Security Enhancement at Lower Layers for SOA Reference Architecture

Anurag Shashwat, Deepak Kumar, Lovneesh Chanana

Abstract: SOA is widely accepted for designing the projects because it provides flexible and extensible architecture to solve the business problem effectively. In fact, SOA attracts the consumer because of its important features like reusability, modularity, composability, encapsulation and interoperability but security is always a concern for this architecture. Security implementation at a granular level for service-oriented architecture is an important concern. Service-oriented architecture is based on the distributed architecture wherein different services are the part of the different domain which is used to create an application. This causes security issue when services are composed for the creation of an application. Current security implementation at SOA based projects don't provide security at lower levels, however higher level is secured. Proposed Model enhances the security and reliability at lower levels of SOA using latest security techniques which also helps in maintaining the SLA after the security implementation.

Index Terms: Service-oriented architecture; Lower Levels; Security; Reliability.

I. INTRODUCTION

Service oriented architecture is one of the popular architectural design which is widely accepted for project implementation on different platforms, so the need of SOA security measures is also increasing. To keep services more reusable, interoperable and composable, security measures are ignored at lower layers of SOA reference architecture. Unfortunately, the designer faced problem in the implementation of secure SOA applications causes security implemented at higher level only in service-oriented architecture (Attri, R. and Grover, S.(2017); L. Srinivasan, 2006). End to end Security is difficult to achieve because it requires each element to be secured (M. Azarmi et al.,2012). Also, interaction between these elements should be secured. A single unsecured element may compromise the overall security of the entire system of systems, so security measures should be taken at each layer (D. C. Chou, and K. Yurov;2005).

The SOA Reference Architecture has nine layers which plays different roles in the process of designing a solution for SOA projects. SOA RA covers requirements aspect which reflects what the layer enables and includes all of its capabilities. It also include the logical aspect which consists of the ABBs, design decisions, options, Key Performance Indicators (KPIs) whereas the physical aspect of each layer includes the realization of each logical aspect using technology, standards, and products. Distribution of the role has been done layer wise in SOA RA. Implementation of the interface or service are covered by the Operational Systems Layer, the Service Component Layer, and the Services Layer where as consumption of services are supported by Business Process Layer, the Consumer Layer, and the Integration Layer. Four layers which include Information Layer, Quality of Service Layer, Integration Layer, and the Governance Layer are called non-functional or supplemental layers. These layers as a whole provide the framework for the support of all the elements of an SOA. SOA reference architecture divides the service design into five layers as shown in figure 1

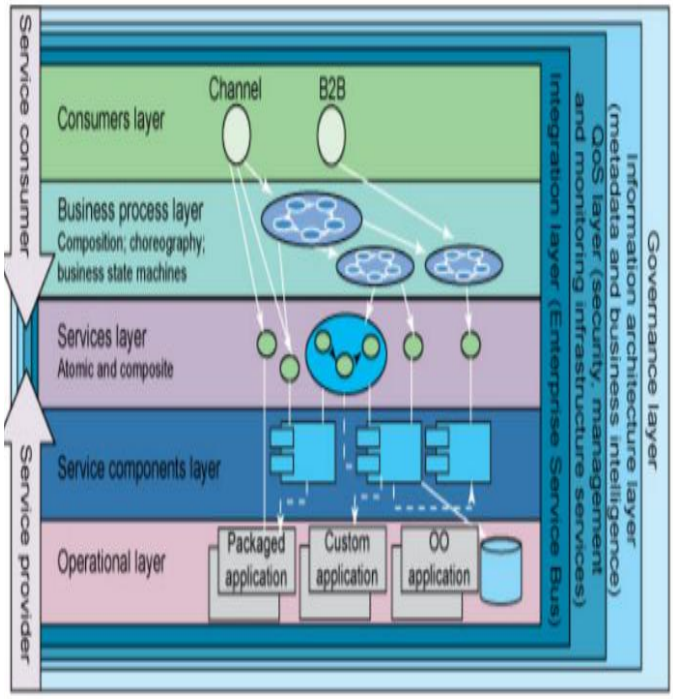

Fig 1: Layers of SOA Reference Architecture

The Operational layer and service component layer are considered as lower layers of service-oriented architecture. Operational layer is very first layer of reference architecture which covers the requirement of client and prepare the architectural design for the project.

