I.J. Wireless and Microwave Technologies, **2022, 1, 41-53**
Published Online February 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2022.01.05

Enabling Trust in Single Sign-On Using DNS Based Authentication of Named Entities

Usman Aijaz N
HKBK College of Engineering / Department of Information Science and Engineering, VTU, HKBKCSERC Bangalore-560045, India
E-mail: uaijaz9@gmail.com

Nikita Mittal
Reliance Jio Infocomm Ltd, Mumbai, India.
E-mail: mittalnikita222@gmail.com

Mohammed Misbahuddin
CDAC (Centre for Development of Advanced Computing)/ACTS & BD Bangalore- 560 100
E-mail: mdmisbahuddin@gmail.com

A Syed Mustafa
HKBK College of Engineering / Information Science and Engineering, Bangalore-560045, India
E-mail: mustafas.is@hkbk.edu.in

Received: 24 August 2021; Revised: 23 September 2021; Accepted: 18 October 2021; Published: 08 February 2022

Abstract: Single Sign-On (SSO) allows the client to access multiple partner e-services through a single login session. SSO is convenient for the users as the user neither needs to set multiple login credentials nor login separately for individual services every time. SSO (single sign-on) authentication is a password-authentication approach that permits end users to login into multiple systems and websites with a single set of login credentials. SSO authentication is mainly useful for IT organizations that consist of many different commercial applications. The outstanding feature of SSO is that it gives organizations centralized control of their systems by giving different levels of access to each individual. It reduces password fatigue and increases security because users only need to remember a single username/password that grants them access to multiple systems. However, the Single Sign-on poses risks related to a single point of attack which may lead to a path for cybercrimes. This paper proposes a trust model to increase the security of Single Sign-on systems against the vulnerabilities discussed in the subsequent sections. The proposed Trust model is named as DANE-based Trust Plugin (DTP) which acts as an added security layer over DNS Based Authentication of Named entities(DANE). The DTP proposes the modified SAML XML schema which enables the DTP to counter the attacks.

Index Terms: DNS, DNSSEC, DANE, SAML, TLSA, IP Address, Digital Certificates

1. Introduction

The proper functioning of the Internet depends on Domain Name Systems (DNS) which translates the domain names (www.abc.com) into their corresponding IP addresses (such as 192.0.48.6) to enable routing of traffic to the right destinations. However, the original design of DNS in the 1980s did not consider security as a prime concern due to which spoofing attacks (due to lack of proper authentication) are possible these days such that a fraudulent user/system redirects a user to a malicious site without the user realizing it. IETF, the organization responsible for DNS protocol standards [19], has long realized the requirement of authentication and hence provided a solution called DNS Security Extensions (DNSSEC). DNSSEC uses the concepts of Public Key Cryptography for digitally signing the authoritative zone data to separate them from forged DNS data, thus enabling strong authentication. Although the authentication-related security issues were addressed, the validation of the TLS certificates issued by a valid CA is resolved by another protocol namely DNS-based Authentication of Named Entities (DANE). In DANE the SAML2 certificates stored with D-TS (DANE based Trusted Server) or federation operator are matched with the stored CERT RR (certificates in Resource Records of DNS). Besides the authentication of servers, under D-TS the DANE also checks the authenticity of the Identity Provider and the Service Provider. Moreover, with the increase in the number of web-based services many

service providers are enabling the Single Sign-On (Login once and access all services under SLA in the same session) for a better and convenient user experience.

Duo Security is a user-friendly authentication and access management solution invented by Cisco in the year 2018. Duo uses multi-factor authentication (MFA), remote access and device trust management, and adaptive access policy configuration. It produces a risk score for each login based on these factors. For high-risk logins, Duo requires users to verify their identity via integrated MFA[22]. The Ping Identity solution is designed in the year 2002 for easy cloud deployment and unlimited application integrations for all customers, partners, and employees. Its federated SSO is designed to work anywhere and from any device, and includes native support for identity standards such as SAML and OpenID Connect tokens. CyberArk combines SSO with adaptive multi-factor authentication so that in doubtful situations, users will need to verify their identity. CyberArk is delivered as a cloud-based solution, and so its Single Sign-On allows users to flawlessly log into their accounts across different browsers, mobile apps, and custom apps, with just one set of login details.

Okta provides a full suite of cloud-based identity management solutions. Okta offers fully-featured Single Sign-On solutions. It integrates across all of a users' web and mobile apps and is fully customizable.RSA offers an enterprise-grade multi-factor and access management solution. The primary functionality of RSA SecurID access is letting organizations consistently and centrally enforce dynamic risk-driven access policies. SecureAuth provides Single Sign-On as part of its identity management platform. It combines single sign-on and adaptive authentication to allow users to log in with one set of credentials to all of their accounts while using contextual factors to verify user identity

Some of the limitations of the above methods are one or more of the following

- Sometimes it feels like it requires users to update their password too often for simple input mistakes.
- Scalability- it is more likely to be used by companies than individuals.
- Although MFA reduces security problems related to access control still there are some security issues like the OTP tokens that can be compromised by man-in-the-middle or phishing attacks [20].
- The cost for licensing is high.
- Using a single password increases the chances of password vulnerability.
- Sometimes Issues in signing[21].
- Often it is super slow, which is time-consuming.

The SSO protocol will have the entities like Identity Provider (IdP), Service Provider (SP), and client. The identity Provider offers Identity registration, authentication, etc. while the Service Provider offers the services to the user. Trust plays a major role in SSO setup between IdP, SP, and client as SPs take the decision of offering services to users based on the assertion by IdP. This paper aims to show how the DANE protocol can be used to enable the Trust between IdP, SP, and Client by creating a trusted environment using a proposed modification to SAML assertions and bindings. The proposed modification is implemented using a Plug-in called DANE-based Trust Plugin (D-TP).

This paper is organized as follows: Section 2 presents a literature review, section 3 presents a brief description of SAML, Section 4 presents DNS, DNSSec, and DANE, and in the process introduces PKI concepts. Section 5 presents the Security Issues with SSO, Section 6 presents the research methodology of the proposed D-TP to prevent the SSO vulnerabilities. Section 7 presents results and discussion and Section 8 presents the conclusion and future work.

2. Literature Review

The traditional password-based authentication techniques need each user to not only log in to several remote servers repetitively but also remember many sets of usernames and passwords. This method is realistically impractical with the ever-increasing number of applications and services that need to be accessed by the user. To sort out the authentication issues numerous authentication schemes for Multi-Server Environment (MSE) have been proposed [11-16].

