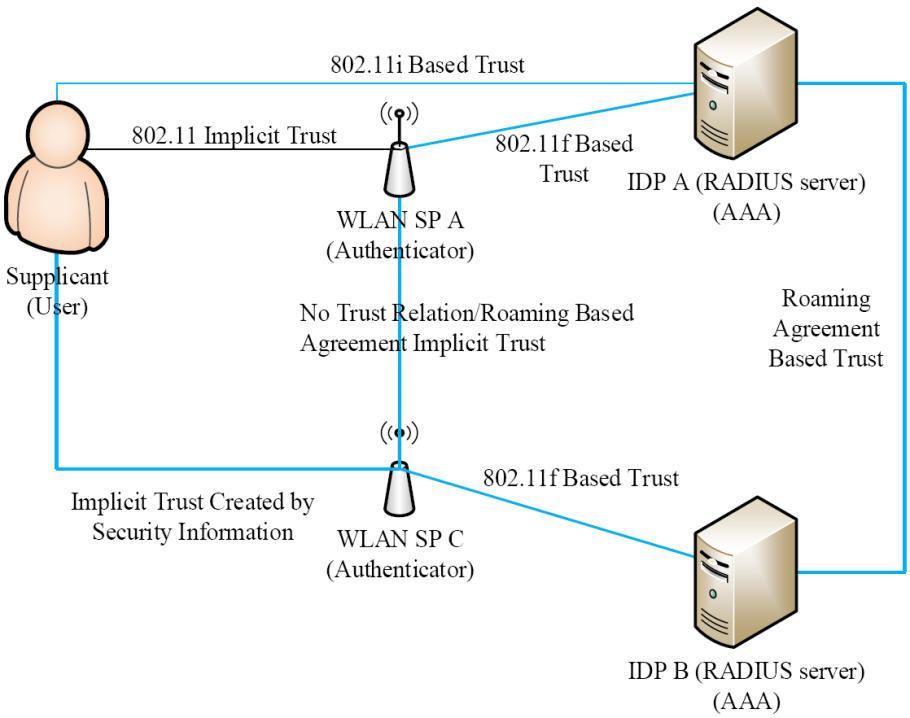


FIGURE 2. Trust relation model

the user enters into the coverage area of AP3 and requests for an association with SP ***C***. The process of authentication aforementioned above is triggered. Since there is roaming agreement-based trust between IDP ***A*** and IDP ***B***, IDP ***B*** requests for users information from home network server to the visited network server. Confirmation of the credentials of the users at the home network necessitates conveying the credentials to the home network and sending the outcome of the authentication back to the visited network using RADIUS protocol. Figure 2 portrays the trust relations for the transportation of key materials in a roaming network.

Trust relation model enables the transfer of context information from one home network to the targeted network using a roaming key and inter-access point protocol. The roaming key is refreshed after the handing over took place. Security information is sent by the serving AP to the supplicant if the handover takes place to a different domain.

4. **The Proposed SAML Web-Based SSO Authentication Mechanism Certification.** In the real environment, whenever a client roams to a different environment administrative domain, a login to the network will be required. Confederating several IDPs and SPs with dissimilar authentication mechanisms requires a single sign-on to be centralized. A user is required to have an account with one trusted IDP in the inter-domain scenario. An implementation of trust relations between IDPs and SPs of different intra-domain should be configured to allow secure roaming.

In this regard, SAML prototype is a preferred mechanism which enhances the exchange of security information across dissimilar security spheres. SAML is based on a security token, which is certified in indirectly with the user's identification entities. This provides robust security of the authentication process. By applying the single sign-on method, the user is relieved from perennial rekeying of usernames and password for the certification process. SAML does not depend on the network with which it interacts with but each infrastructure can configure its own strategy user's authentication and authorization procedure. This accords dynamic authentication through different domains to confederate the different SPs and IDPs. The salient features of interoperability and attributed based authentication rate SAML. SAML standardizes that the assertions and messages must be scrambled by using Secure Socket Layer (SSL) throughout the transmission session to thwart message interception as well as replay attacks [26].

SAML authentication protocol mostly consists of client's web browser, IDP, Lightweight Directory Access Protocol (LDAP) [27,28] directories of the inter-domain X, and the web SP's website in the inter-domain Y. Figure 3 shows SAML certification procedure.

The detailed process of the certification mechanism is provided in Steps 1 to 10 as follows.

Step 1: The user key in his credentials on the SP's website in the inter-domain portion labeled "X", and perform an IDP selection and the LDAP server authenticate him to the services and store the credentials for the subsequent re-authentication.

Step 2: The inter-domain SP portion "X", forwards the user information to the side of the home domain, and appeals for authentication.

Step 3: The user's identity is created or verified via the process of the authentication session. The user will be required to establish his identity by providing the username and password in order to be authenticated to the services.

Step 4: Upon passing the required verification, the identity statement is proven and stored in the home domain. At that juncture, the authentication session is mutually formed. The user is redirected to inter-domain service provider at part "X".

Step 5: The SP at "X" accesses the SAML authentication statement which is created during the redirection process and sends it to the IDP to request to authenticate the user's statement.

Step 6: The IDP then sends back an SAML authentication statement to the SP in the inter-domain "X" after validating.

Step 7: The user requests to access secured resources of the SP in the inter-domain "Y".

Step 8: The inter-domain "X" SP readdresses the user to the IDP of the inter-domain "Y" via the link.

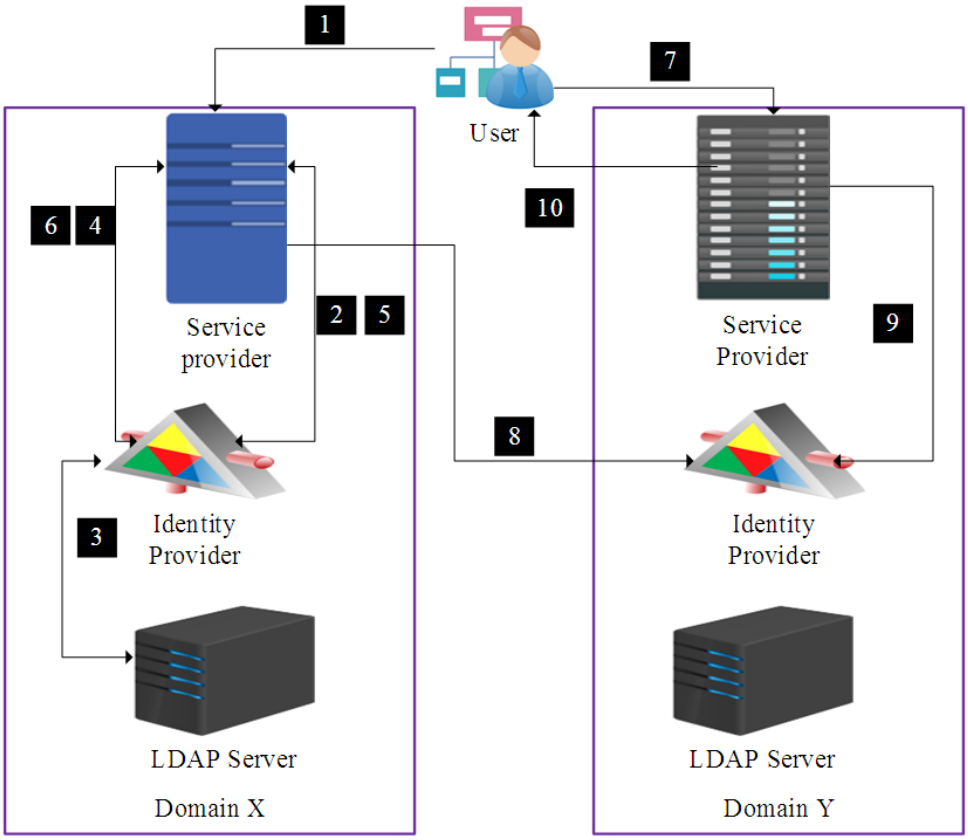


FIGURE 3. SAML certification procedure

Step 9: The inter-domain "Y" service examines the services of the user. It might request for an inside authentication statement that the SP of the inter-domain "X" bids the user. The log-in process in the inter-domain "Y" is skipped and the single sign-on is achieved.

Step 10: The inter-domain SP "Y" responds to the service request of the user. If allowed, the requested service is delivered to the user. Likewise, If not then the service is repudiated.

