IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Security Enhancement at Multiple Layers of SOA ReferenceArchitecture

Raj Kumar Mishra
Bhabha University,
Bhopal, India.

Manish Rai , Bhabha
University, Bhopal,
India.

Abstract— **SOA reference architecture consists of service provider and service consumer layer. Security enhancement at each layer is essential to ensure end to end security for an application.SOA provides better features like encapsulation, reusability, interoperability, modularity and composability. These features come along with security concerns which cause a major incident at a later stage for SOA projects. Based on security analysis of different SOA projects the author(s) found ignorance in implementation of security at many layers of SOA reference architecture. The proposed model enhances the security at each layer of SOA reference architecture which will improve service reliability and trust for service oriented architectural projects. This model will secure each service at each layer of SOA reference architecture. It uses the latest technology which helps in balancing the Service level agreement of the service after the security implementation.**

Keywords— Security; Reliability; Service-oriented architecture; Layers; Reference Architecture; Service level agreement

I. Introduction

The SOA reference architecture has nine layers which are used for designing a solution of the project. Each layer plays a vital role in project designing but security is a concern at each layer. SOA reference architecture has different capabilities which are being fulfilled in different layers which performs their assigned roles. This reference architecture uses a distributed model where tasks are divided into different layers based on their roles [9]. These tasks are part of the requirements which are being fulfilled in different layers of SOA reference architecture based on assigned task. The SOA reference architecture consists of service provider and service consumer. The service provider consists of Operational System Layer, Services Layer and Service Component Layer are considered as lower layers where as the service consumer layers consists of Consumer layer, Services layer, Business Process layer are considered as the upper layer of SOA reference architecture. Service implementation is done at Operational Systems layer, the Service Component Layer, and the Services Layer whereas support to business is carried out in Process Layer, the Consumer Layer, and the Integration Layer. The SOA reference architecture also includes four non-functional layers the Governance Layer, Information Layer, Quality of Service Layer and Integration Layer which are used to support different elements of SOA. The different layers of SOA reference architecture have been shown in figure 1:

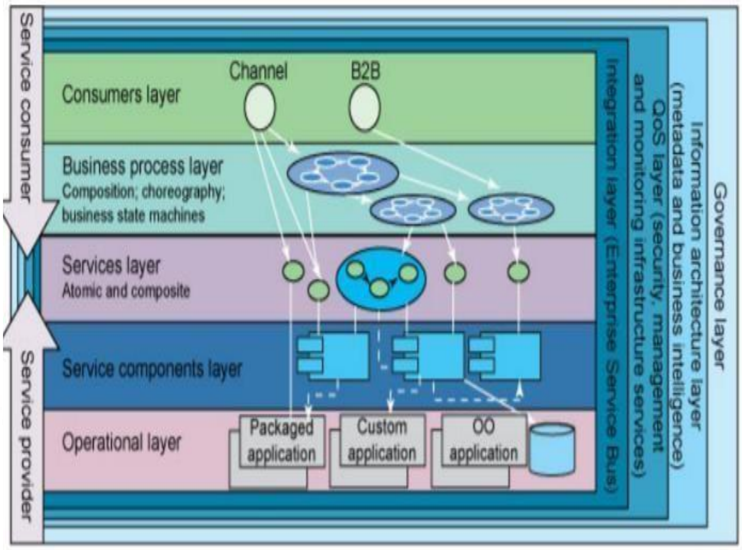

Service consumer
Service provider
Consumers layer
Channel
B2B
Business process layer
Composition; choreography; business state machines
Services layer
Atomic and composite
Service components layer
Operational layer
Packaged application
Custom application
OO application
Integration layer (Enterprise Service Bus)
QoS layer (security, management and monitoring infrastructure services)
Information architecture layer (metadata and business intelligence)
Governance layer

Fig 1: Layers of SOA Reference Architecture

Security is a concern for both service provider and service consumer. The author(s) found security concerns at each layers so proposed a model to implement security at granule level. Security must be included as part of the requirement. Security verification should be enabled at each layer of SOA reference architecture to enable end to security for SOA based projects[14, 19]. In the proposed model the authors(s) tries to enhance the security at each layer of SOA RA so that an application can be more secure and reliable.