In 2000, Lee and Chang [14] first proposed a user identification protocol that offers session key establishment and user confidentiality for distributed computer networks. In 2004, Wu and Hsu [15] detected that Lee and Chang's protocol might suffer from masquerading attacks, and they proposed a modification to correct this issue. later on, Yang *et al.* [16] presented that Wu–Hsu's modified version could not protect the user's secret token against a malicious service provider, and they proposed an enhancement to avoid this kind of attack. In 2005, Lee [17] proved two possible attacks on Wu–Hsu's scheme. . In 2006, Mangipudi and Katti [19] exhibited a denial-of-service (DoS) attack on Yang *et al.*'s scheme and proposed an enhancement to overcome this drawback. Recently, Hsu and Chuang [21] presented that both Yang *et al.*'s and Mangipudi–Katti's schemes are susceptible to identity disclosure attacks and proposed an improvement to prevent such attacks.

In 2009, Liao and Wang [11] proposed a dynamic ID-based authentication protocol for MSE. Hsian and Shih [12] detected that Liao-Wang's protocol is susceptible to many attacks and proposed a better scheme. Later Shao and Chin [13].identified that Hsiang and Shih's protocol is susceptible to server spoofing attacks and fails to preserve user

anonymity. Lee et al., [14] proposed a better scheme but Li et al.[15] found that Lee et al.'s scheme is susceptible to forgery attacks and server spoofing attacks. They proposed their authentication scheme for MSE. In 2014, Madhusudhan and Adireddi [16] evidenced that Li et al.'s scheme is susceptible to replay attack, smart card loss attack, eavesdropping, and server spoofing attack

3. Security Assertion Markup Language

SAML is a standard Single Sign-On (SSO) protocol that provides a system for interchanging authentication and authorization between network nodes. The advent of SSO has led many web-based service providers to adopt it by replacing traditional multiple individual Sign-up systems requiring domain-specific credentials with a system. The SSO requires the client to log in to a system once and allows access to all the services offered by the organization's partner under SLA. Information used for authentication is exchanged through digitally signed XML documents via SSL links [1]. The process of digital signing and validation process is depicted in Figure 3.

SSO eliminates the need for every time signup verification as well as provides access to many services with a single sign-on thus enabling the user to experience the usability of the system. It also prevents users from remembering multiple complex passwords for different services thus reducing the burden of tedious password management. The service provider (SP) and identity provider (IdP) are the two main SAML providers. An SP needs IdP to provide client authentication. An IdP performs the authentication and sends SAML assertion to the SP along with the client's access rights.

However, the SP and IdP must be under a service level agreement (SLA) beforehand and exchange the security parameters/credentials such as Digital Certificates which plays important role in the exchange of communication.

4. DNS, DNSSEC, and DANE

Each system/device connected over the network has a unique IP Address that the other machine uses for identifying and communicating with that device. In the case of humans, remembering the IP address to access a particular service, provided through a server on Internet, is very difficult as a user has to remember numerous addresses for these services. Domain Name System eliminates the need for humans to memorize IP addresses by translating domain names to their respective IP addresses. Since 1985, DNS has been an essential component of the Internet. All IPs are maintained by the Internet Assigned Number Authorities (IANA) and Internet Corporation for Assigned Names and Numbers (ICANN) [5] [14]. DNS database is hierarchically distributed across the globe within DNS servers, which have resource records included in zone files.

There are mainly three types of DNS servers. 1) Recursive server which queries other DNS servers to get the IP address. 2) Iterative servers which provide the best answer it has without asking other servers, thus, reduces the additional overhead and providing faster responses. 3) Authoritative servers, which hold the IP address of the domain name being searched in its resource records and provide the address without further queries.

When a user searches for a domain name such as www.dnsexample.com, first the browser cache is searched for the IP address and then the query goes to the DNS recursive resolver which contacts the root server. There is a total of 13 root servers around the world [11] that maintain information about TLD servers and respond with the IP address of the needed TLD (.com IP in this case).

The recursive resolver uses this address and goes to TLD and gets the second level domain address (dnsexample.com in this case). Similarly, next, it goes to the subdomains server and so on till it reaches the final authoritative server where the IP of www.dnsexample.com could be found and returned. The system stores the new IP in cache and the HTTP request is loaded. The hierarchy of DNS is depicted in Figure 1.

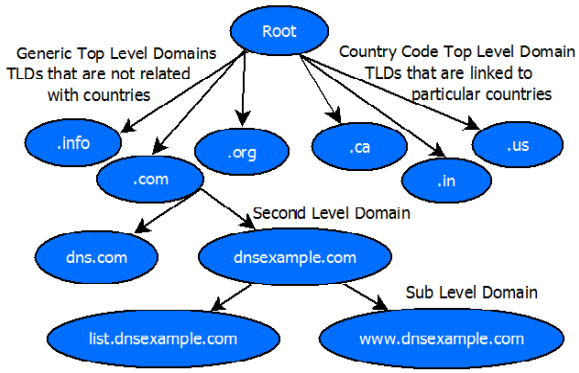


Fig. 1 DNS Hierarchy

4.1. DNS Vulnerabilities

Few of the DNS vulnerabilities discussed in [3][12] are presented here to explain in 'B', how DNSSEC resolves these issues. All the vulnerabilities discussed are depicted in Fig 2.

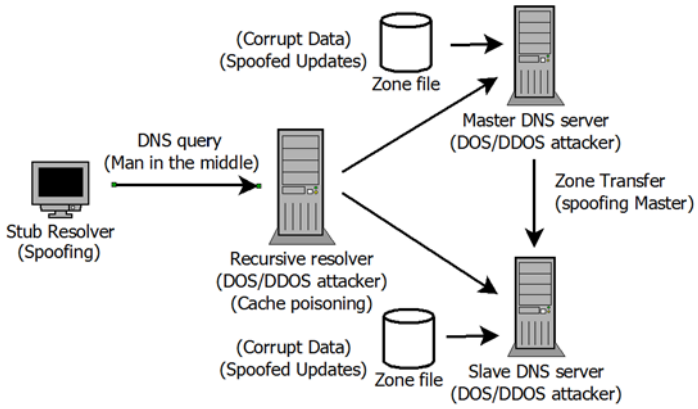


Fig. 2 DNS Vulnerabilities

- Cache Poisoning: Corrupt data is stored in the browser or recursive resolver cache by malicious nodes that route the user to bogus or phished websites.
- Impersonation: Since there is no sender or receiver verification in DNS which may lead to attacks such as Spoofing, Identity Theft, Man-In-The-Middle attack. Here a person or program can smartly impersonate another by imitating the open data, to gain an illegitimate advantage [12].
- Breach of Confidentiality: The open and unsecured communication in DNS allows the hackers to secretly listen to the private conversation thus breaching the data confidentiality.
- DDOS (Distributed Denial of Service): The attacker disrupts the services of a host connected to the Internet by flooding the target machine with dummy requests to overload systems and cause failure such that, the service becomes unavailable to users temporarily or indefinitely [3].