The operation layer and service component layers are part of service provider layer where security enhancement is necessary to implement end to security. Legacy applications are used for integration with new SOA based services. Also, integration activity is started from service component layer where security not considered to keep reusability of the service as it is. Similarly, Service Component fulfills the goals like Realizes one or more services, provides an enforcement point for service realization, provides an enforcement point for service realization but security is a concern

Revised Manuscript Received on July 05, 2019
Anurag Shashwat, Amity University Uttar Pradesh ,Noida , India
Deepak Kumar, Amity University Uttar Pradesh ,Noida , India
Lovneesh Chanana, Visiting Faculty 'IIT Delhi, Delhi, India'

when different services are composed to fulfill business requirement. The lower layers of SOA which includes Operational Systems Layer and Service Component Layer are concerns for Providers whereas higher layers (Services Layer, Business Process Layer, and Consumer Layer) are concerns for the consumers. The author(s) proposes different ways of security implementation to secure the lower layers of services-oriented architecture. It will enhance the overall security for service oriented architectural projects.

Section 1 describes SOA reference architecture and security implementation at lower layers. In section 2, The authors collected security issues at lower layers of SOA. Section 3 focuses on literature review which includes related research done by different researchers. It also describes the framework and techniques to enhance lower layers security implementation. Section4 covers security enhancement using proposed model Section 5 contains an experimental analysis of 100 sample services of different service oriented architectural project which indicates that the proposed model will be better in terms of security implementation as compared to existing service oriented architectural framework. Section 6 includes conclusion of the paper.

II. SECURITY ISSUE AT LOWER LAYERS IN SOA

Submit As per reference architecture, Operational layer and Service component layer are considered as lower layers of service-oriented architecture. As per existing SOA framework, security is implemented at higher levels only where in lower levels are left unsecured to keep services reusable, composable and flexible. The Author(s) collected some of the security issues:

- Security attack on service at lower layers: Lower Layers of service-oriented architecture are not secure which causes a security attack.
- Authentication and Authorization issue: Authentication and authorization does not take place across intended end points, such as between the requestor and service provider. At lower layer authorization and authentication is not implemented for the services as per current SOA framework.
- Data security and data control Issue: Data security is always a concern at lower layers of service-oriented architecture. Sometime data is consumed by unauthorized users.
- SOA development and usage Issue: Services at lower layer are not secured. The consumption of the services for creation of an application is not authorized causes security issue.
- No trusted boundaries Specified for different layers: Currently security is not required for interaction of data between different layers of SOA.
- Unsecure Service discoverability: Services are discoverable in SOA, any consumer can search the service from different applications and even organizations. This causes unauthorized use of services.

III. LITERATURE REVIEW

Many researchers have already raised concern for SOA security. SOA facilitates with different facilities like reusability, composability, interoperability and distributed deployment bring security concerns especially at lower layers where security implementation is not considered while service interaction. Many research has been performed to keep higher layer of SOA secured. To provide end to end security to SOA based projects, lower level security consideration is important. The Author(s) chosen some of the research which provides security at higher layers of SOA can be beneficial in security implementation at lower layers too.

Channabasavaiah et al. (2004) defines SOA as "an application architecture within which all functions are defined as independent services with well-defined invokable interfaces which can be called in defined sequences to form business processes". Security is necessary for SOA based project to authorize requests, encrypt and decrypt data as required, and validate information. Trust based security implementation has been proposed by these authors to enhance the current security implementation, However the proposed solution by these authors are beneficial for higher layers of SOA. It defines the parameters and the output and hence addressing the needs of security, policy, reliability and accounting required for SOA (Papazoglou et al., 2006). Azarmi et al. (2012) provided a way to achieve end to-end security in SOA. Liu et al. (2014) described trust as an approach to enhance the security.