In this paper, the author(s) tried to implement security at granular level to achieve almost complete security for an application. Section 1 defines the functionality of different layers of SOA reference architecture where author(s) identified security Issue at different layers. Section 2 describes different security issues. In section 3, the author(s) described the proposed model which will be helpful in implementing security at each layers of SOA reference architecture. In section 4, the author(s) validated the model using experimental analysis and fond reduction in security Issue. Section 5 includes the conclusion of the paper.

II. SECURITY ISSUES AT DIFFERENT LAYERS OF SOA REFERENCE ARCHITECTURE

In Service oriented architectural project, security Implementation is generally ignored where as security consideration is required from the beginning of the project. Security should not be considered as technology only, but it should be included as part of the business requirement [6]. SOA based projects faces some of the security challenges are listed by the author(s) as below:

- User service identification should be secured. Sometime the user credentials are propagated within and across organization causes security Issues.
- Security should be implemented at granular level to secure each service
- Security and Identity management should be secured
- Data in transit and at rest must be secured

Security challenges of service oriented architectural project can be divided into two parts :

1. Security Issues while Integrating different Infrastructure
   Different components have different security implemented like different authorization engines, identity and authentication systems causes issue in integration so called as SOA challenges.

2. Security management challenge:
   Managing the security of different SOA components is not easy. Lack of coordination, administration and resources causes security issue in SOA environments.

III. SECURITY ENHANCEMENT AT MULTIPLE LAYERS OF SOA REFERENCE ARCHITECTURE

SOA framework is based on an SOA reference architecture which has different layers to perform a specific role. Existing SOA RA based project uses security as a technology not as part of project implementation.The author(s) proposes security implementation at each layers of SOA RA so that end to end security for SOA based projects can be achieved [1,6] . SOA RA layers primarily divided into service consumer and service provider layer where author(s) are trying to implement security implementation along with project implementation. The author(s) also tries to maintain SLA of the interface same as existing interface implementation. End to end security can be enhanced for SOA RA using different tools and techniques, Project implementation must include security consideration in each phase of project deliverable so that security can be implemented and tested at a granular level [3,7]. Some of techniques which can be used to achieve end to end security for SOA based project has been identified by the author(s):

a. Identity and Authentication Services

It is a service which handles the user identity. User identity is being authenticated using different tools and techniques. We should have a standard framework for these services so that the security implementation should follow a standard and service can be more secure and reliable.

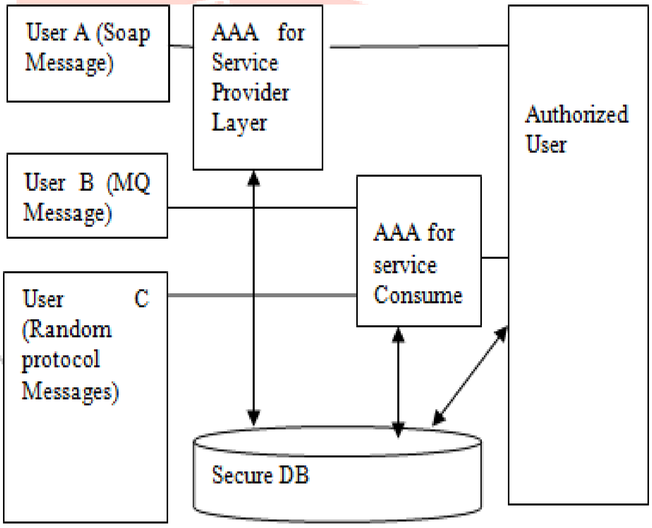
b. Policy Management f Policy

A Policy is one of the building blocks of the project. The project should have a good infrastructure to maintain the policy. This will help policy to complete policy life cycle. Policy management should follow a standard which will be helpful in ensuring enforcement of correct policies and securities.

c. Confidentiality and Integrity Services

It is a service which handles the data issue and protects the data from external attack. These services are used to enhance the security of an application. Secure socket layer (SSL) is one of the examples of confidentiality services which will help in protecting whole data stream at the protocol level below the application layer.