Public Key Cryptography uses a key pair wherein one is a Private Key known only to the user and another is a Public key published in the directory. Out of these one key is used for encryption and another key is used for decryption such that knowledge of the encryption key doesn't give knowledge about the decryption key [18].

Public Key Infrastructure (PKI) comprises of User, Digital Certificate, Digital Signature, CA, CRL, CPS as major components [18]. The Certifying Authority (CA) is responsible for validating the entity, issuance, and revocation of the certificate. The certificate issued will be digitally signed by CA which is then used for domains. The digital signature is the private key encryption of the message digest of the document using a one-way hash function. Digital Signatures are used to provide Authenticity, Integrity, and Non-repudiation to electronic documents. The unique property of the hash function and the irreversible nature of the one-way functions leads to the creation of a unique message digest for different documents and hence unique signatures. The digital signature implementations are done in such a way that the changes to a digitally signed document will not be allowed and if someone tries to do so, the software will remove the signature from the document thus preventing the breach of integrity.

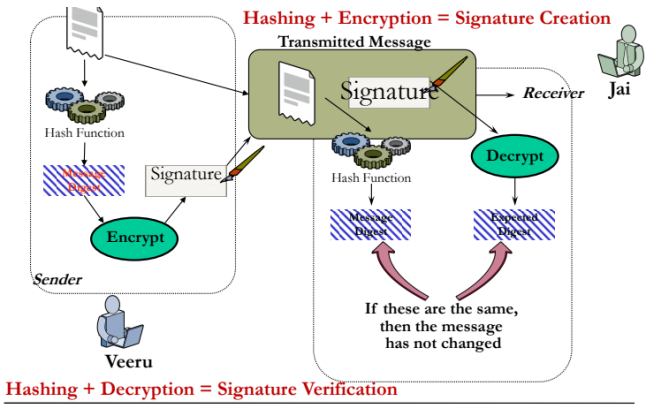


Fig. 3 Digital Signature Verification [6]

DNSSEC uses public-key cryptography to digitally sign the zone data. It does not encrypt the data but attaches cryptographic information to the DNS records which assures that the records are originated from the claimed source and are not modified during transmission. In the process of obtaining an IP address from the DNS lookup, it verifies the signature and checks its validity. This prevents the possibility of cache poisoning attacks. The complete process of obtaining an IP address through DNSSEC is explained in [9].

If the server fails in verifying at any of the stated constraints the process is stopped. Hence complete DNS chain of getting an IP address is shielded from Man-in-the-Middle attacks, spoofing, and identity theft. It is backward compatible with the current system that allows it to be clubbed over the existing protocol. To prevent hackers from deciphering the keys using the brute force method they must be updated regularly.

4.2 DNSSEC Limitations

Although it provides authentication of data, it fails to provide confidentiality and availability to the data.

1. The data sent over communication links are not encrypted making it prone to many security threats as discussed in [19].
2. It fails to redirect to the correct site in case the verification or validation of certificates fails to cause a denial of service [9].
3. Signed Zone files are larger which requires more time to process this increases the response latency making the loading of pages slower [9] also strengthening DDOS possibilities.

DANE is a set of new mechanisms and techniques that allows SSL/TLS to be bound to DNSSEC [4]. SSL/TLS over HTTP provides HTTPS used in the network protocol stack to provide a secure channel between the web server and the web browser. By using SSL both client and server sides are authenticated from their certificates during the handshake protocol. As well as the data transferred between them is protected by encrypting it thus eliminating the chances of phishing, tampering, eavesdropping, and packet sniffing this resolves the DNSSEC limitation discussed in Section. 3.2.1. SSL certificates digitally bind hostname, server or domain name, and geographical location of the organization.

IETF has developed a new type of DNS record for DANE that allows a domain itself to sign statements about which entities are authorized to represent it i.e. domain holders can specify which certificates can be used to authenticate that domain [7]. Eliminating the fear of attackers gaining fraudulent certificates by known or small-scale certifying authorities.

The new TLSA records include additional CA Constraints which specify the CA a client should trust. The Service Certificate Constraints specify the exact TLS certificate to be used to avoid their misuse. Lastly, the Trust Anchor Assertion specifies the trust anchor for validating the certificates. At the time of handshaking, domains are authenticated by checking trusted anchors and authorizing CA. Apart from additional certificates checking at each level of the communication chain, the procedure is the same as DNSSEC [17].

4.3 DANE Limitations

It succeeds in providing data confidentiality but does not guarantee the availability of data. The time complexities increase many folds because of TLS handshake, certificate validation, and then validating the chain of DNSSEC signatures. The lack of guarantee on availability may lead to an increase in the number of DOS/DDOS attacks. The proposed solution addresses this limitation as well and is discussed in the conclusion section.

5. Single Sign-on and its Security Issues

Single sign-on (SSO) is an authentication technique that allows users to securely authenticate with multiple applications and websites by using just one set of login credentials as shown in figure 3. For example, logging in to a Google account once will permit the user to access Google applications such as Google Docs, Gmail, and Google Drive.

Without the SSO technique, the website maintains a database of login credentials – username and passwords. Whenever the user login to the website, it checks the user's credentials against its database and authenticates the user. With the SSO, technique the website does not store the login credentials of users in its database. Rather, it makes use of a shared cluster of authentication servers where users are only required to enter their login credentials once for authentication

Some SSO services use protocols, such as Kerberos, and Security Assertion Markup Language (SAML). SAML is an extensible markup language (XML) standard that enables the exchange of user authentication and authorization data across secure domains. SAML-based SSO services include communications among the client, an identity provider that maintains a user directory, and a service provider.

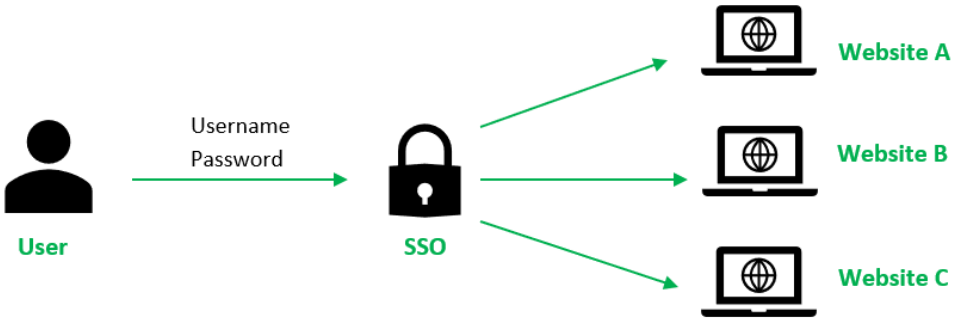


Fig 4. Single Sign-on

Consider the following scenario in Fig. 5 to understand the SSO process. A user is already logged into IdP and wishes to log in to a service provider (SP). The user requests the SP to allow access to its resources; the service provider redirects the user to IdP for verification purposes. IdP checks the user credentials with its database, and as per SAML standard, builds the authentication response in the form of an XML document containing the user's information and, signs it using an X.509 certificate, and posts this information to the service provider. The SP verifies the IdP signature and then allows the user to use the service based on the IdP response.