Presently, other significant common methods used to authenticate users securely to the WLAN network include the RADIUS or liberty based architecture. These standards can also offer SSO authentication mechanisms [29,30]. The liberty-based protocol has a benefit of hiding client's identity and logs in credentials where a weak SP is used in a WLAN scenario. These methods are also taken into consideration in this paper to ensure multiple and dedicated authentication methods have been met.

RADIUS uses a proxy-based verification method; the user sends the data to the SP which in turn forwards it to the client's IDP. Figure 4 shows a streamlined sequence of RADIUS-based authentication messaging. RADIUS' main weakness is that the user does not hide his identity and credentials to the SP with weak security, owing to the HTTPS-RADIUS transformation process at web server of the SP. RADIUS causes major risks to the user where passwords and usernames are exposed to the web server's of the untrusted SP through the HTTP-RADIUS translation practice [31].

In the process of liberty-based artifact verification method, utilize a redirect-based authentication exemplary as shown in Figure 5. The client notifies the SP of the name identifier of his IDP, and then the SP forwards the client to that IDP. The client then

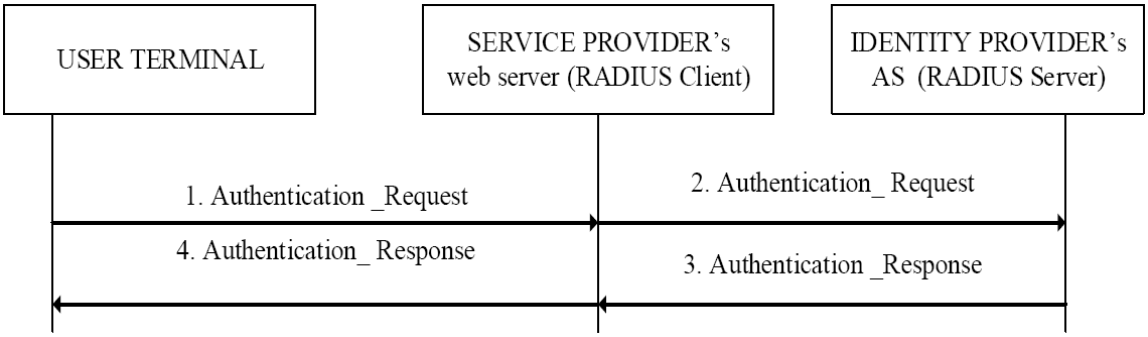


FIGURE 4. RADIUS authentication proxy-based protocol

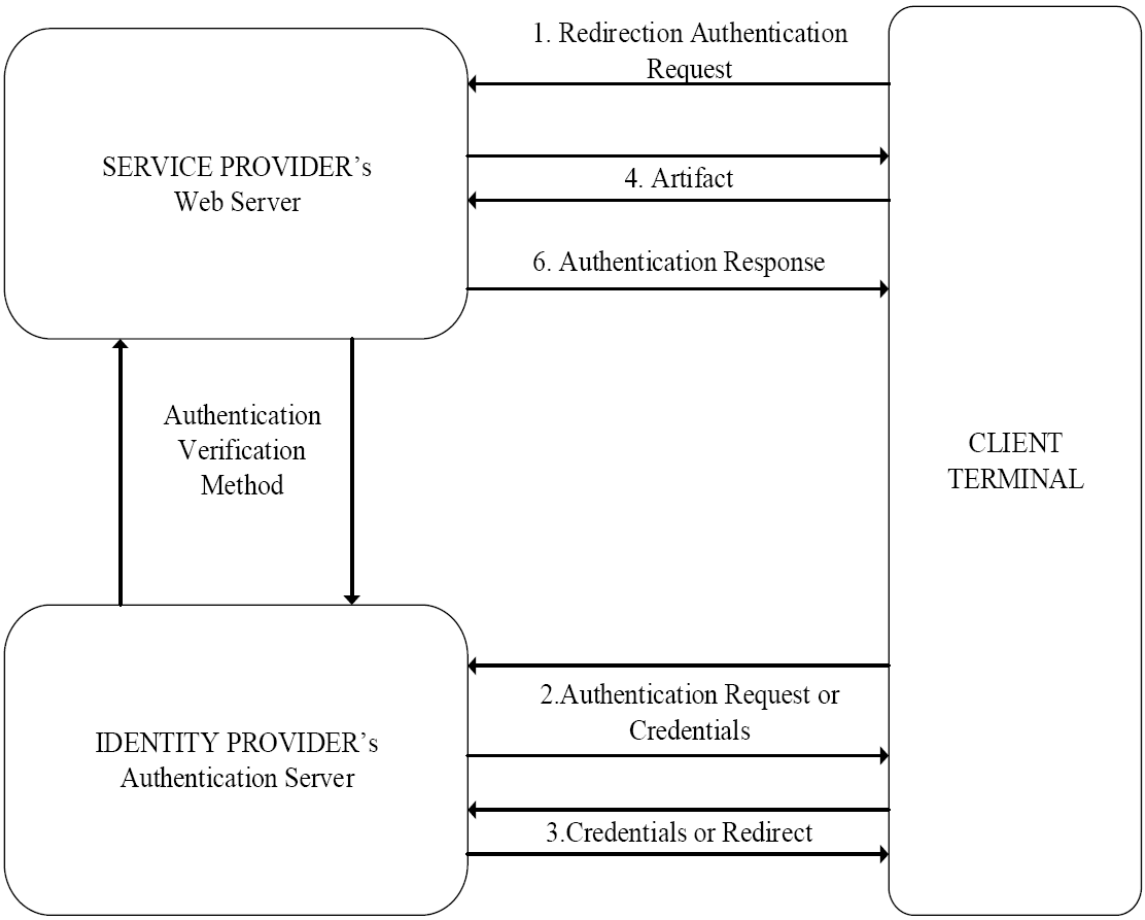


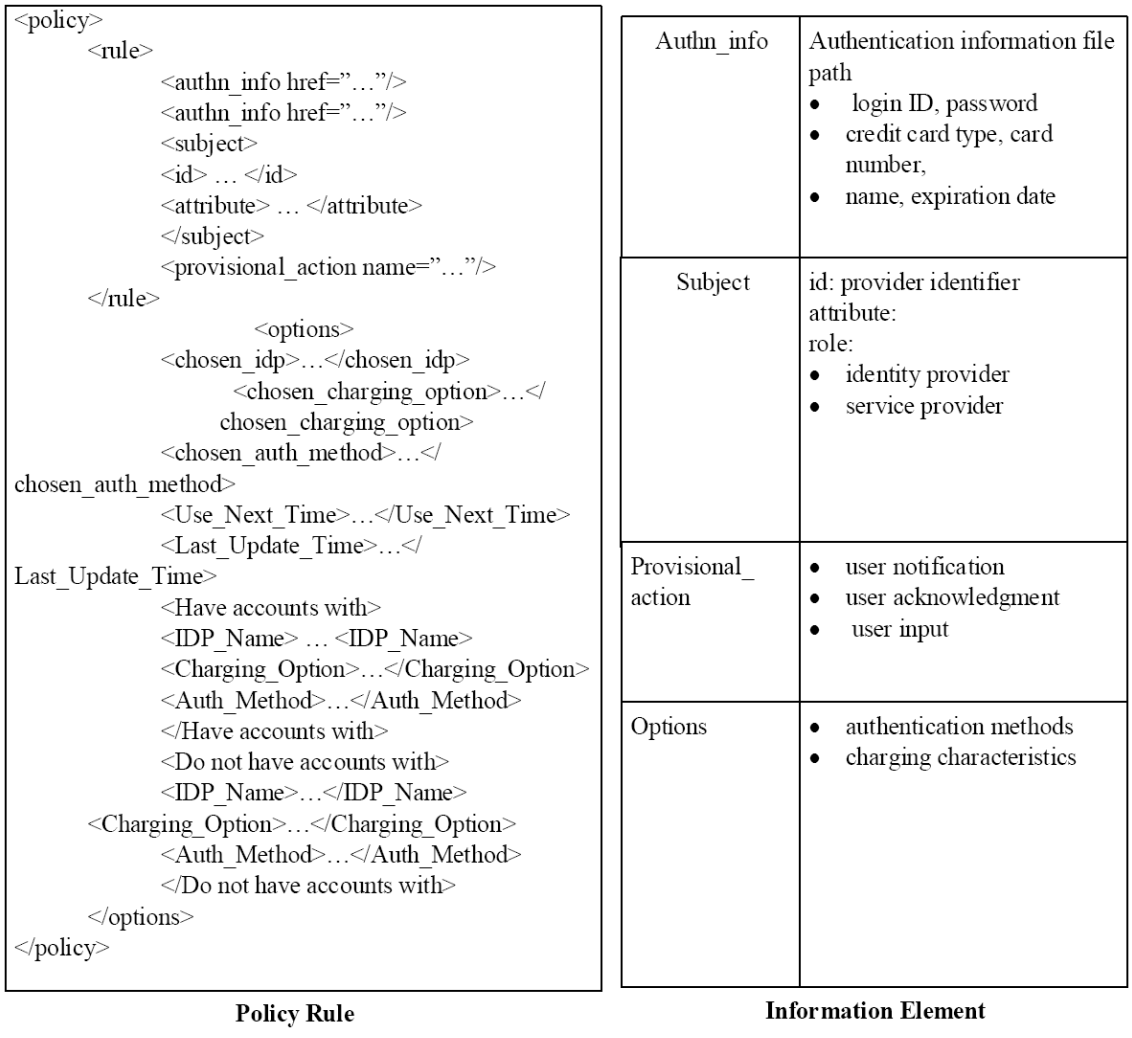
FIGURE 5. Liberty-based browser's redirect artifact profile verification