Many researchers provided their ideas to enhance the security using security certificate, trust-based model to satisfy consumer security requirements (Anisetti et al., 2013; Cimato et al., 2013, Kaluvuri et al., 2013; Katopodis et al., 2014;). Michael Hafner and Ruth Breu provided model-driven security approach which includes security goals in domain-specific languages. Y. Badr and S. Banerjee provided fuzzy logic which will be helful in achieving end to end security. Security auditing approach has been provided by M. Azarmi et al. SOA includes loose coupling, reusability, interoperability, composability but the services are not secure and reliable at lower level (Karastoyanova et al). The author(s) found different ideas by different researchers as shown in Table 1

Table1: A survey on SOA Security:

Survey result of different SOA Security	Granularity	Optional Impact
Techniques for SOA Security	Medium	Address specific classes of vulnerability
XML Threat Assessment Lists	Very Granular	Specific security operations required
Software Engineering Models	Global	For SOA security enhancement is need.

It is observed that majority of research work is focused around security implementation at higher level only to keep features

like reusability, composability, interoperability unaffected. The Author(s) proposes a model which enhances the security at lower levels of service-oriented architecture. This enhancement will also help consumer to achieve end to end security.

IV. SECURITY ENHANCEMENT AT LOWER LAYERS OF SOA

Service oriented architectural framework is widely accepted by the consumer because of the facility provided in the architecture are more flexible as compared to other architecture. But Security is a concern for SOA, The Author(s) have identified the area where security enhancement is required to improve the quality of the application. Security enhancement at lower layers (Operational layer and Service Component layer) is necessary because interactions between these layers are still open, no security is implemented. Whereas the authors found many tools and techniques have been proposed by many researchers for higher layer security implementation. To achieve end to end security for SOA based projects, it is necessary to enhance the security at lower layers (A. Shashwat, D. Kumar and L. Chanana,2017).

4.1 Areas influenced by SOA Security standards

The Author(s) identified the area where security enhancement is necessary to achieve end to end security:

a. Policy Standards

The policy standards include trust and Confidentiality.

b. Identity Management

Identity management include business partner entitlements and service partner entitlements

c. Messaging integrity and confidentiality

This include lower layer security, key management and encryption management.

4.2 Categories of Security standards

SOA security standard has three categories:

a. Identity Management Standards

b. SAML – XACML, Liberty ID-FF – DSML, SPML - WS-Federation is included under Identity Management Standards.

c. Web Services Standards

WS-Security, WS Security Policy, WS-Secure Conversation, WS-Trust, WS-Reliable Messaging is included under Web Services Standards (Michael P, Papazoglou, Benedikt Kratz, 2007)

d. Digital Security Standards

Digital Security Standards include XKMS - XML-SIG, XML-ENC - TLS IPSec, PKI – SSL, S/MIME – LDAP, Kerberos.

4.3. Interaction of Lower Layers of SOA and Security Implementation

The proposed model enhances the security at lower layer of SOA to achieve end to end security for SOA based project. Current SOA model enables loose coupling interaction between layers of SOA. This loose coupling allows services to interact without security. Also, this helps in increasing reusability, composability and interoperability. But security is a constrain for this architecture. Sometime provider of the service has no ideas of the consumers who are consuming the services and performance and security become an issue. The current service interaction has been shown in fig 2:

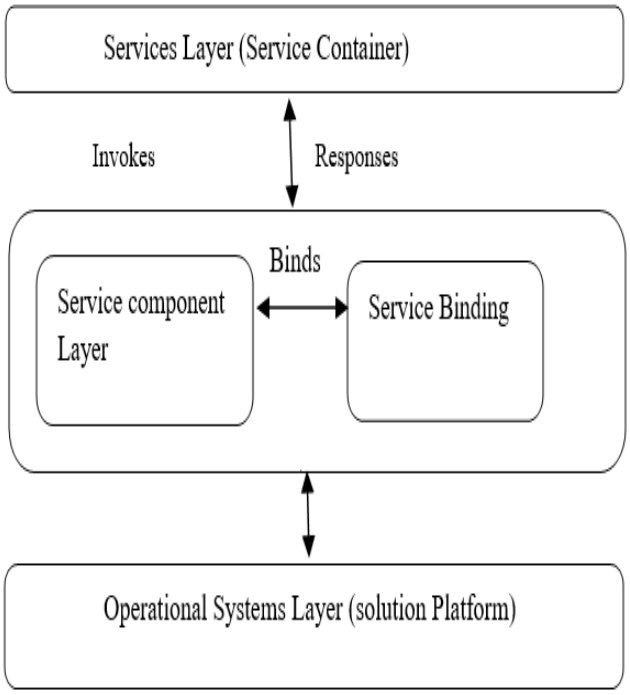

Fig 2: Existing Interaction of SOA Layers

The Author(s) identified authentication, authorization and accounting implementation at lower layers of SOA. This will enhance the security for SOA based projects which will help in achieving end to security. The proposed model also includes signed certificate installation for individual layers of SOA, so that no layer can interact with other layer without a valid certificate authentication as shown in fig 3:

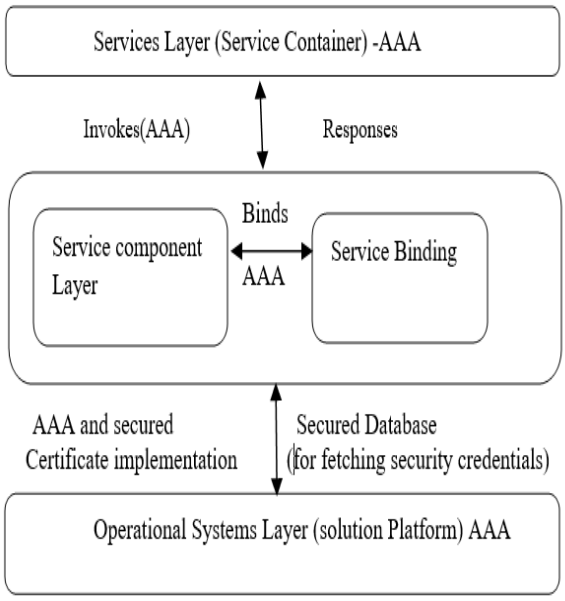

Fig 3: Proposed Interaction of SOA Layers (with Security)

4.4 Proposed Techniques for security enhancement at lower layers of SOA

To ensure end to end security functions required are: authentication, authorization, auditing, assurance. In SOA, these functions will be helpful in making services as "security services". The Author(s) proposes AAA implementation at each and every layer of SOA as part of security enhancement.

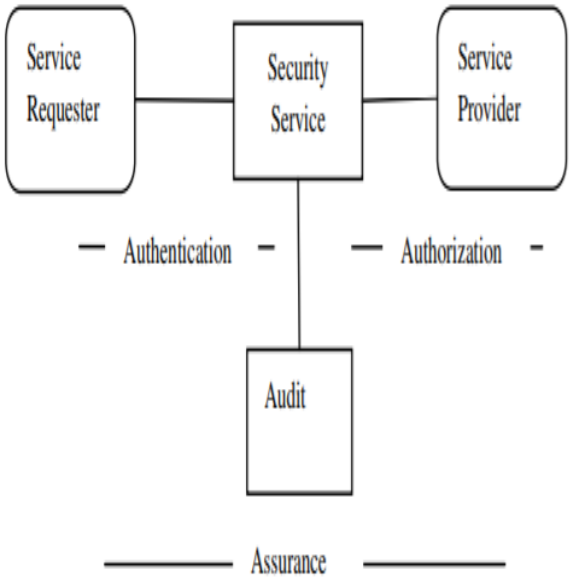

Fig 4: Service level security at SOA

4.4.1 Authentication at lower layers of SOA

SOA based project consists of service requesters, service providers, and message exchange patterns (A. Shashwat, D. Kumar and L. Chanana; 2018). The Author(s) found the incorporation of the authentication, authorization, audit, and assurance services add true value with in the message exchange. Many unauthenticated is processed which usually causes heavy load on service. As part of the system authentication system policies (such as password policies) and complex protocols (like Kerberos) should be used to validate the consumer (Mohamed Ibrahim B, Mohamed Shanavas A R,2015).