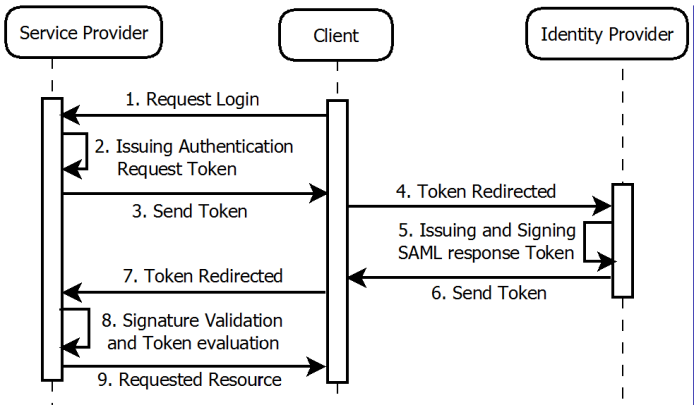


Fig. 5. SSO Signup Process

5.1 Security issues

1. A fraudulent node (MITM) can impersonate an SP and client and can successfully act as an SP for client and client for SP leading to Cross-Site Scripting or denial of service attack [1]. Figure 6 depicts the attack. SP can detect this attack by verifying the receiver of the authentication request and the sender of the authentication assertion are the same or not.
2. XML Signature Wrapping attack: SAML assertions are digitally signed and go to SP through the client's browser that can be skillfully tampered with a fake SAML assertion [10]. Figure 7 depicts the attack. The service provider detects this attack by comparing the signing ID with the assertion ID. If they match, the assertion is validated and if they do not match assertion is considered invalid.

The solution to the above attacks are discussed in the next section

6. Research Methodology

DANE protocol must be working on the systems at both ends of the communication channel. All communications links are secure SSL channels Because of DANE. We are using DANE based trust server to provide full security to the SAML SSO system. D-TP will use the DANE mechanism to authenticate the network entities within the trusted platform network as shown in figure 6.

The following use cases will explain the different scenarios which can occur and how D-TP will react to it to provide the user the needed security. We are providing the user with a choice if he/she wants to opt for higher security in the communication process. As comparatively the higher security option will be slower in working and if the user doesn't want that much security he/she can go for normal security which will be comparatively faster.

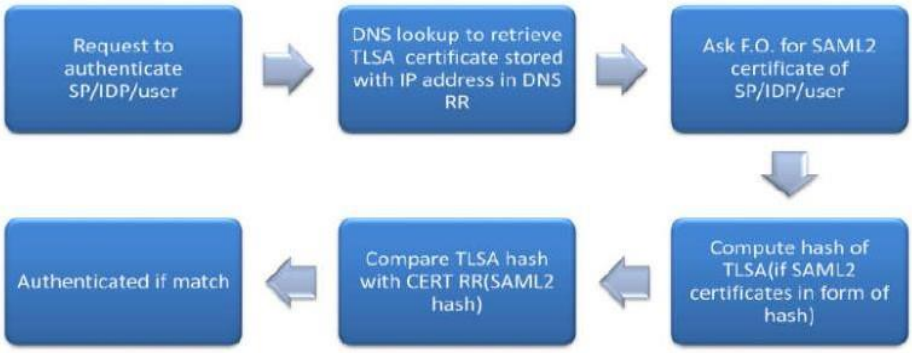


Fig.6. Information and message flow between the network entities

Use Case 1: If a new user wants to register using normal Security:

As shown in figure 7, First User Request the SP for service. SP post the request to IDP through Browser. IDP Request the User for credentials. The user returns the credentials to IDP. IDP Verify and store the information. IDP Response with signed assertions to SP. SP provides the Service if the user is authenticated.

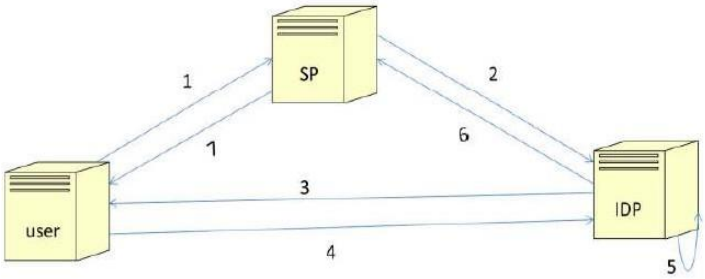


Fig.7. Use case 1, New user wants to register using Normal Security

Use Case 2: New user wants to register using a High level of security

As shown in figure 8, the First New user Asks D-TS to check SP. D-TS Verifies the SP and linked IDP's and sends Token containing verification of SP and IDP's to the client. The user Retrieves SP information from the token and acts accordingly. User Requests SP for service and forwards the received token to it. An authentication request from SP is posted to the IDP through the browser after checking IDP through the received token. IDP Asks the user for his/her credentials (name, location, id proof, etc). The user provides the details to IDP. IDP verifies the credentials by checking its database. Depending upon the verification of credentials a signed assertion is posted by IDP to the SP. Depending upon the signed assertion SP grants service to the user.

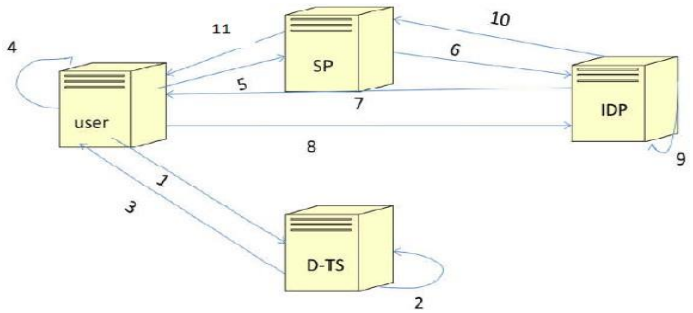


Fig.8. Use Case 2, New user wants to register using a High level of security

Use Case 3: If an already registered user wants to log in using a high level of security:

If the user is already logged in he/she doesn't need to register every time and can use his/her login ID and password to use the services provided by SP's of the trusted network. The process of login is as shown in figure 9.