The author(s) proposes a model to enhance security for SOA reference architecture for each layer so that security can be enhanced at a granular level and each layer of SOA RA can be reliable, trusted and more secure:



——Security for SOA RA____
Figure 2: Layer wise security for SOA RA

The Author(s) proposes AAA (Authentication, authorization and accounting) for service provider layer and service consumer layer to ensure each layer of SOA RA is secured. Only authorized to use will able to enter the layers of SOA RA. The user details will be in securing DB cache, which will be helpful in authenticating the correct user. User

Identity will be saved in database. For authenticating any user, service will send a request to database to validate the user's identity. User credentials are matched with the saved details of the database. Fetching the data from the database each time might breach service level agreement so author proposes to use global cache where user details can be saved. These details are getting updated in case of any change in the database [13,16]. Security verification and validation using AAA has been shown in figure 3:

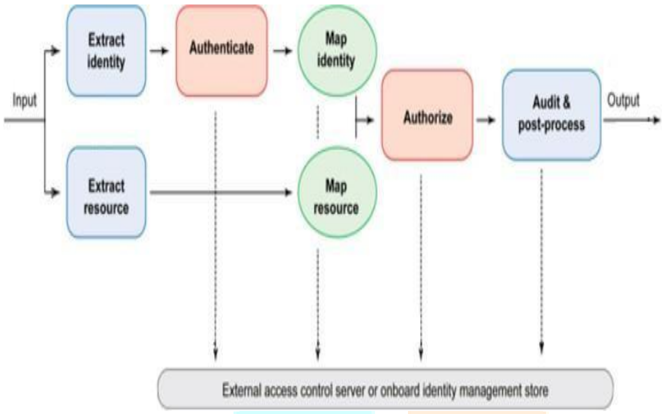


Figure 3: Overview of AAA(Authentication, authorization and accounting)

3.1 Security Enhancement at Service provider layers of SOA RA

A service provider of SOA RA consists of Operational System Layer, Service Component Layer, and Services Layer. These layers are also called as lower layers of SOA RA where security implementation is normally ignored causes incident at a later stage [2,4]. The author(s) proposes a model to enhance the security at each layer so that all layers of SOA reference architecture can be secured.

3.1.1 Security enhancement at Operational System Layer

The Operational system layer is a part of a service provider layer of SOA reference architecture. The operational system layer helps SOA solution in the design, deployment and runtime. This layer acts as an integration point between infrastructure as a service (Iaas) and the rest of SOA cloud computing service.Security Implementation at this layer will secure the design and deployment process. Implementation of AAA will not allow unauthorized persons to use the design or to deploy the content on the server [. This will improver service performance and security.

3.1.2 Security enhancement at Service Component Layer

The Service Component layer is used to implement the services. These services are used to build the services such as technical libraries or functional components. In most of cases, it has been analyzed that some unauthorized person is consuming the service which degrade the service performance. SOA provides reusability so that any persons within the system can use the service. But this leads to issue sometime. Many users consume the services without having permission from service owner. The Proposed will resolve this Issue where consumption of service allows for authorized users only.

3.1.3 Security enhancement at Services Layer

The layer consists of logical services which has service description, business capabilities and IT manifestation. These services are called when project is being designed. This layer is used by the project to implement the business functionality[4]. The Proposed AAA security mechanism will not allow any unauthorized persons to consume this service.

3.2 Security Enhancement at Service Consumer layers ofSOA RA

A service consumer layer of SOA RA consists of Services Layer, Business Process Layer, and Consumer Layer. These layers are called higher layer of SOA RA. In these layers security implementations exists which protect SOA application, but these security implementations are apart from project implementation. This freedom causes many security issues at these layers [5,10] . The author(s) tries to enhance the security for these layers by adding security implementation along with project implementation.

3.2.1 Security enhancement at Services Layer

This layer is an intermediate layer between service consumer and service provider. This area should be more protected so that any authenticated elements cannot enter to SOA layers [15] . AAA implementation of The proposed method will resolve this issue, Only authorized users will be allowed to enter to SOA layers.

3.2.2 Security enhancement at Business Process Layer

This layer of SOA reference architecture acts as coordinator, which fulfills the business requirements using IT solutions through collaborating with service layer, integration layer and information architecture Layer. Proposed method will verify the authentication at each layer in case of interaction with different layers. This will increase the security of the data and implementation will be safe from external attack.

3.2.3 Security enhancement at Consumer Layer

The Consumer Layer is the point where consumer interact with different layers of SOA. This Layer acts as an entry point for external consumers. This layer helps the business process to enable channel independent access. This layer provides capabilities required to deliver IT functionality and data to end user. It has the ability to integrate services from within the SOA [12]. Many new consumers added in this layer. Proposed method will verify the user's credentials before the consumption of the service of this layer.