sends the login credentials towards the IDP, obtains its result, and forwards it to the SP. The IDP's result contains an indicator to a verification assertion.

5. **Client-Side's Policy Engine.** In this segment, the policy engine for the client side is designed to select a suitable SSO method while shielding the privacy of user information in Wi-Fi network environments. The policy engine is a computerized framework that facilitates policy-based authorization and accounting [32,33]. As the client roams across the inter-domain technology, two issues must be taken into account to realize seamless user experience; protection sensitive user's verification information against disclosure to entities not permitted to see and minimalize user intervention for the sign-on practice.

The policy engine is blended with rules and services where rules describe the standards for resource access and usage [34]. The policy engine is a self-governing module that can be invoked via a simple Application-Programming Interface (API) from an authentication negotiation client, link-layer network access client or ordinary web browser. It required as input an XML file formatted according to the XML schema definition for the authentication capabilities statement of the negotiation based authentication standard. This file comprises the AS identifier, with companion information to validate it, the requested user information, and context information. As a result, it returns an XML file structured according to the XML schema definition for the authentication query of the negotiation based authentication standard comprising the requested information.

The policy rules may contain provisional actions to be satisfied such as user notification and acknowledgement. The user terminal always requests user input or acknowledgement. The receiver is the one who makes the access control decision regarding security policy and context. Policies may also include information about authentication query, authentication abilities for a precise subject element as well as the user's charging option. If a user roams into a provider, the client policy engine will perform a comparison with the previously saved options and when a match occurs, it executes an automatic selection. If a mismatch is traced, the user is alerted by the policy engine to use the interface for the novel selection. A sample of the information element and policy rule is shown in Figure 6.



```
<policy>
    <rule>
        <authn_info href="…"/>
        <authn_info href="…"/>
        <subject>
        <id> … </id>
        <attribute> … </attribute>
        </subject>
        <provisional_action name="…"/>
    </rule>
            <options>
        <chosen_idp>…</chosen_idp>
            <chosen_charging_option>…</
          chosen_charging_option>
        <chosen_auth_method>…</
chosen_auth_method>
        <Use_Next_Time>…</Use_Next_Time>
        <Last_Update_Time>…</
Last_Update_Time>
        <Have accounts with>
        <IDP_Name> … <IDP_Name>
        <Charging_Option>…</Charging_Option>
        <Auth_Method>…</Auth_Method>
        </Have accounts with>
        <Do not have accounts with>
        <IDP_Name>…</IDP_Name>
    <Charging_Option>…</Charging_Option>
        <Auth_Method>…</Auth_Method>
        </Do not have accounts with>
    </options>
</policy>
```

Policy Rule

Authn_info	Authentication information file path • login ID, password • credit card type, card number, • name, expiration date
Subject	id: provider identifier attribute: role: • identity provider • service provider
Provisional_ action	• user notification • user acknowledgment • user input
Options	• authentication methods • charging characteristics

Information Element

FIGURE 6. A sample of information element and policy rule

The policy block engine contains three components with precise functionalities. These parts include the secure component, the root component and the specific component.

The root component is the only module that encountered the accessor where the XML file input is conducted. The root component verifies the initial information about the SP's identity before executing a decision tree. First, it checks if an SP precise policy subsists for this SP. If so, it interacts with the precise component to validate if the user desired the stored choices to be automatically applied when roaming into this SP's network. If this is correct, it matches that saved information against the choices declared to confirm if these choices are still valid. If this is correct, then the root element intermingles with the secure component and generates an XML file that contains the choices selected for this SP and the prerequisite information for these choices. If any of the decision questions reverted a false option, the root element alerts the negotiation client authentication. It then invokes its Graphical User Interface (GUI) so that the user can select options manually and agree whether to save these for subsequent time.

The secure component stores the crucial information for the user to be authenticated at any point. It stores IDP, username and password for an individual account the user owns. This module is only accessible and interpreted by the root component and is thus concealed from the SP. It is only accessible if the standards are encountered in the root component. A cryptographic algorithm is used to shield the stored information from illegal access.

The specific component contains SP precise rules. It also stores the user choices for backward roaming to enhance automatic sign on. Next, it holds information from the declaration that provided these choices. The precise rules for an SP can only occur if the user has beforehand signed on to this network using the manual graphical user interface. Figure 7 shows a typical policy block engine.

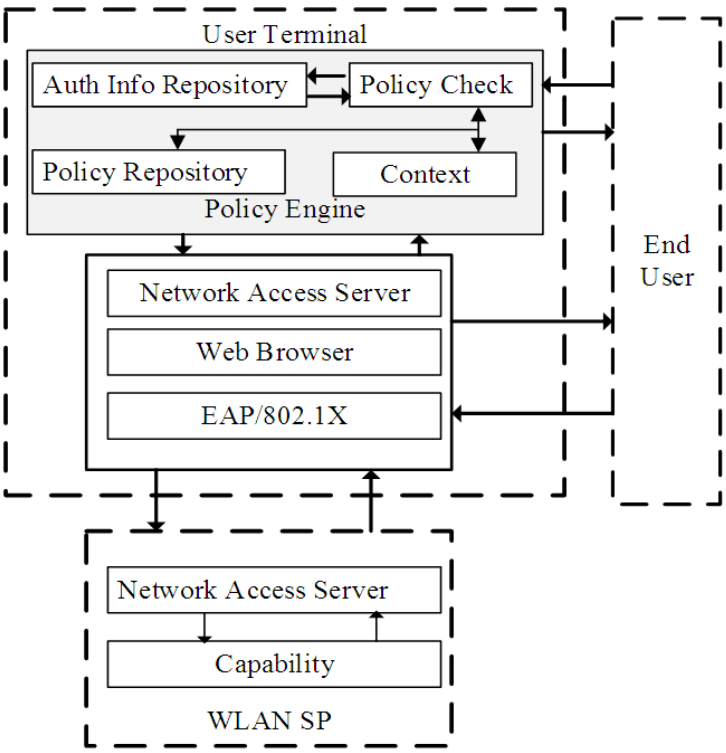


FIGURE 7. Policy engine block diagram

6. **Simulation of Access to Intranet (Wi-Fi) Network Using RADIUS Authentication.** Figure 8 and Figure 9 show the screenshots simulated using Cisco Packet Tracer. The network comprises the ISP, the Intranet network (192.168.0.1/24) and the private network (192.168.1.0/24). The Intranet comprises the Linksys Wireless Router (WR), the hacker, client 1 and client 2 and the RADIUS server providing triple "A" services.