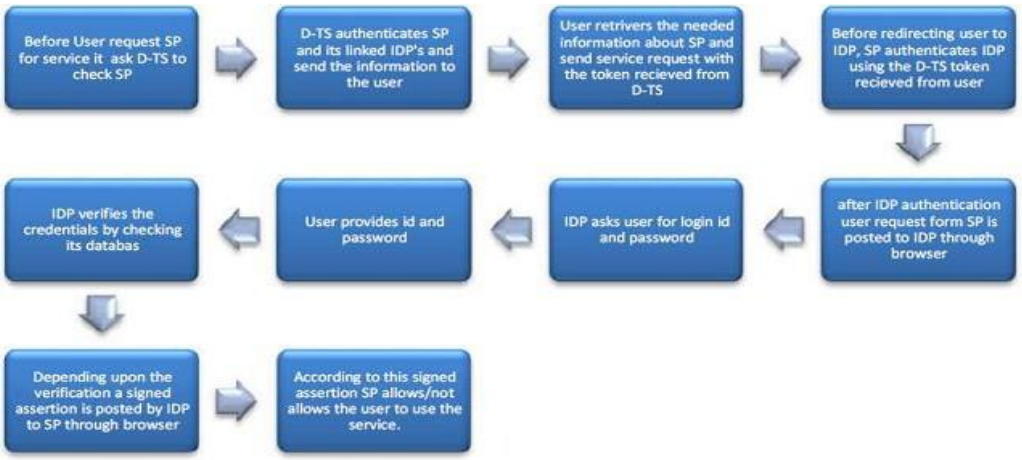


Fig.9. Information and message flow between the network entities

Use Case 4: If a new SP or IDP wants to join the trusted network.

In case a new service provider or new identity provider wants to join in the trusted network there is a provision to doso in this method and is shown in figure 10.

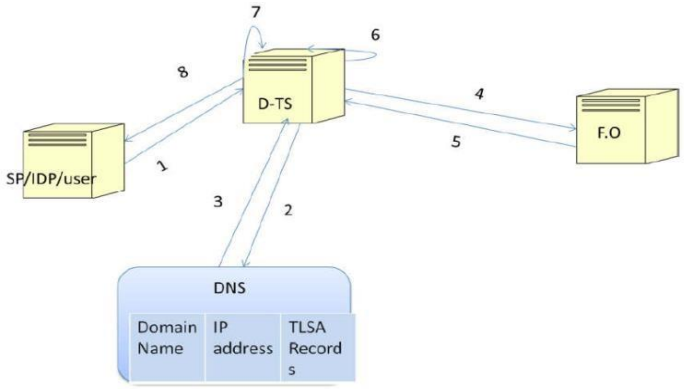


Fig.10. Use case 4, New SP or IDP wants to join in the trusted network

D-TP uses DANE to authenticate new SP or IDP using the following steps. A Request is sent to D-TS to authenticate SP/IDP/user. D-TP performs DNS lookup to retrieve the TLSA certificate stored with IP address in DNS RR. DNS returns TLSA Certificate to D-TP. D-TP asks F.O. for the SAML2 certificate of SP/IDP/user. F.O. returns SAML2 Certificates to D-TP. It computes the hash of TLSA (if SAML2 certificates are in form of hash) and Compares TLSA hash with CERT RR (SAML2 hash). If a match is found then SP/IDP/user gets authenticated. Figure 11 shows the Flowchart showing the information and message flow between the entities in the above case

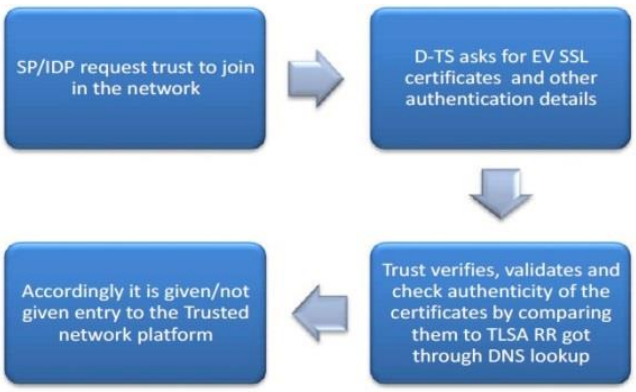


Fig.11. Information and message flow between the entities.

Building a trusted platform between identity providers, service providers, and the users provide many benefits that were not obtained until now with other protocols and drafts. A trusted network allows users to use the services freely without any fear of any kind of DNS attack. As well as it installs trust for SPs and IDP's in each other for secure and authentic communication.

6.1 Enabling Trust in SSO Using Dane

D-TP (DANE-based Trust Plug-in) is the proposed browser plug-in that acts as a third-party authenticator that validates the certificates of all the entities of the network maintaining a secure network in which users can freely access services at faster rates without compromising with security. DANE protocol must be working on the systems at both ends of the communication channel, as all communications links are secure SSL/TLS channels due to DANE and thus eliminates any kind of confidentiality and integrity threats during message transfer. The proposed D-TP must be installed at all the SSO entities including client, IdP, and SP. This section discusses how the proposed browser plug-in resists the attacks discussed above.

MITM*:* Figure. 12 depicts the issue discussed in section 5.1.1. The fraudulent node activity can be resolved if the SP can detect whether the receiver of the authentication request and the sender of the authentication assertion are the same or not [1]. In the proposed D-TP model, all communications take place over the DANE protocol which ensures that the sender verifies the intended receiver by validating and verifying its present certificates before the messages are exchanged. D-TP will authenticate and register each node before it enters the SSO network including SP, IdP, and clients. Without valid authentications, they will not be allowed to enter the system. D-TP will act as a supervisor to keep an eye on all the activities. Hence in the given scenario when the client wants resources from SP, it will validate SP first through the handshake mechanism of DANE and will then send the message requesting resources. Therefore, even if a fraudulent node tries to imitate as an SP it will fail in providing authentic certificates which can be easily detected in the DANE protocol

XML Signature Wrapping Attack (XSW): In the SSO system, IdP asks the client to provide credentials based on which it authenticates the clients. Then a response is a build that is signed by the Identity provider using its private key and sent as an assertion. A message can hold multiple assertions which are verified by the Service provider by comparing the signing ID with the assertion ID. If they match, the assertion is validated and if they do not match assertion is considered invalid. A service provider processes a complete response message even if one assertion is validated. As multiple assertions are allowed and this assertion response is sent to the Service provider through the client browser, an XML signature wrapping attack is possible [10]. Fig. 13 shows the point where this attack occurs while SSO sign-up process.