3.2.4 Security enhancement at Integration Layer

This layer helps in routing and transforming the messages. It also helps in protocol conversion to support heterogeneous environments.Proposed method will allow only authorized user to perform the routing and transformation activities. This will not allow unauthorized developer to make changes in the service [17]. In SOA system, the developer who is not the owner of service can make the changes which lead the incident some time. Proposed method will reduce such incidents, only authorized person will allow to enter into the service.

3.2.5 Security enhancement at Governance Layer

This layer ensures the SOA solution in an organization are adhering to defined guidelines, policies and standard. This layer includes SOA governance and service governance. SOA governance layer ensures service consistency and service life cycle management. It is aligned with an SOA framework which defines an SOA reference model. Proposed model will verify and remove unauthorized users from accessing policies or guidelines.

3.3 End to end security enhancement using the proposed method

SOA based projects are attacked mostly so we should protect the services from different attacks like XML attack, WSDL attack, Phishing attack and SOAP attack. To protect SOA based projects from security attacks, different security techniques like data mining, XML encryption, Message confidentiality, Message integrity is used [8,11] . Some of the techniques to protect the services from security attack has been listed in table 1:

SOA RA Layer	Security Technique Implementation at SOA RA Layer	Protection from proposed Model
Service Consumer	XML signatures	XML attacks
Service Consumer	XML Encryption	WSDL attacks
Service Provider	Packet Level Authentication Information Key Exchange	Phishing attacks
Service Provider	Mining (Association, OLAP Cube, clustering)	SOAP attacks

Table 1: Different Security attacks and their protection

The Proposed method will implement AAA at each layer of the SOA reference architecture, keeping the SOA features unaltered. Services will be reusable, consumable, distributed deployable. But these functionalities will be allowed only for authorized users and authenticity will be verified at the beginning of the service of each layer. This will reduce unauthorized access of the service and attack on the service will be reduced. Also, It will reduce the incidence of different layers of SOA reference architecture which helps to ensure end to end security for SOA based projects [18,20].

The Author(s) proposes a framework to implement layer wise security for SOA based projects. The proposed framework uses some of IBM tools to implement security at each layer of SOA reference architecture.

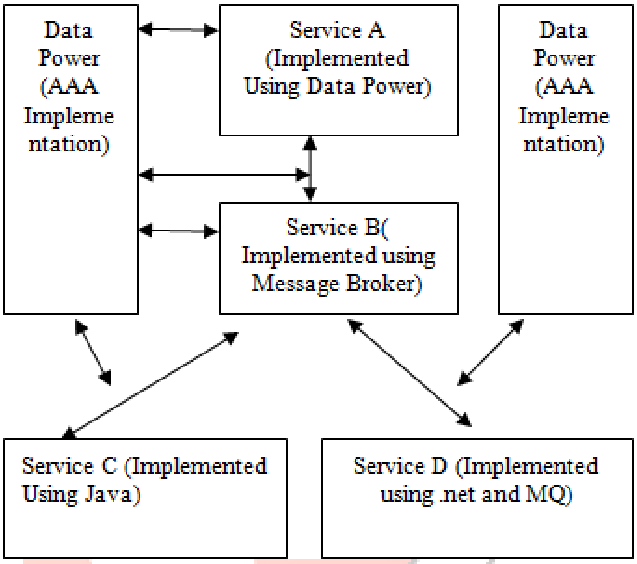

Data Power (AAA Implementation)
Service A (Implemented Using Data Power)
Data Power (AAA Implementation)
Service B(Implemented using Message Broker)
Service C (Implemented Using Java)
Service D (Implemented using .net and MQ)

Figure 4: Proposed Framework of security Implementation at multiple layers

In proposed model, the Author(s) have used different tool and technology for implementing security at each layers of service interaction. AAA has been implemented at data power as shown in figure 4, which is being called every time when service integration is done between different services. This implemented security for every service call. Data power has a global cache which helps in keeping service level agreement of each service unaltered. This framework will be helpful in implementing security at granular level which will increase service reusability and trust.