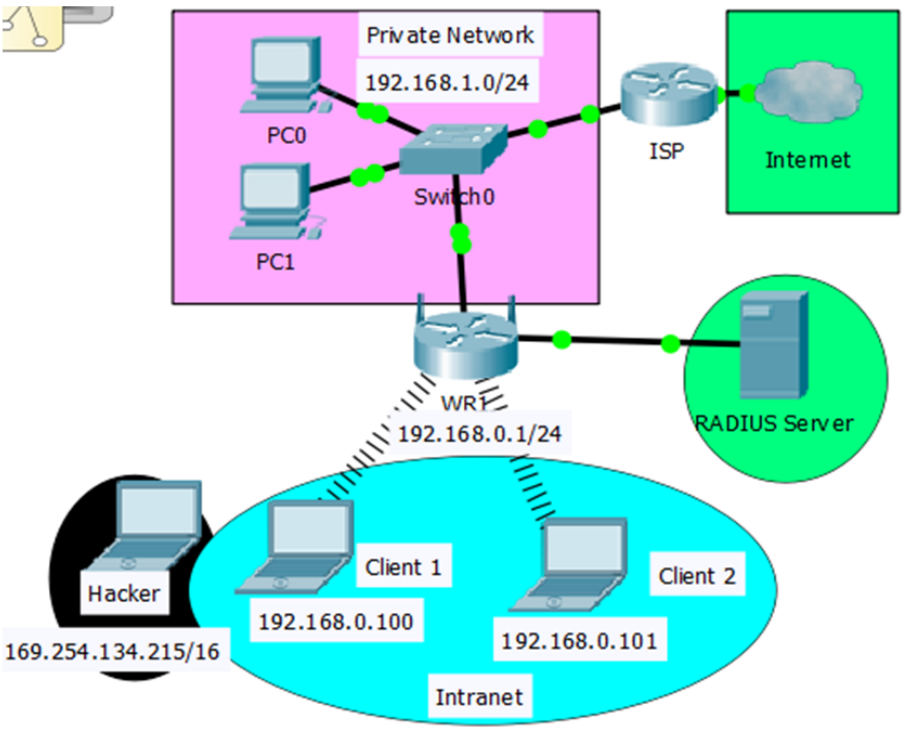


FIGURE 8. Wi-Fi with RADIUS authentication standard

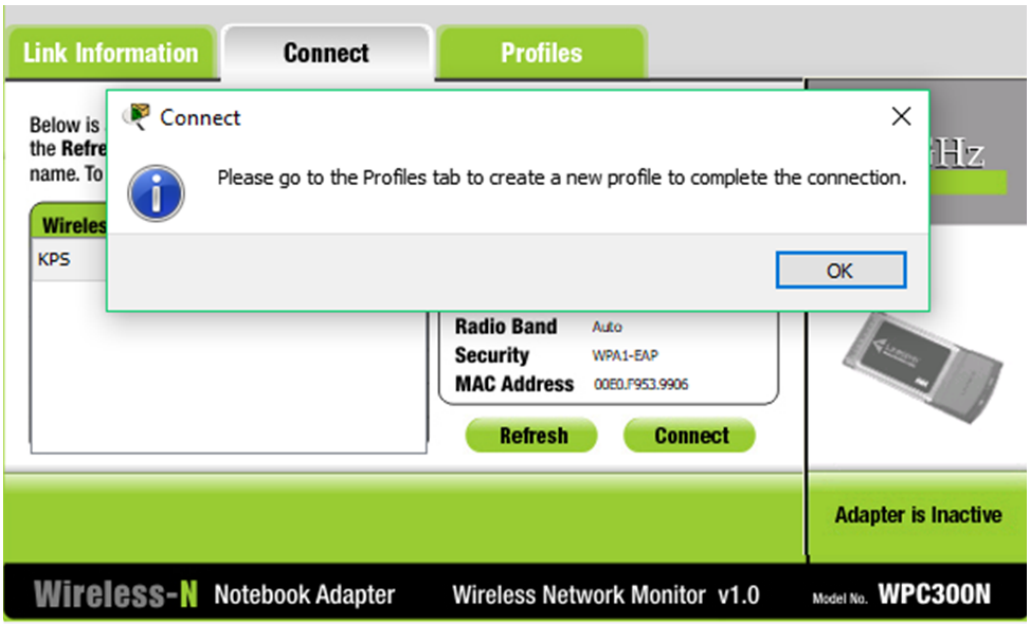


FIGURE 9. Network prompting for creation of hacker's profile

In the simulation, client 1 and client 2 usernames and passwords have been created in the RADIUS server except for the hacker and configure to use WPA2 enterprise as the encryption mode using the capabilities of Linksys wireless router provided by CPT network designing software.

Clients 1 and 2 are connected to the network since they are authorized to join the network via their credentials stored in the AAA server.

When the hacker tries to join the network, he is redirected to the profile setup page to complete his profile update in order to join the network as shown in Figure 9. If he tries to use MAC spoofing, the hacker cannot join the network since the network is using RADIUS protocol for authentication. The security mode is disabled and his card becomes inactive to connect to the network. Therefore, the RADIUS protocol is ideal for an enterprise Wi-Fi network.

This simulation describes how the RADIUS authentication mechanism with WPA enterprise can be used to control users access to the network resources [35].

Figure 10 comprises a 12-steps detailed procedure showing how 802.1X can be used to control access to Wi-Fi network. Only users offering verifiable credentials against a precise local database of the RADIUS server or fetched by RADIUS server from external database servers such as the active directory are granted access to the WLAN. RADIUS authentication assumes the prior authentication took place on an open and insecure infrastructure.

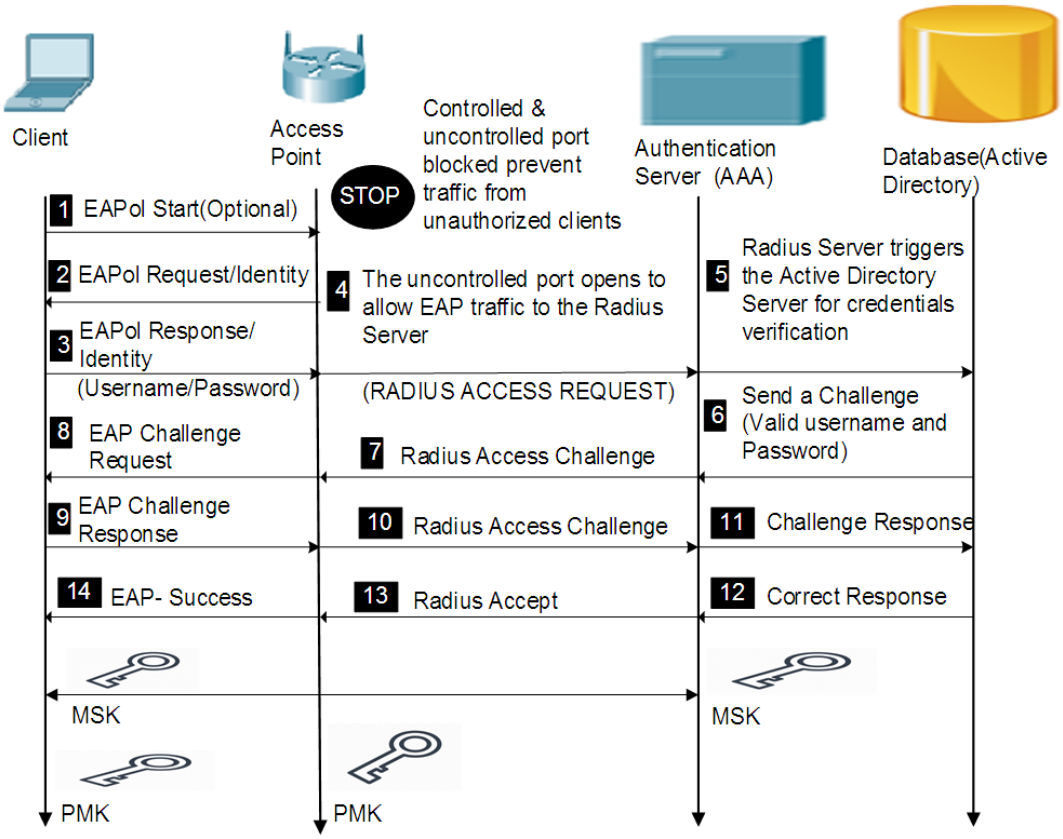


FIGURE 10. 802.1X/EAP messages exchange

Table 1 shows the steps of 802.1X/EAP message exchange as depicted in Figure 10.