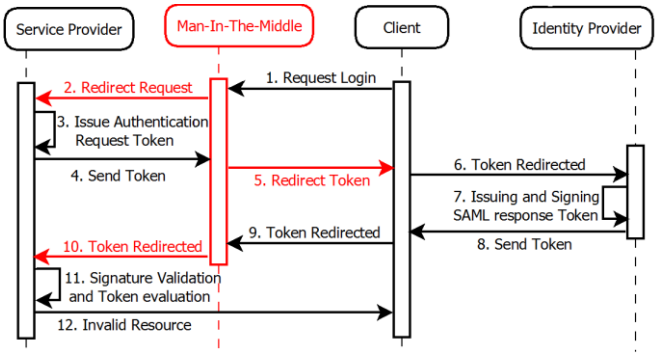


Fig. 12. Fraudulent Node Man in the middle attack

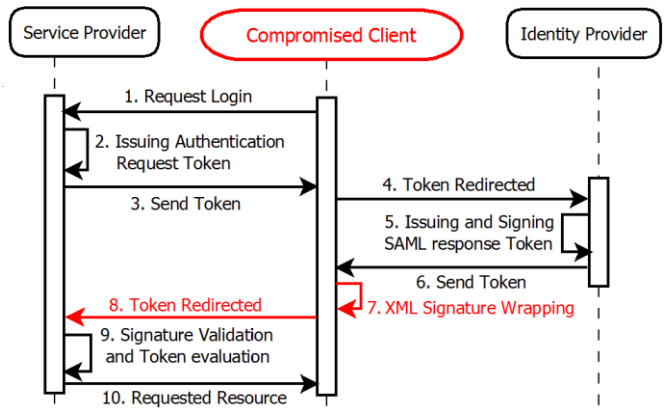


Fig. 13. Sign up Process with XML signature wrapping attack

The OWASP Top 10, a standard awareness document for developers and web application security lists the injection attack as the number one security risk in the 2020 list [13]. In the injection attack, the attacker inputs additional data or modifies the script with intentions of self-benefit [13]. XSW is a type of injection attack where the attacker uses the SOAP message response to check if the XSW is possible or not based on the assertion structures and then changes or inputs extra assertions to bypass the security checks [10]. Various ways through which XSW is possible are described in [10].

In the proposed D-TP, the XSW can be prevented by modifying the SAML XML schema. XML Schema is commonly known as XML Schema Definition XSD. It is used to describe and validate the structure and the content of XML data. An XML schema defines the elements, attributes, and data types. The schema element supports Namespaces. It is similar to a database schema that describes the data in a database. The main aim of the XML schema is to provide an inventory of XML markup constructs to write schemas. A schema intends to define and describe a class of XML documents by using these constructs to constrain and document the meaning, usage, and relationships of their constituent parts, data types, elements, and their content, attributes, and their values, entities, and their contents and notations. Schema constructs may also provide for the specification of implicit information like default values.

XML schema contains a single D-TP assertion signed by the private key of sender D-TP. Therefore, if a fraudulent node tries to surpass the D-TP assertion-check, similar to the SAML assertion by adding extra fake assertions, it can be detected as the fraudulent node does not have access to the original entity's private key and only one D-TP assertion can be present. Also if the client tries to replace the assertion with a fake assertion it can be detected as it will fail in key authentication when SP will use D-TP published public key to verify it. The D-TP assertion will hold the list of all true assertions that will be computed by matching the assertion ID with the IdP Signing ID. Based on this list the SP will process only the mentioned assertions ignoring the rest of the message.

The standard SAML XML schema structure can be referred to as form [15]. The proposed modification in SAML XML schema with D-TP messages is given below. …

</SOAP-ENV:Envelope>
<SOAP-ENV:Header>…<SOAP-ENV:Header>
<SOAP-ENV:Body><SAML:Response>
<saml:Assertion></saml:Assertion>
<D-TP :Assertion>
<Assertion Id>
<Asserted SAML Assertions ID List="…">
<D-TP signature>
<signatureInfo></signatureInfo>
<signatureID></signatureID>
</D-TP signature>
</D-TP_assertion>
</SAML:responce></SOAP-ENV:Body>
</SOAP-ENV:Envelope>

7. Result and Discussion

First-time user needs to be authenticated by entering their login credentials such as username/email and password in an SSO login page required by the Identity Provider(Idp) as shown in figure 14 below.

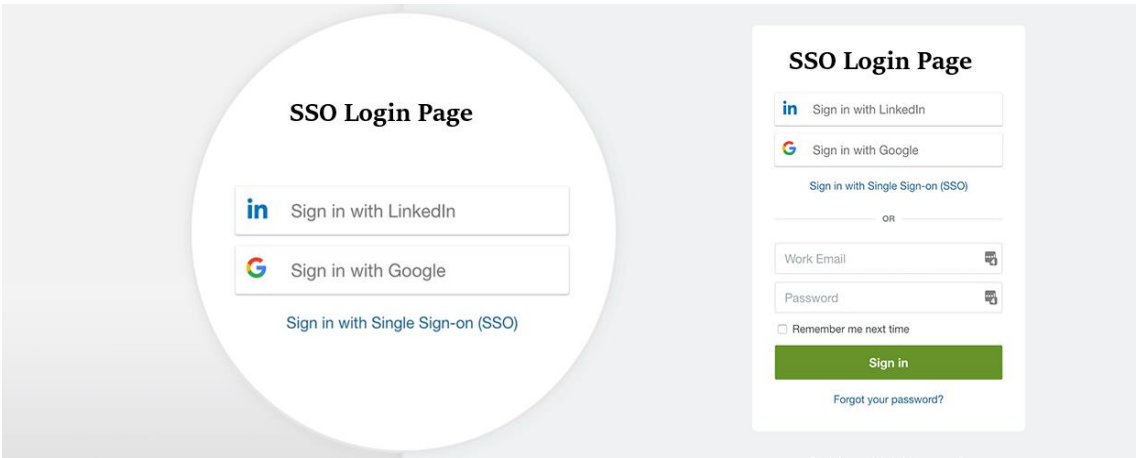


Fig.14. SSO login page

Once the IdP validates the user's login credentials, it sends an assertion back to the Service Provider(SP) to authorize successful authentication. The user will then get a list of frequently accessed applications as well as a list of all applications to which he can log in directly as shown in figure 15.