IV. Experimental Analysis

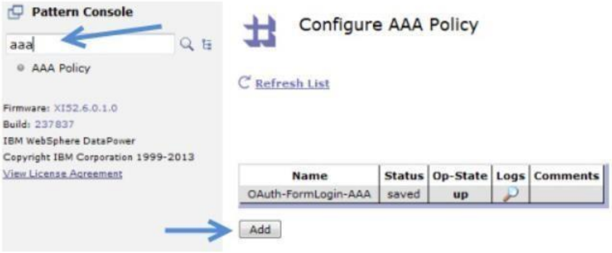
Service oriented architecture RA has an amount of flexibility, but security is a concern. The author(s) suggested to enhance the security at granular level of SOA RA and tried to implement the proposed model of security in some of projects. The author(s) collected the security gaps and implemented as part of project requirement which has been implemented at each layers of SOA reference architecture as mentioned in table 2:

SOA RA Security Analysis		
SOA RA Elements	Security element	Requirements
Security for service consumer	Service protection	Authority Authentication Confidentiality
Security protection	Service protection Service security Business process	Business security policy SOA security policy
Message Protection	Transport protocol Application security Protocol	Authority Authentication Confidentiality
Resource protection	Service registry Service description Business process	Privacy Authorization Audit
Security for Service provider	Service description	Security policy

Table 2: SOA RA Security Analysis

4.1 Proposed Security implementation using IBM Data Power as tool

After implementation of security at each layer, The author(s) compared the service level agreement (SLA) of some the services and found SLA is almost unaltered. It is because of global cache implementation for authentication and authorization of users. The author(s) suggested AAA(Authentication, authorization and accounting) implementation at each layers of SOA reference architecture. This can be implemented using different tools. The author(s) selected IBM Data power as a tool which has pre-configured security objects and implemented AAA as a service. This Service is called at each layer of SOA reference architecture before processing their assigned tasks.

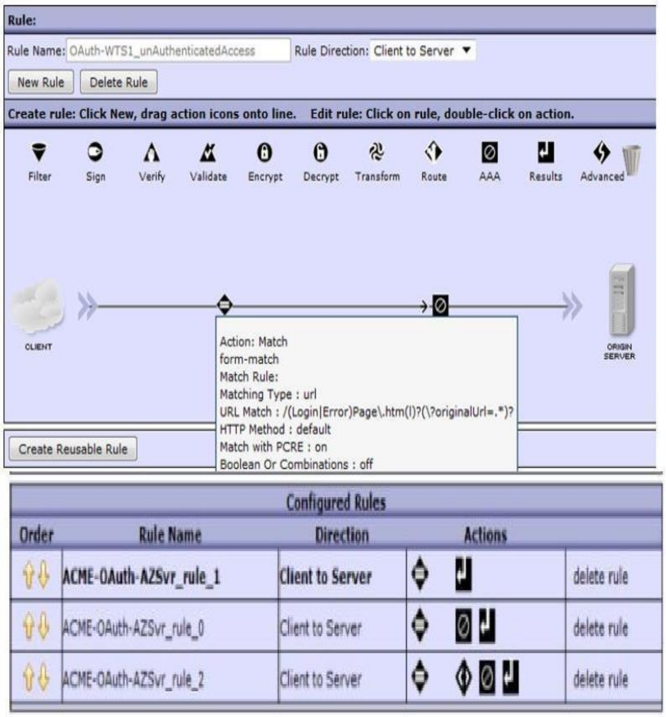


Firmware: XI52.6.0.1.0
Build: 237837
IBM WebSphere DataPower
Copyright IBM Corporation 1999-2013
View License Agreement

Name	Status	Op-State	Logs	Comments
OAuth-FormLogin-AAA	saved	up		

Figure 5: AAA configuration policy of IBM Data power

The Author(s) tested different application where services uses different tools like message broker, mq, .net and java. Service oriented architecture provides reusability, which becomes security concerns at a later stage. Using proposed framework, we can implement AAA security at a granular level. AAA security implemented using IBM data power as shown in figure 6 is being called at service interaction between the services.This policy also uses a global cache which is used for maintain service level agreement.



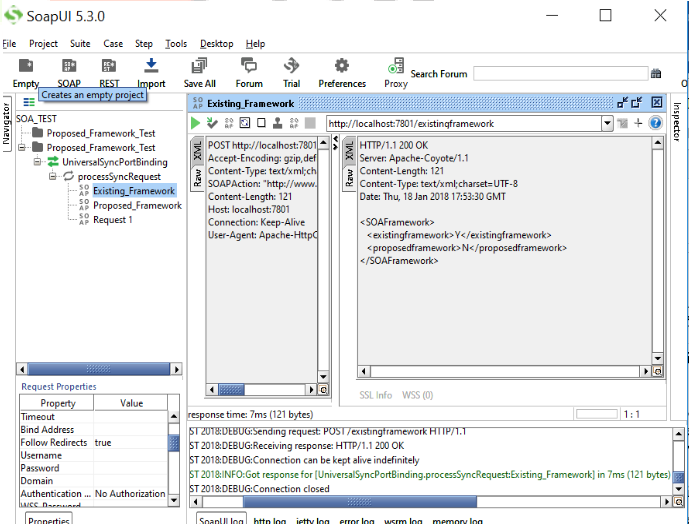
Rule Name: OAuth-WTS1_unAuthenticatedAccess
Rule Direction: Client to Server