If the response is incorrect, the process loop to the initial EAPol message exchanges. At this point, the Master Session Keys (MSK) are installed at the AS and the supplicant. MSK is unique and cannot be shared amongst the supplicants. MSK is used to compute

Table 1. 802.1X/EAP message exchange process

Steps	Description
1.	The 802.1X supplicant client send extensible authentication protocol over local area network (EAPol) to the AP
2.	The AP response with an EAP-Request identity to the supplicant
3.	The supplicant then responded with an EAP-Response identity to AP, i.e., the username and password
4.	The AP opens uncontrolled port to the AS and forward RADIUS access request from the supplicant to the AS
5.	The AS triggers the active directory (AD) if the database has not been configured in the AS database and forward the username and password for verification
6.	The AD answer with a challenge of either valid or invalid username or password
7.	The AS forward the RADIUS access challenge to the AP basing on the verification details from the AD database.
8.	The AP forwards the EAP challenge request to the supplicant
9.	The supplicant responds the AP with an EAP challenge response
10.	The AP forwards a RADIUS access challenge to the AS
11.	The AS forwards the challenge response to the AD
12.	The AD verifies if the client is the one to whom username and password were being validated and answer either correct response or incorrect response
13.	The AS sends RADIUS to accept message to the AP
14.	The AP forwards EAP success to the supplicant

the Pairwise Master Key (PMK) on both the supplicant side and the AS side. The AS then forwards the PMK to the authenticator for the entire client session. The 802.1X/EAP authentication occurs after the open authentication process. If the supplicant sends an EAP to log off the AP uncontrolled port changes from authorized state to unauthorized state.

7. **The Proposed Authentication Framework.** To incorporate providers with diverse underlying authentication schemes, this research focuses on developing an architecture that can involve alternative authentication schemes. The advantage of this proposal is that not all providers support a similar authentication scheme. Occasionally, a provider can only interact with others that deploy similar authentication methods. In this innovation, each provider must support more than one authentication method in order to communicate with a large number of existing providers. More decisively, in the scenario where a WLAN ISP provides multiple authentication choices, users can choose the scheme they desire. User preference is predominantly used in a case where providers that uphold interactions with diverse trust levels with the users are federated since some methods of authentication are highly secure than others. A user can choose one subject to their level of trust with the SP.

To permit users to select, SPs must communicate their methods of authentication they support. Even if the SP merely supports one method, it is helpful that the user knows the method that the provider deploys. Therefore, they can decide if they are free to provide this information. Users may also need to know the SP's identity and the companion data to validate it, to determine provider's trust level. This definitely affects their decision.

The charging option of a server is also a factor to be considered. Inline with the payment mode, minimum charging period, price, and services allowed, a user could choose whether the provider services are of importance and the charging methods he prefers are available. Definitely, in this design IDPs might be several in the architecture. A user with accounts at various IDPs would like to be aware of the SPs with roaming agreements. In this architecture, SPs must advertise their server's authentication abilities.

To enable roaming, it is beneficial if the communication of authentication capabilities can meet the user's choice with marginal user's involvement. A new SAML web-based protocol, the negotiation-based scheme, which computerizes this progression by permitting SPs to broadcast their abilities to clients and clients to communicate their selections to SPs is crucial. Rather, an installation of negotiation-based client software component from the IDP's web-portal is also required. Several enterprises developed a user graphical user interface to allow users to key in their credentials. In this design, a GUI was developed that presents the server's authentication capabilities to enable users to make their own selection. Authentication of clients is still practical even if the negotiation-based utility is not installed at the server or the user's node. In this case, users can be verified via the web interface.

Figure 11 shows the flow of authentication sequence. As portrayed in the illustration, in reaction to an authentication demand from a new user requiring access permission to the exterior network, the authentication server grants him with the available substitutes and the information necessary for using each. The user then chooses the suitable authentication scheme manually or through the policy engine in relation to the user's preference and trust. The client then delivers the information demanded by the SP for that precise scheme. The SP's server, changing between substitute methods as per the user favorites, processes the information. Lastly, the server sends the authentication outcomes to the client.

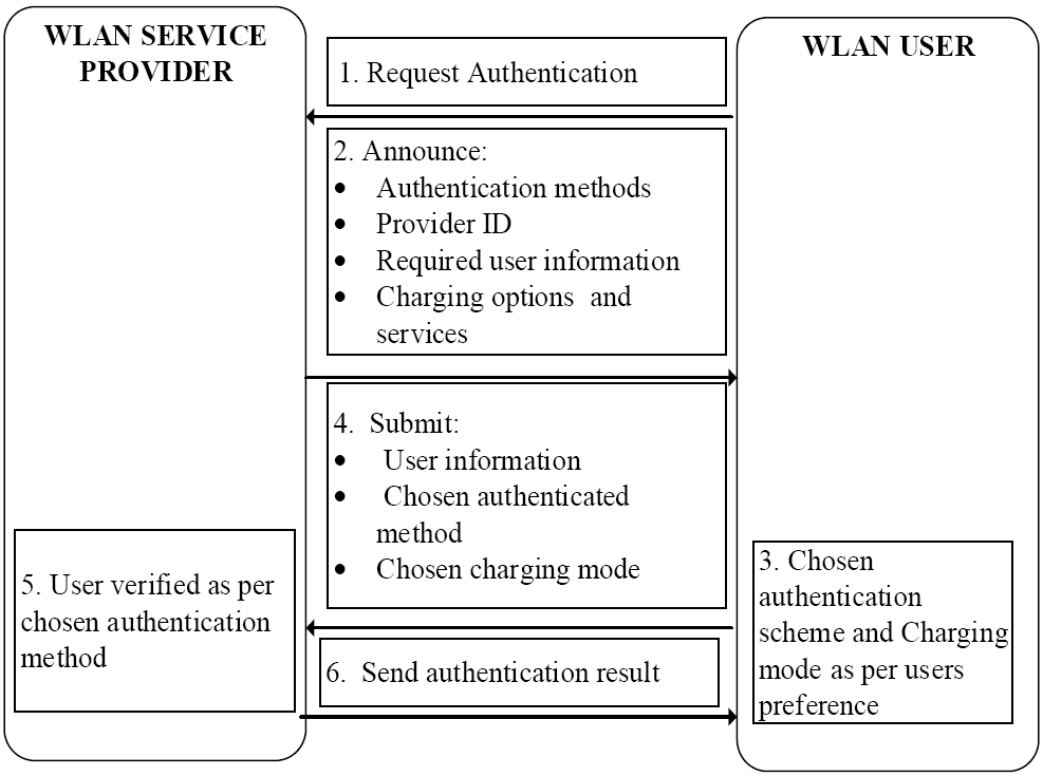


FIGURE 11. Proposed authentication framework

7.1. **The user interface design.** Figure 12 depicts a GUI form displaying the options presented by a specific SP. This is extracted from the authentication abilities statement transmitted by the SP in Step 2 of the proposed authentication framework as shown in Figure 11. It clusters the information into classes of IDPs for which the client may or may not have registered their accounts in them. Upon choosing one from either with or without accounts fields, the GUI shows the charging preferences offered by the selected IDP. Upon choosing from the item list of charging options, the GUI displays the precise information for that particular charging choice. Authentication scheme and the required data for each are presented in the same style. Above each combo box field where a choice is made and the current option chosen. The button labelled 'OK' selects the options chosen and then triggers the client if he would like to accept these for the subsequent verification. The Exit button closes the GUI. Sign Up button simply redirects the user to the normal web browser to update the personal data. Details button merely is coded to show the last options selected by the client. The client is also allowed to edit the details available either instantly or offline via the GUI.