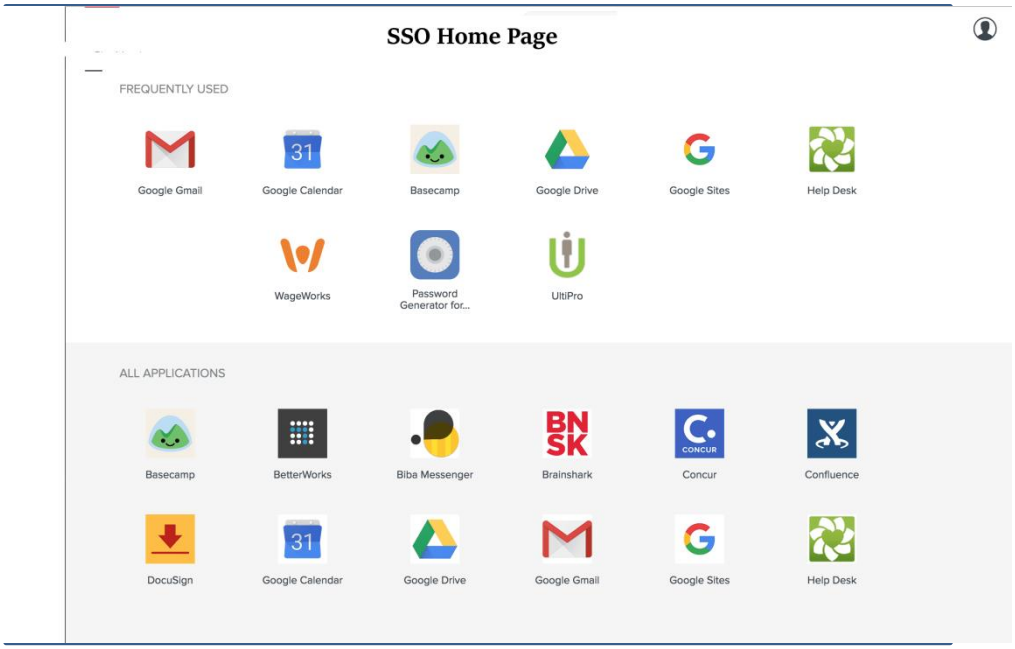


Fig.15. SSO Home Page

If the user clicks on the Google Gmail application then he will be granted access to his application without asking for his credentials as shown in figure 16.

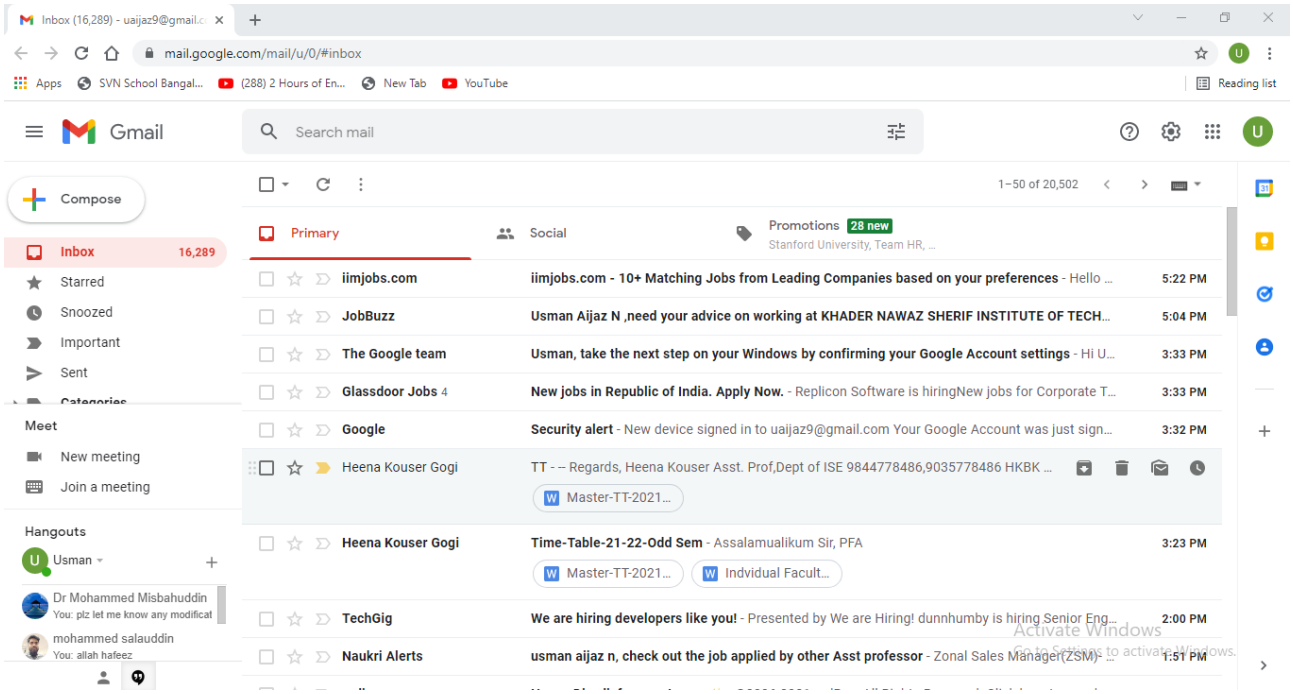


Fig. 16. SSO Google Gmail Page

8. Conclusion and Future Work

There are many SSO Solutions that exist in the market, most of them are using multifactor authentication methods. MFA method reduces security problems related to access control but still, it is vulnerable to man-in-the-middle and phishing attacks [20]. This paper concludes that SAML SSO security issues can be resisted by the proposed D-TP plugin which acts as another security layer over DANE. Thus providing added security to the users in the SSO

environment against man-in-the-middle and phishing attacks. D-TP does not require additional hardware or changes in configurations. It also prevents major implementation changes in the existing code and requires it to be installed as a plug-in. The security mode can be set based on the user's security requirement. D-TP reduces the time complexity and provides better data availability. Since the time delay is reduced, the possibility of the DOS/DDOS attack is also minimized. Also as only authenticated and registered nodes are allowed in the SSO network be it SP, IdP, or client possibility of such attacks by corrupted nodes is reduced which also resolves the DANE issues stated in issue 3 under section 4.3. As security depends somewhat on how difficult it is to factor in huge numbers, the quantum computer might easily decrypt messages using the brute force method [8]. Researchers are exploring the possibilities of using hybrid systems against quantum algorithms to develop a system that is more secure against attacks that can decrypt encryption keys [16]. Another way of improving Security is IP Encryption in which sent IP addresses will be encrypted such that they cannot be intercepted by a hacker. As IP encryption conversion poses a lot of size and length constraints, it is still under process [2].