4.4.2 Authorization at lower layers of SOA

Authorization is enforced locally in many systems. The author(s) proposes fine grained implementation of authorization for every layer of RA.

4.4.3 Audit services at lower layers of SOA

The implementation of audit and assurance services will improve the security for SOA based projects. The Audit service is responsible for detection and response features whereas Assurance services provides confidence in the given system. It will be helpful in achieving enhanced security and reliability.

V. EXPERIMENTAL ANALYSIS – COMPERISION OF PROPOSED MODEL WITH EXISTING MODEL

Because The authors have collected different security concerns at lower level of service-oriented architecture. Using proposed model, security can be enhanced at lower layer which will also helpful in enhancing the end to end security. Existing model has security implementation at higher levels only. To provide secure application, security has been implementation at both the levels of SOA and latest technology has been used to maintain service level agreement for each service. A sample of 100 SOA services from different domains has been taken for the experimental analysis. The author tested security implementation and service level agreement:

5.1 Proposed Model Implementation

The Author implemented all security standards at lower layers of SOA without impacting reusability functionality. Services will be ready to be reused still but security standard will be needed at lower layers too. The author uses secured database and global cache techniques to ensure authorization, authentication and audit at followed at granular level of service. The author used IBM integration bus to create different services where security has been implanted at granular level to ensure end to end security for SOA. The author(s) tested the proposed model to ensure SLA has no impact after the security implementation at lower layers of SOA.

5.2 Proposed Model Test using SOAPUI

The author has chosen 100 exiting services of SOA where security enhancement has been performed at lower layer.

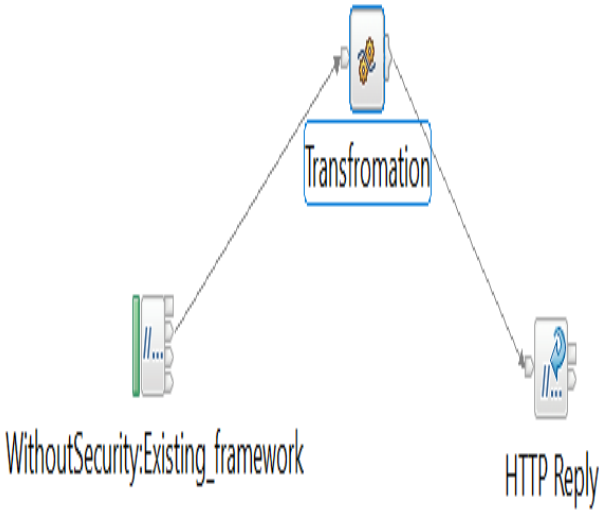

Fig 5 : IIB message flow using Existing SOA framework

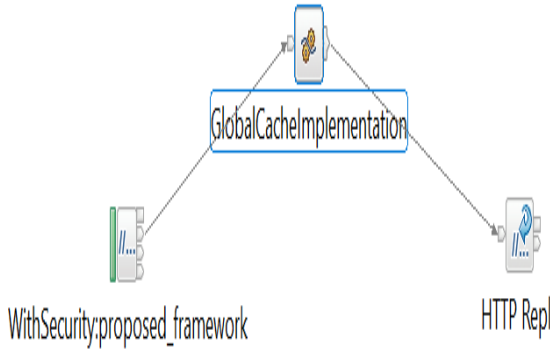

Fig 6 : IIB message flow using Existing SOA framework

Service response time of message flow using Existing framework is 7ms as shown in the figure 5 under SoapUIlog. In figure5, no authentication is being passed along with service message.