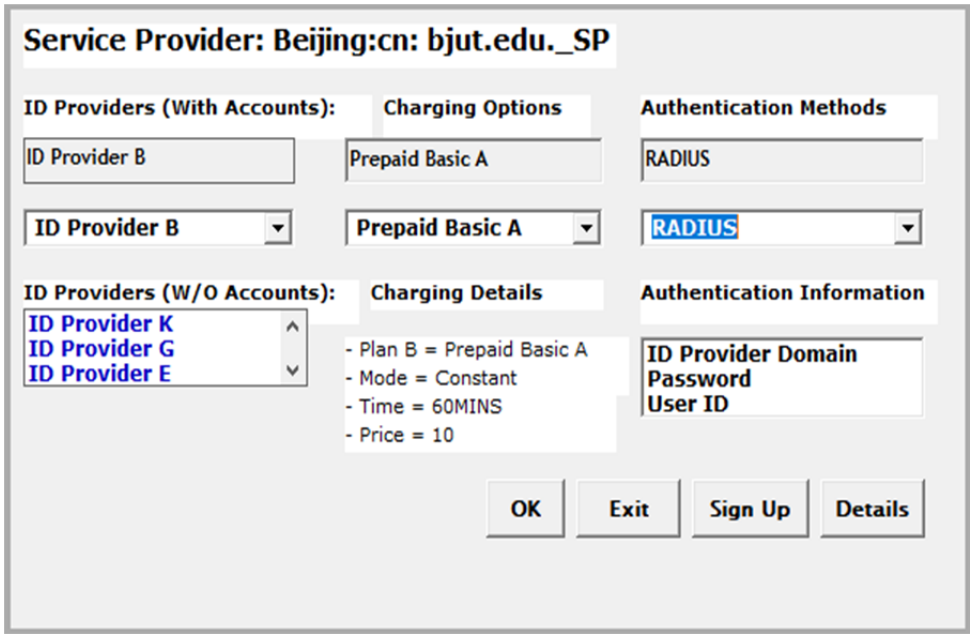


FIGURE 12. User interface design

7.2. **Overall architecture of the proposed authentication scheme.** This section describes the overall design of the proposed authentication framework and its strategic real-world components. On the client portion, the negotiation based client authentication is in control of encrypting and decrypting the authentication negotiation information, giving the authentication abilities information to clients via its GUI and gathering the user's selection and information. The policy engine on the client side can be self-reliant of this authentication framework. Negotiation client based authentication uses the policy engine rather than requesting the inputs from the user manually. In this scenario, the negotiation based authentication client passes the deciphered authentication abilities messages to the policy engine. The policy engine instantly verifies the charging option as per the user's terminal preferences. This means that the user intervention is not mandatory, except explicitly stated in the user's defined rules. On the server portion, analogously to the client portion, negotiation based authentication server is responsible for decrypting

and encrypting the authentication messages. When a server's authentication abilities information is requested, it re-claims it from the manager authentication abilities which is responsible for maintaining information prior to availing the information to other units. If all information is correct, it transmits them to authentication manager to take care of verification process and give back the result. The negotiation-based server makes use of the web server for the interchange of HTTP info with the client, i.e., for the primary conveyance functionality. The web server is capable of detecting if an acknowledged message belongs to the negotiation based authentication protocol and to validate if it has passed through the negotiation based authentication server. If it is a clear HTTP text information, then the web portal will be executed.

Figure 13 shows a demonstration of the key modules of the proposed scheme adopted. If the user cannot afford negotiation based authentication client mode, it adopts the upper dotted line, where the user's web browser and the server's web portal will be used during the authentication process.

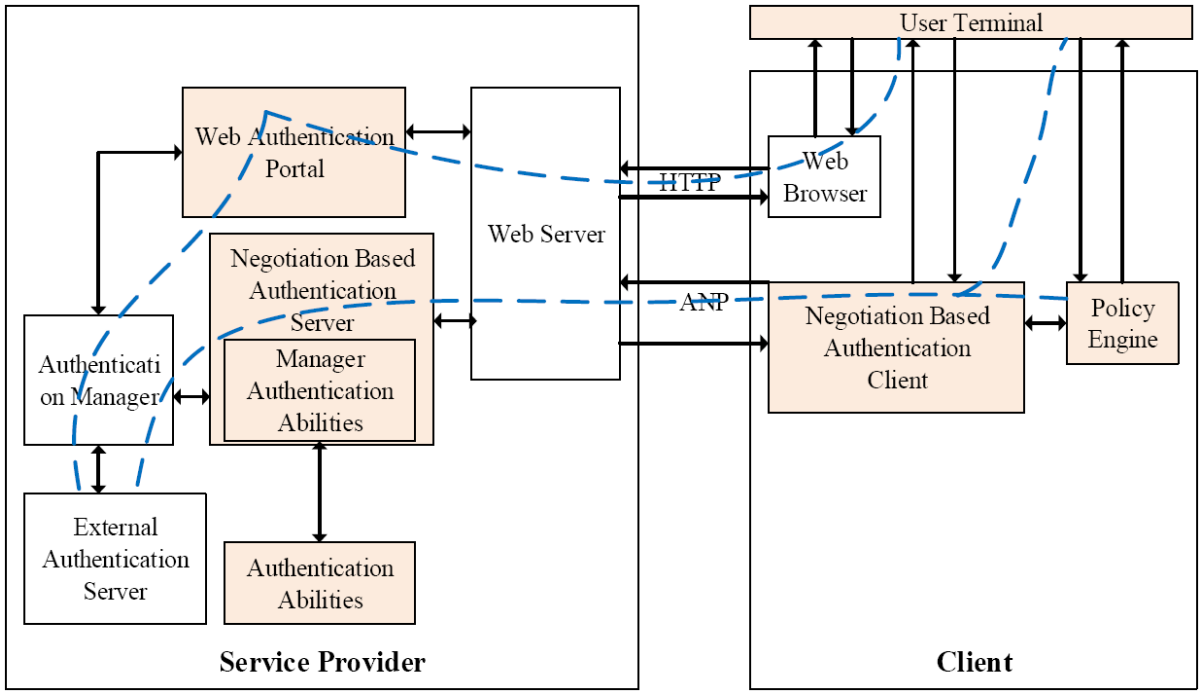


FIGURE 13. Overall design of the proposed authentication scheme

8. Securing Authentication of Web-Based Protocol and Access Control.

8.1. **Web-based security attacks.** Wi-Fi users authenticate themselves via web-based verification methods. Therefore, users can access IP level in the network prior to revealing their credentials. Open network authentication facilitates service authorization and accounting possibilities, lack of link layer cryptographic leads to possible security attacks such as service theft through IP and MAC spoofing, eavesdropping message modification and denial of service. IEEE 802.1X port-based network access control is being used in enterprises/corporate WLANs, and it uses such a cryptographic algorithm for client network authentication and access control [36] to yield cryptographically protected access in Wi-Fi-based networks.

To safeguard access to Wi-Fi-based networks, a composite layer 2 and web-based approach is sufficient. To use this technique, the WLAN SP must support 802.1X protocol

APs and AS(s). Nevertheless, a client that does not support 802.1X authentication can sidestep link-layer verification and cause threats to the network [37].

8.2. **Security threat analysis.** In this portion, the proposed composite layer 2 and web-based mechanism can tackle a variety of known security threats as described below.

a) Message Modification/Eavesdropping

L2 frames are encrypted by per-client session key that is provided by EAP-TLS in 802.1X authentication [38]. These vulnerabilities have been addressed in the 802.11i draft. Virtual Private Network (VPN) provides a secure data exchange remotely does prevent hackers from eavesdropping sensitive information during transmission.

b) Theft of Service

An imposter may spoof the IP or MAC address of an authorized client to offer the session. In the simulation process, theft of service is addressed where all clients are granted network resources via the RADIUS service. The web server differentiates the mischievous user from a genuine one by scrutinizing the MAC and session-digest key set in the web authentication request with the one informed by the RADIUS server. A more classy attack involves a rogue AP between the genuine user and the legitimate AP. IEEE 802.11i has suggested a countermeasure for attacks by man-in-the-middle attack by executing a 4-way handshake instantaneously prior to the 802.1X authentication process.

8.3. **Evaluation of authentication delay.** A testbed model has been developed to ascertain the practicability of the architectural concepts and integration of the system. Table 2 shows the components and open source software used during the experiment.