Action: Match
form-match
Match Rule:
Matching Type : url
URL Match : /(Login|Error)Page\.htm(l)?(\?originalUrl=.*)?
HTTP Method : default
Match with PCRE : on
Boolean Or Combinations : off

Configured Rules				
Order	Rule Name	Direction	Actions	
↑↓	ACME-OAuth-AZSvr_rule_1	Client to Server		delete rule
↑↓	ACME-OAuth-AZSvr_rule_0	Client to Server		delete rule
↑↓	ACME-OAuth-AZSvr_rule_2	Client to Server		delete rule

Figure 6 : AAA security policy in IBM data Power

After implementation of security, the model has been tested using SOAP.Firstly, the author(s) tested the service in existing SOA environment as shown in figure 6:



http://localhost:7801/existingframework

```
POST http://localhost:7801
Accept-Encoding: gzip,def
Content-Type: text/xml;ch
SOAPAction: "http://www.
Content-Length: 121
Host: localhost:7801
Connection: Keep-Alive
User-Agent: Apache-HttpC
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 121
Content-Type: text/xml;charset=UTF-8
Date: Thu, 18 Jan 2018 17:53:30 GMT

<SOAFramework>
  <existingframework>Y</existingframework>
  <proposedframework>N</proposedframework>
</SOAFramework>
```

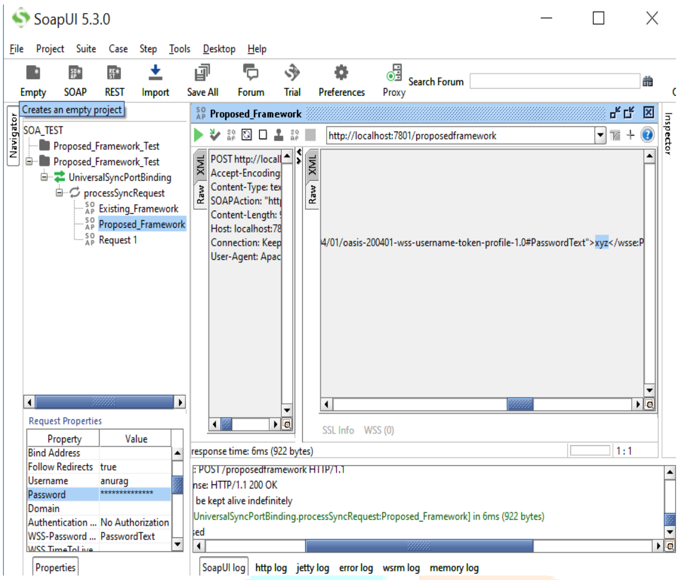
Property	Value
Timeout	
Bind Address	
Follow Redirects	true
Username	
Password	
Domain	
Authentication ...	No Authorization
WSS Password	

response time: 7ms (121 bytes) 1 : 1

```
ST 2018:DEBUG:Sending request: POST /existingframework HTTP/1.1
ST 2018:DEBUG:Receiving response: HTTP/1.1 200 OK
ST 2018:DEBUG:Connection can be kept alive indefinitely
ST 2018:INFO:Got response for [UniversalSyncPortBinding.processSyncRequest:Existing_Framework] in 7ms (121 bytes)
ST 2018:DEBUG:Connection closed
```

Figure 6: Existing SOA framework test

The author(s) performed same test in Proposed model shown in figure 7 and found increase in security where as service response time was almost same as existing framework service:



http://localhost:7801/proposedframework

```
POST http://local
Accept-Encoding
Content-Type: tex
SOAPAction: "htt
Content-Length: 
Host: localhost:78
Connection: Keep
User-Agent: Apac
```

```
4/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">xyz</wsse:P
```