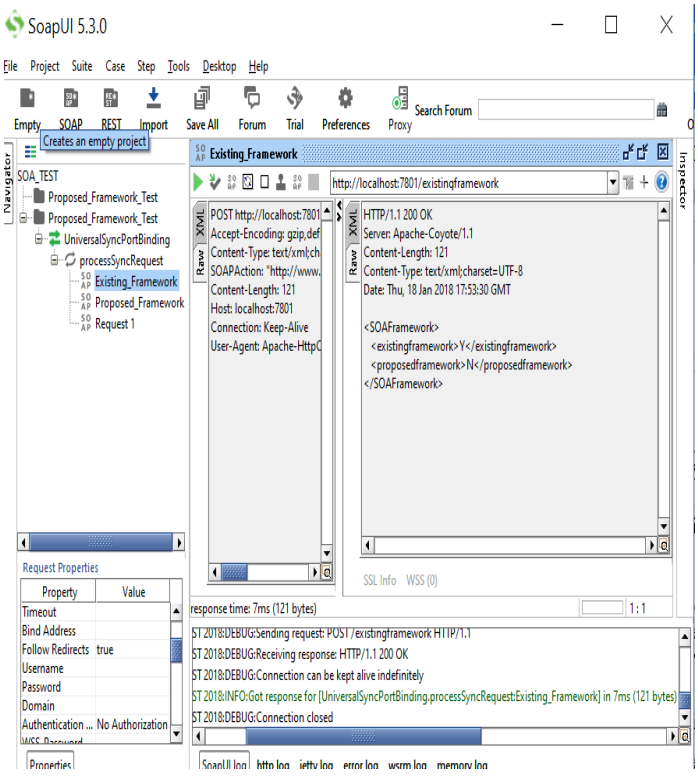

Fig 7 : SOAP test for Existing SOA framework

Authentication of the user has been enabled for proposed model, the author(s) found SLA proposed framework is 6ms.In the below figure 6, we can see the userid and password is being sent to the IBM integration bus for verification.

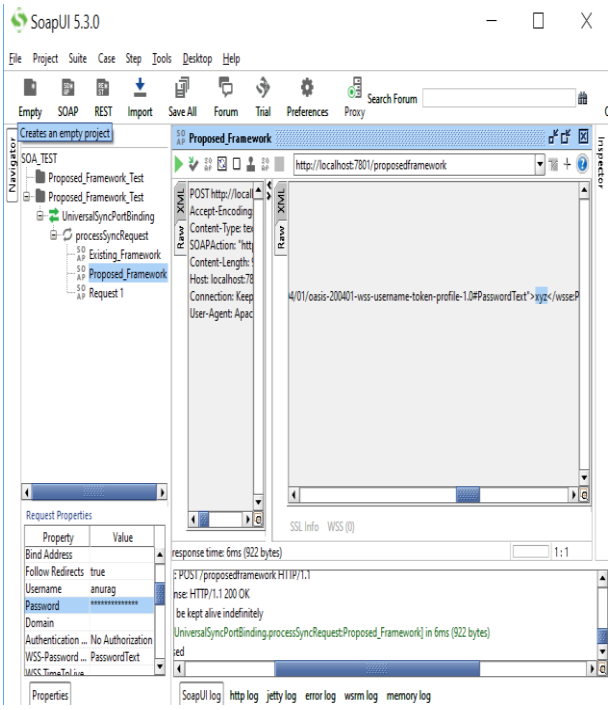

Fig 8 : SOAP test for Proposed SOA framework

5.3 Comparison of Exiting Model vs Proposed Model

The Author(s) tested the proposed model vs existing model using different parameter and found security enhancement at lower has no impact on SLA. Also, security standard implementation has enhanced the security at lower layer of SOA, which will be helpful in reducing n number of incident. Performance of service will increase as no unauthorized user will able to use the service.

Parameter	Result for Exiting model from SOAP UI	Result for Proposed model from SOAP UI
Service Response time in ms	7	6
Lower level security in percentage	0	80
Data security at lower layers	0	75
Message level security in percentage	40	80
Authentication, Autherization and Audit(AAA) at Lower layers in percentage	0	70
End to End Security for SOA based project	60	75

Table 2 : Comparison of existing Model Vs Proposed Model

The author(s) found lower layers security implementation enhances end to end security for SOA based project.