The setup consists of five servers: two IDPs, two SPs and one 802.1X AS. Access point connected to 802.1X AS with one wireless user terminal B and the other user terminal A connected to policy engine environment. Each server was connected using a 100Mb/s Ethernet cable and link delay was slight. All of them are implemented on typical Linux or Windows Personal Computers using open source software. Linux based operating systems

Table 2. Hardware components and open source software specifications

Hardware	Software
Identity Provider A: Toshiba Intel ® Pentium ® N3520 2.16 MHz (Linux)	GPL RADIUS v2 (ID/password) authentication server)
Identity Provider B: HP Intel ® Core ™ 2 Duo 2.20GHz (Linux)	GPL FreeRADIUS version 2 (802.1X authentication server)
Service Provider A: HP Intel ® Core ™ 2 Duo 2.20GHz (Linux)	XSupplicant v2.2.2 (802.1X client)
Service Provider B: HP Intel ® Core ™ 2 Duo 2.20GHz (Linux)	daloRADIUS Client v0.9.9
User Terminal A: Acer Intel ® Pentium IV 2.16 GHz (Windows 10)	Sun's Liberty prototype
User Terminal B: HP Intel ® Core ™ 2 Duo 2.20GHz (Windows 8.1)	LDAP Server v3
802.1X Authentication Server: HP Intel ® Core ™ 2 Duo 2.20GHz (Linux)	iptables v1.6.2 (Firewall)
WLAN Access Point: Cisco AIR-AP352	libwwwPerl 6.32 (Web client)
	VPN (psiphon3)
	VMware Workstation

were executed in VMware workstation as guest operating systems to avoid formatting the entire hard disk with Windows operating systems. To prevent wireless delay variance, link-layer authentication delay and other delay were conducted independently. The layout plan is depicted in Figure 14.

The study carried out the authentication delay in two scenarios: (1) the user terminal A with a negotiation client based authentication and a policy engine, and (2) the user terminal B with a web browser but with no policy engine nor negotiation client based authentication. In addition, the virtual private network is installed on the users' devices. During the experiment, the authors carried out two authentication schemes both locally and remotely. Table 3 shows the outcomes achieved for roaming authentication using the

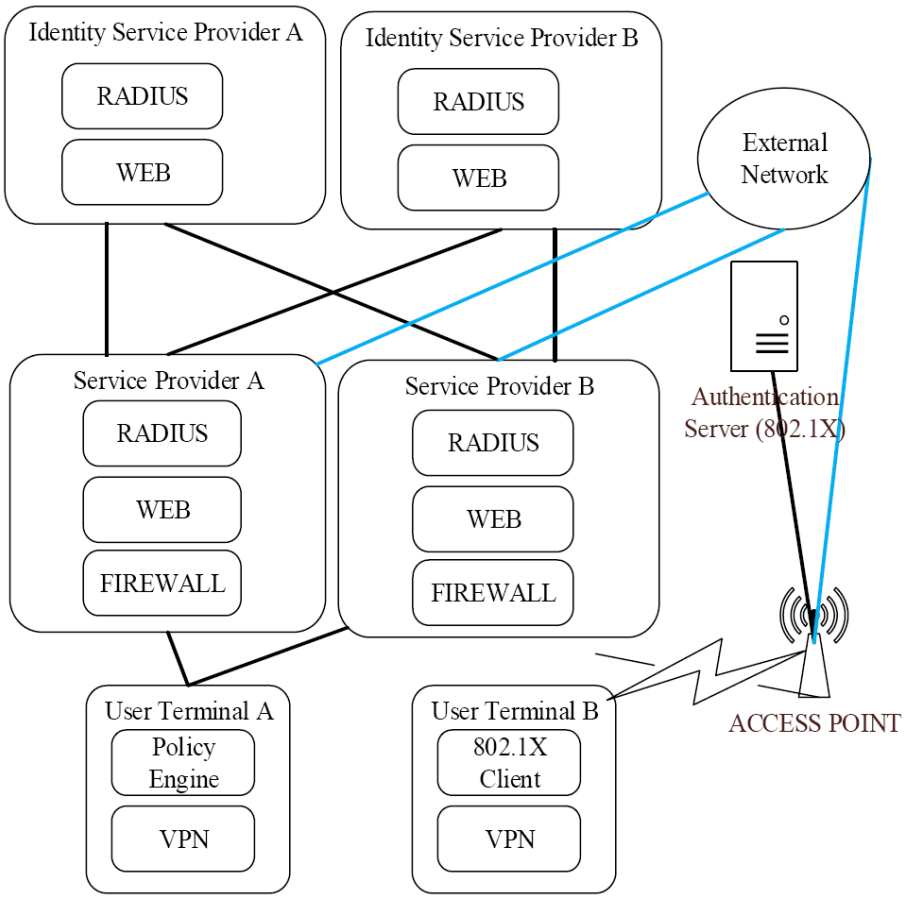


FIGURE 14. Testbed plans

TABLE 3. Authentication latency profile with negotiation based authentication and policy engine

	RADIUS (Proxy-based)		**Liberty (Redirect-based)**	
	Local	Remote	Local	Remote
Authentication via web browser	256ms	262ms	271ms	1311ms
Policy engine	212ms			
Authentication abilities statement	201ms			
802.1X authentication	154ms			
Total delay	731ms	829ms	838ms	1878ms

negotiation client based authentication to request the authentication abilities information to the server and the policy engine during data submission. The worse total delay noted in the worse case is 1878ms. This delay is suitable for a user roaming through multiple Wi-Fi networks.

Where a user does not use the verification adaptation client to request the authentication abilities statement to the server, he will validate by accessing a web browser and accessing the server web-based interface for authentication. The highest delay is when the user is redirected by a firewall to access the server web interface when trying to access protected information.

The delay in this scenario can be categorized into three: link-layer authentication, web authentication and firewall redirection. The firewall rerouting delay includes the discovery of an unauthorized user and his redirection to the web-based interface using Secure Sockets Layer (SSL). In this situation, the data is a swap over using Hypertext Markup Language (HTML). Apparently, the user's time entering the authentication details in the web authentication interface is ignored.

Web authentication latency is higher when negotiation based protocol is used during the interchange of information than using the plain HTML. The formation of SSL session in negotiation based scheme leads to long latencies for the web-based authentication process. When the authentication is executed using the standard web browser, the SSL session formation must be done in a standard way to secure user's information during redirection to the web authentication interface. Table 4 portrays an authentication delay outline with a web browser.

Table 4. Authentication delay outline with web browser

	RADIUS (Proxy-based)		**Liberty (Redirect-based)**	
	Local	Remote	Local	Remote
Authentication via a web browser	86ms	113ms	78ms	1.260ms
Authentication abilities statement	76ms			
802.1X authentication	154ms			
Total delay	316ms	343ms	308ms	1490ms

The main cause of delay in the negotiation-based protocol with policy engine is the parsing of XML files. Moreover, the server's authentication abilities information creation usually takes no time. Since the server, authentication abilities do not change frequently. The authentication abilities information is usually executed when the server is powered on. This data is usually modified when a change in the authentication abilities transpires.

9. **Conclusion.** Dynamic choice of the authentication method and the IDP is crucial for permitting the confederation of WLAN SPs under diverse trust levels and with substitute authentication methods. The proposed authentication framework hosts multiple authentication schemes. This study united two single sign-on mechanisms: the RADIUS framework and Liberty based architecture. A client policy engine allows the client to choose which substitute single sign-on authentication methods to adopt. The policy engine also guards the user's confidential information by compelling him to input authentication information when he roams into an SP in which the user does not trust. Moreover, a roaming agreement trust model with well-defined user-policies is rudimental in an environment of multiple SPs and IDPs to enable nomadism of a user. In addition, a composite Layer 2 and web authentication method thwarted service theft, eavesdropping,

and modification of message in 802.11-based networks. A robust model for single sign-on was developed to illustrate the strength of the approach.

This study carried out experiment locally and remotely in two classes: (1) in policy engine concatenated with negotiation based authentication standard and (2) authentication framework via web browsers. The results in policy engine with client negotiation authentication, compound L2 and web authentication mechanisms were 256ms, 212ms and 154ms respectively. These delays are acceptable to offer seamless user capability for multimedia applications as compared to the previous results achieved in [39-46].

In future, this study can be adopted in a vertical inter-technology WLANs milieu to integrate these networks to provide single sign-on value to ease users from creating several accounts of usernames and password while preserving the security concern.

REFERENCES

[1] M. Georgiades, N. Akhtar, C. Politis and R. Tafazolli, AAA context transfer for seamless and secure multimedia services over all-IP infrastructures, *The 5th European Wireless Conference – Mobile and Wireless Systems Beyond 3G*, Barcelona, Spain, pp.1-7, 2014.

[2] A. R. Prasad and H. Wang, Roaming key based fast handover in WLANs, *IEEE Wireless Communications and Networking Conference (WCNC)*, vol.3, pp.1570-1576, 2005.

[3] Y. B. Choi, J. Muller, C. V. Kopek and J. M. Makarsky, Corporate wireless LAN security: Threats and an effective security assessment framework for wireless information assurance, *International Journal of Mobile Communications*, vol.4, no.3, pp.266-290, 2006.