References

[1] Armando A., Carbone R., Compagna L., Cuellar J., Pellegrino G., Sorniotti A. (2011) From Multiple Credentials to Browser-Based Single Sign-On: Are We More Secure?. In: Camenisch J., Fischer-Hübner S., Murayama Y., Portmann A., Rieder C. (eds) Future Challenges in Security and Privacy for Academia and Industry. SEC 2011. IFIP Advances in Information and Communication Technology, vol 354. Springer, Berlin, Heidelberg.

[2] B. Hubert, "On IP address encryption: security analysis with respect for privacy", May 2017 [Online] Available: https://medium.com/@bert.hubert/on-ip-address-encryption-security-analysis- with-respect-forprivacy-dabe1201b476

[3] B. Todd, Distributed Denial of Service Attacks, Feb. 18, 2000, [online] http://www.linuxsecurity.com/resourcefiles/intrusion detection/ddos–whitepaper.html

[4] Barnes, Richard (October 6, 2011). "DANE: Taking TLS Authentication to the Next Level Using DNSSEC". IETF Journal. Retrieved August 5, 2018.

[5] Cheshire, S. and M. Krochmal , "Special-Use Domain Names", RFC 6761, February 2013.

[6] DITISS– 2014 October, 2014, "Cryptography and PKI".

[7] Dukhovni, V. and W. Hardaker, "The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance", RFC 7671, Oct 2015.

[8] G.Gabriela, A Lopez & B. J. V. Brochero "Quantum Computing", 2019, DOI: 10.13140/RG.2.2.18905.36969.

[9] Herzberg, A., & Shulman, H. (2013). Towards Adoption of DNSSEC: Availability and Security Challenges. IACR Cryptology ePrint Archive, 2013, 254.

[10] J. Somorovsky, A. Mayer, J. Schwenk, M. Kampmann, and M. Jensen. "On breaking SAML: be whoever you want to be", In Proc. 21st USENIX conf. Security symposium (Security'12). USENIX Association, USA, pp. 1-21, 2012.

[11] List of root servers https://www.iana.org/domains/root/servers

[12] M. H. Jalalzai, W. B. Shahid and M. M. W. Iqbal, DNS Security Challenges and Best Practices to Deploy Secure DNS with Digital Signatures. Proceedings of 2015 12th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 13th – 17th January 2015.

[13] OWASP foundation, Inc. "OWASP top 10" [Online] Available: https://owasp.org/www-project-top-ten/# (accessed June. 9, 2020).

[14] Postel, J., "Domain Name System Structure and Delegation", RFC 1591, March 1994.

[15] S. Cantor et al. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite. Working Draft 06, 8 September 2015. Document ID sstc-saml-bindings-errata-2.0-wd-06.

[16] The National Academies Press," Qunatum Algorithms and Applications," in Quantum Computing: Progress and Prospects, 1st ed. of National Academies of Sciences, Engineering, and Medicine, us, 2019, ch iii, pp. 57-94.

[17] Vixie P., Gudmundsson O., Eastlake 3rd D., Wellington, B., "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[18] William Stallings, "Authentication Applications," in Cryptography and Network Security Principles and Practices, 4th ed. of Prentice-Hall, us, 2005, ch. xiv, sec. iii, pp. 427-430.

[19] Yao Y., He L., Xiong G. (2013) Security and Cost Analyses of DNSSEC Protocol. In: Yuan Y., Wu X., Lu Y. (eds) Trustworthy Computing and Services. ISCTCS 2012. Communications in Computer and Information Science, vol 320. Springer, Berlin, Heidelberg

[20] https://www.researchgate.net/publication/309225903_A_Review_on_Single_Sign_on_Enabling_Technologies_and_Protocols [accessed Nov 17 2021].

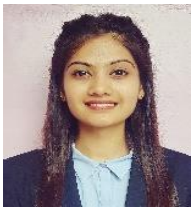
[21] https://www.trustradius.com/products/cisco-secure-access-duo/reviews?qs=pros-and-cons

[22] https://www.g2.com/products/duo-security/features.

Authors' Profiles

Mr. Usman Aijaz N did his B.E in (ISE) from Vidya Vikas College of Engineering in the year 2004, Mysore, VTU University, India. M.Tech (CSE) from Dayanand Sagar College of Engineering in the year 2010, Bangalore, VTU University, India. Currently pursuing a Ph.D. (CSE) in Cyber Security from VTU University, India.

He is having 16 years of Teaching Experience as an Assistant Professor. Currently, he is working as an Assistant professor in the Department of ISE at HKBK College of Engineering, Bangalore, India. He has published two papers one in Springer and the other in the IEEE International Conference on cyber security. His research area is Cyber Security and Machine Learning.



Nikita Mittal completed her bachelor's with the Gold Medal in Computer Science from the Indian Institute of Information Technology, Una in 2019. She is a Software Developer working with Reliance Jio, Mumbai. Her areas of research and interests include cyber security, big data analytics, AI, ML, soft computing, and image processing

Dr. Mohammed Misbahuddin did his B.Tech (CSE) from Gulbarga University, M.Tech (S/w Engg.) from JNTU-Anantapur, and Ph.D. (CSE) in Network Security from JNTU Hyderabad. He is currently working as an Associate Director (Scientist 'E') in Centre for Development of Advanced Computing (C-DAC), E-City, Bangalore. He is the Chief Investigator of the Cyber Security Awareness Project namely Information Security Education and Awareness (ISEA) – Phase II at C-DAC Bangalore. He is a key member of a Nationwide awareness project on Digital Signatures and PKI namely Next Generation PKI for Smart Applications. He is the Co-Investigator of a National Project named "e-Pramaan – A National e-Authentication Service along with Aadhaar". He has 17+ years of experience in Research, Training, and Project Management. He has applied for 3 patents with IPO in the area of Secure and Usable Authentication. He has been in various Programme committees of IEEE /ACM conferences and is a reviewer for two International Journals. His area of interest is Network Security & Cryptography especially Secure and Usable Authentication, Public Key Cryptography, and Risk-based Engines.

Dr. Syed Mustafa obtained his Ph.D. in Computer Science and Engineering from Satyabhama University, Chennai, India. He is currently working as a Professor and the Head of the Information Science and Engineering Department of HKBK College of Engineering under the Visvesvaraya Technological University. His area of research includes Web services, Web Mining, Social Media Data Mining, and Image Processing.

How to cite this paper: Usman Aijaz N, Nikita Mittal, Mohammed Misbahuddin, A Syed Mustafa, " Enabling Trust in Single Sign-On Using DNS Based Authentication of Named Entities", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.12, No.1, pp. 41-53, 2022.DOI: 10.5815/ijwmt.2022.01.05