Request Properties

Property	Value
Bind Address	
Follow Redirects	true
Username	anurag
Password	**************
Domain	
Authentication ...	No Authorization
WSS-Password ...	PasswordText
WSS TimeToLive	

response time: 6ms (922 bytes)

```
: POST /proposedframework HTTP/1.1
nse: HTTP/1.1 200 OK
 be kept alive indefinitely
UniversalSyncPortBinding.processSyncRequest:Proposed_Framework] in 6ms (922 bytes)
ed
```

Figure 7: Test result of Proposed Framework of SOA security

The author(s) tried implementing the authentication for each service at each layer of SOA RA using proposed model and found no impact of SLA of service, test result using SOAP UI has been shown in table 3 :

Parameter	Result of existing model using the SOAP UI	Result of proposed model using the SOAP UI
Service Response time in ms	7	7
Service response after implementation of Service authentication using userid and password in ms	7	6

Table 3 : Experimental result using the SOAP UI

The author(s) also found significance decrease in different attacks like Man in the middle attack, Message alteration, SOAP attack, Path/Field/SQL injection, Malicious morphing. The proposed model validates the user at each layer and allow authorized users only access the data which reduces a number of attacks. The Data power acts as a gateway of each layer which removes unauthorized users to access the data. The author(s) compared leagacy Service oriented architecture security Framework and Proposed service oriented atrchitecture security framework as shown in table 4s:

Security Parameter	Existing SOA Security Framework	Proposed SOA Security Framework
Message propagation Security in percentage	70	95
Average Service level agreement in millisecond	7	8
Security at service consumer layers in percentage	60	85
Security at service provider layers in percentage	20	85
Reliability in percentage	63	85
Authentication/Autherization in percentage	60	95
Increase Privacy in percentage	55	95

Table 4 : Comparison of Legacy security model Vs Proposed model

The Author(s) have collected data from 50 project to validate the model using t –test :

Steps of t-test for comparison of the existing Model vs the proposed Mode Table 3.

STEP 1. Null Hypothesis: Let us assume that the proposed implementations have no statistically significant difference in security. Alternative Hypothesis: Proposed implementations have a statistically significant increase in security.

STEP 2. Level of significance(α) = 0.05

STEP 3. The degree of freedom = 10

t-Test: Existing Model Vs Proposed Model		
	Existing Model	Proposed Model
Mean	44.16666667	75.5
Variance	587.7666667	1117.5
Observations	6	6
Hypothesized Mean Difference	0	
Df	9	
t Stat	c	
P(T<=t) one-tail	0.048013591	
t Critical one-tail	1.833112923	
P(T<=t) two-tail	0.096027183	
t Critical two-tail	2.262157158	

Table 4: t -test result

STEP 4. Here, variances s1= 587.7666667 and S2 = 1117.5
STEP 5. Using t-test, t Stat = -1.85860059839923, t Calculated =absolute (t Stat)= 1.8 and t Critical two-tail = 2.26
STEP 6. Here, t Calculated > t Critical and P(T<=t) onetail (0.005) < α (0.05). So, the Null hypothesis will be rejected. This indicates that the proposed implementations have a statistically significant increase in security. This t-test validates that the proposed model enhances the security features for service-oriented architectural projects without impacting the existing service level agreement for the services.

Statistical analysis of legacy model Vs proposed model has been shown in figure 3:

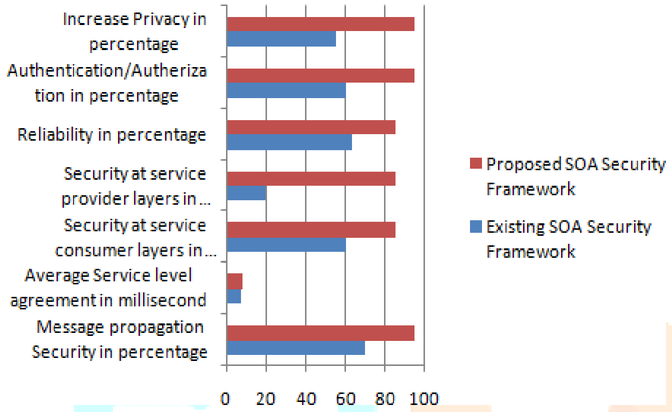


Fig 3 : Statistical comparison of security Framework

The Author(s) found increase of security at each layers after implementation of the proposed model which decreased number of attacks on SOA services which makes SOA service more secure and reliable.

V. Conclusion

Security is one major concern for SOA based projects. The author(s) found security issues at each layer of SOA reference architecture so proposed a model to enhance the security at each layer of SOA without impacting service level agreement. The proposed model has been tested on some the projects where author(s) found security enhancement at each layer and decrease in security attacks on SOA services. This model will helpful in securing an end to end security for the project and will also increase trust and reliability.