[4] C. T. Clancy, A. Mishra, H. M. Shin, J. L. Petroni and W. A. Arbaugh, Proactive key distribution using neighbor graphs, *IEEE Wireless Communications*, pp.26-36, 2004.

[5] D. Harkins and D. Carrel, The Internet key exchange (IKE), *IETF RFC 2409*, pp.1-41, 1998.

[6] T. Dierks and E. Rescorla, The transport layer security (TLS) protocol version 1.2, *IETF RFC 5246*, pp.1-104, 2008.

[7] E. Rescorla and N. Modadugu, Datagram transport layer security, *IETF RFC 4347*, pp.1-25, 2006.

[8] S. P. Vijayan, S. Venkataramani and V. Kulkami, *Systems and Methods for Mitigating Remote Authentication Service Unavailability*, United States Patent 8959588, 2015.

[9] P. Eronen, T. Hiller and G. Zorn, Diameter extensible authentication protocol (EAP) application, *Network Working Group*, pp.1-33, 2005.

[10] T. Clancy and K. Hoeper, Making the case for EAP channel bindings, *IEEE Sarnoff Symposium Conference Proceedings*, pp.1-5, 2009.

[11] B. Aboba and P. Cahhoun, *RADIUS (Remote Authentication Dial in User Service) Support for Extensible Authentication Protocol (EAP)*, pp.3-28, 2003.

[12] A. Masoumzadeh, M. Amini and R. Jalili, Context-aware provisional access control, *Information Systems Security*, pp.132-146, 2006.

[13] OASIS, eXtensible access control markup language (XACML) version 1.0, *OASIS Open*, 2003.

[14] S. Paul and S. Kumar, Comparative analysis of various PPP authentication protocols, *International Journal of Innovative Research in Computer and Communication Engineering*, vol.5, no.2, pp.1302-1309, 2017.

[15] M. Vysogorets and E. Shablygin, Authentication service, *WWPass Corporation*, pp.26-46, 2014.

[16] V. Bahl, A. Balachandran and S. Ventatachary, *The CHOICE Network: Broadband Wireless Internet Access in Public Places*, Technical Report MSR-TR-2000-21, 2000.

[17] H. Moustafa, G. Bourdon and Y. Gourhant, Authentication, authorization and accounting (AAA) in hybrid ad hoc hotspot's environments, *Proc. of the 4th International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots – WMASH'06*, p.37, 2006.

[18] A. Mishra, M. Shin and W. A. Arbaush, Context caching using neighbor graphs for fast handoffs in a wireless network, *IEEE INFOCOM*, vol.1, pp.351-361, 2004.

[19] J. Zhang, J. Li, S. Weinstein and N. Tu, Virtual operator based AAA in wireless LAN hot spots with ad-hoc networking support, *ACM SIGMOBILE Mobile Computing and Communications Review*, vol.6, no.3, pp.10-20, 2002.

[20] A. Hassan and X. Zhang, Bypassing web-based wireless authentication systems, *IEEE Long Island Systems, Applications and Technology Conference*, no.2, pp.1-4, 2011.

[21] OASIS, *Profiles for the OASIS Security Assertion Markup Language (SAML)*, 2005.

[22] OASIS, *Binding for the OASIS Security Assertion Markup Language (SAML)*, 2015.

[23] K. Wu and X. Yu, A model of unite-authentication single sign-on based on SAML underlying web, *The 2nd International Conference on Information and Computing Science*, vol.2, pp.211-213, 2009.
[24] K. S. Bhosale, M. Nenova and G. Lliev, The distributed denial of service attacks (DDoS) prevention mechanisms on application layer, *The 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*, pp.136-139, 2017.
[25] S. Fahmy, A. Nasir and N. Shamsuddin, Wireless network attack: Raising the awareness of Kampung WiFi residents, *International Conference on Computer & Information Science (ICCIS)*, pp.736-740, 2012.
[26] OASIS, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, 2015.
[27] Z. Wu, W. Huang and L. Yu, Design and implementation of unified identity authentication system based on LDAP in digital campus, *Advanced Materials Research*, nos.912-914, pp.1213-1217, 2014.
[28] Y. He, J. Li and H. Tang, Research of heterogeneous authentication information synchronization based on LDAP and web service, *International Symposium on Computational Intelligence and Design*, pp.52-55, 2010.
[29] S. K. Sood, A. K. Sarje and K. Singh, SSO password-based multi-server authentication protocol, *International Journal of Communication Networks and Distributed Systems*, vol.9, nos.1-2, pp.161-180, 2012.
[30] B. Zwattendorfer and A. Tauber, Secure single sign-on authentication using eIDs across public clouds, *International Journal of Internet Technology and Secured Transactions*, vol.5, no.4, pp.291-306, 2014.
[31] A. Hassan and X. Zhang, Bypassing web-based wireless authentication systems, *IEEE Long Island Systems, Applications and Technology Conference, LISAT 2011*, no.2, pp.1-4, 2011.
[32] B. Sundaram and B. M. Chapman, Policy engine: A framework for authorization, accounting policy specification and evaluation in grids, *Grid Computing – GRID 2001, Lecture Notes in Computer Science*, vol.2242, pp.145-153, 2001.
[33] B. Sundaram and B. M. Chapman, XML-based policy engine framework for usage policy management in grids, *Grid Computing – GRID 2002, Lecture Notes in Computer Science*, vol.2536, pp.194-198, 2002.
[34] R. Yavatkar, D. Pendarakis and R. Guerin, A framework for policy-based admission control, *IETF RFC 2753*, pp.1-19, 2000.
[35] G. Zheng, Design and solution scheme based on WEB accessing authentication, *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, vol.2, pp.897-901, 2008.
[36] V. Padmavathi, B. V. Vardhan and A. V. N. Krishna, Significance of key distribution using quantum cryptography, *International Journal of Innovative Computing, Information and Control*, vol.14, no.1, pp.371-377, 2018.
[37] J. B. Evans, W. Wang and B. J. Ewy, Wireless networking security: Open issues in trust, management, interoperation and measurement, *International Journal of Security and Networks*, vol.1, nos.1-2, pp.84-94, 2006.
[38] S. R. Tuladhar, C. E. Caicedo and J. B. D. Joshi, Inter-domain authentication for seamless roaming in heterogeneous wireless networks, *Proc. of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp.249-255, 2008.
[39] H. Aissaoui, P. Urien and G. Pujolle, Low latency of re-authentication during handover: Re-authentication using a signed token in heterogeneous wireless access networks, *International Conference on Wireless Information Networks and Systems (WINSYS)*, 2013.
[40] I. Martinovic, F. A. Zdarsky, A. Bachorek and J. B. Schmitt, *Measurement and Analysis of Handover Latencies in IEEE 802.11i Secured Networks*, Distributed Computer Systems Lab, University of Kaiserslautern, Germany, 2007.
[41] L. Zan, J. Wang and L. Bao, Personal AP protocol for mobility management in IEEE 802.11 systems, *MobiQuitous 2005: The 2nd Annual International Conference on Mobile and Ubiquitous Systems – Networking and Services*, pp.418-425, 2005.
[42] K. A. Kastell, Challenges for handovers in hybrid networks, *REVISTA TELECOMUNICAÇÕES*, vol.13, no.2, pp.52-59, 2011.
[43] L. Chen, T. Sun, B. Cheung, D. Nguyen and M. Gerla, *Universal Seamless Handoff Architecture in Wireless Overlay Networks*, UCLA Computer Science Department Technical Report CSD-TR No. 040012 Universal, pp.1-4, 2004.
[44] S. Shin, A. G. Forte, A. S. Rawat and H. Schulzrinne, Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs, *Proc. of the 2nd International Workshop on Mobility Management & Wireless Access Protocols*, pp.19-26, 2004.

[45] W. K. Lai and J. C. Chiu, Improving handoff performance in wireless overlay networks by switching between two-layer IPv6 and one-layer IPv6 addressing, *IEEE Journal on Selected Areas in Communications*, vol.23, no.11, pp.2129-2137, 2005.

[46] A. Wei, G. Z. Wei and G. Dupeyrat, Improving mobile IPv6 handover and authentication in wireless network with E-HCF, *International Journal of Network Management*, vol.19, no.6, pp.479-489, 2009.