References

[1] Shashwat, Anurag & Kumar, Deepak. (2020). Service identification by enhanced K-mean algorithm in service-oriented architecture. International Journal of Process Management and Benchmarking. 10. 132. 10.1504/IJPMB.2020.104237.

[2] Shashwat, Anurag & Kumar, Deepak & Chanana, Lovneesh. (2019). A Framework with Enhanced Security for Service Oriented Architecture. International Journal of Sensors, Wireless Communications and Control. 09. 10.2174/2210327909666190710122505.

[3] A. Shashwat and D. Kumar, "A service identification model for service oriented architecture," 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, 2017, pp. 1-5, doi: 10.1109/CIACT.2017.7977299.

[4] A. Shashwat, D. Kumar and L. Chanana, "Service Level Security Enhacement for Service Oriented Architecture," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, Uttar Pradesh, India, 2018, pp. 79 -83, doi: 10.1109/GUCON.2018.8674897.

[5] A. Shashwat, D. Kumar and L. Chanana, "Message Level Security Enhancement For Service Oriented Architecture," 2018 4th International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, 2018, pp. 1-6, doi: 10.1109/CIACT.2018.8480347.

[6] A. Shashwat, D. Kumar and L. Chanana, "An end to end security framework for service oriented architecture," 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, 2017, pp. 475-480, doi: 10.1109/ICTUS.2017.8286056.

[7] Attri, R. and and Grover, S.(2017) 'Developing the weighted ISM-MICMAC framework for process design stage of production system life cycle', Int. J. Process Management andBenchmarking, Vol. 7, No. 1, pp.94–119.

[8] Mohamed Ibrahim B, Mohamed Shanavas A R. Identifying SOA Security Threats using Web Mining International Journal of Computer Applications 2015; 120(4)

[9] Identifying SOA Security Threats using Web Mining, International Journal of Computer Applications (0975 – 8887) Volume 120 – No.4, June 2015

[10] Macy Wong; Ronnie Cheung, " Service improvement in Hong Kong retail banking through satisfied and committed employees", Int. J. of Process Management and Benchmarking, 2014 Vol.4, No.1, pp.3 – 21

[11] Badr Y, Banerjee S. Managing End-to-End Security Risks with Fuzzy Logic in Service-Oriented Architectures 2013 IEEE Ninth World Congress on Services Santa Clara, CA. 2013; pp. 2013; 111-7. [http://dx.doi.org/10.1109/SERVICES.2013.28]

[12] Masood A. Cyber security for service oriented architectures in a Web 2.0 world: An overview of SOA vulnerabilities in financial services 2013 IEEE International Conference on Technologies for Homeland Security (HST) Waltham, MA. 2013; pp. 2013; 1-6. [http://dx.doi.org/10.1109/THS.2013.6698966]

[13] Azarmi M, et al. An End-to-End Security Auditing Approach for Service Oriented Architectures IEEE 31st Symposium on Reliable Distributed Systems Irvine, CA. 2012; pp. 2012; 279-84. [http://dx.doi.org/10.1109/SRDS.2012.5]

[14] Kalantari, A., Khezrian, M., Esmaeili, A. and Taherdoost, H. (2011). Enabling Security Requirements for enterprise Service Oriented Architecture. International Journal of Recent Trends in Engineering and Technology, the Association of Computer Electronics and Electrical Engineers (ACEEE), 6(1), 75-81.

[15] Security Model for Service-Oriented Architecture, Advanced Computing: An International Journal (ACIJ), Vol.2, No.4, July 2011

[16] Ramarao,k. & Prasad, C.(2008). SOA Security. USA: Manning Publication.

[17] Da Veiga, A. and J.H.P. Eloff, "An Information Security GovernanceFramework. Information Systems Management", 2008(24): p. 361-372

[18] M.Veger, "A Stage Maturity Model for the adoption of an enterprise wide Service-Oriented Architecture (SMM-SOA), University of Twente, Enschede, Netherlands, 2008.

[19] Eric Pulier & Hugh Taylor (2006) Understanding Enterprise SOA. USA Manning Publication

[20] D. C. Chou, and K. Yurov. "Security Development in Web Services Environment". Computer Standards & Interfaces, v. 27, n. 3, p. 233–240, 2005.