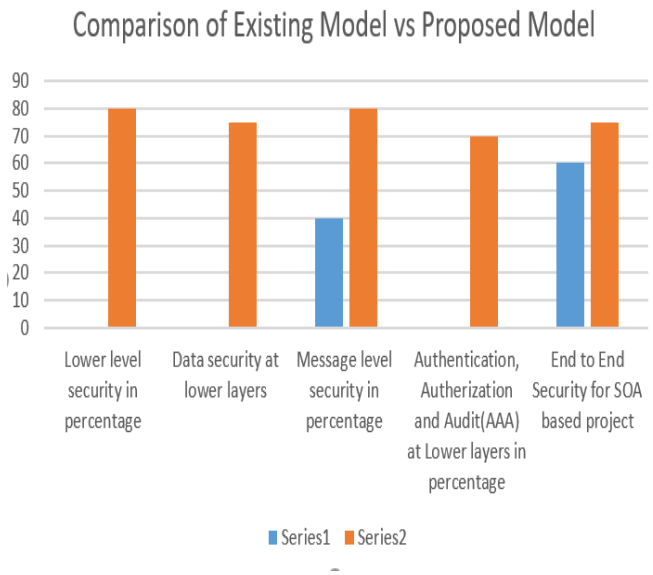

Fig 9 : Comparison of Existing Model vs Proposed Model

VI. CONCLUSION

Service oriented architecture has features like reusability, composability, interoperability and distributed deployment which are concerns for security implementation. The Author(s) found major incidents of SOA are due to securiy issues at lower layer. The Proposed Model enhances the security at lower layers without impacting the service level agreement. This model enhances the security at lower layers of SOA using different security techniques. This implementation will help in achieving end to end security for SOA based project. Also, this model will be helpful in enhancing the performance and reliability of each services.

REFERENCES

1. 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, United Arab Emirates, 2017, pp. 475-480.
2. 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
3. A. Shashwat & Deepak Kumar, "Service Identification by Enhanced K Mean Algorithm in Service Oriented Architecture" accepted for publication in International Journal of Process Management and Benchmarking, Inderscience. ISSN online:1741-816X, ISSN print: 1460-6739
4. 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, India, 2018, pp. 1-6.
5. Y. Badr and S. Banerjee, "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. 111-117.
6. M. Azarmi et al., "An End-to-End Security Auditing Approach for Service Oriented Architectures," 2012 IEEE 31st Symposium on Reliable Distributed Systems, Irvine, CA, 2012, pp. 279-284
7. Michael P, Papazoglou, Benedikt Kratz, "web services technology in support of business transactions" SOCA Springer,2007
8. K. Channabasavaiah and K. Holley, "Migrating to a service-oriented architecture, on demand operating environment solutions," White paper, IBM. 2004.
9. A. Arsanjani, S. Ghosh, A. Allam, T. Abdollah, S.Ganapathy and K. Holley, SOMA: "A Method for Developing Service-Oriented Solutions" In IBM System Journal, vol. 47, no. 3, pp. 377-396, 2008.
10. D. C. Chou, and K. Yurov. "Security Development in Web Services Environment". Computer Standards & Interfaces, v. 27, n. 3, p. 233–240,2005.
11. M. Hafner and R. Breu,"Security Engineering for Serviceoriented Architectures", Springer, October 2008
12. Deepali Tripathi, "Towards Introducing and Implementation of SOA Design Antipatterns", International Journal of Computer Theory and Engineering, Vol. 6, No. 1, February 2014
13. Thomas Erl, "Service-Oriented Architecture: Analysis and Design for Services and Microservices (2nd Edition)". December 22, 2016
14. Attri, R. and Grover, S.(2017) 'Developing the weighted ISM-MICMAC framework for process design stage of production system life cycle', Int. J. Process Management and Benchmarking, Vol. 7, No. 1, pp.94–119.
15. M. Khan, A. Mishra and R. Agarwal, "Security framework based on QoS and networking for service-oriented architecture," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 1106-1109
16. L. Srinivasan, "An overview of Service Oriented Architecture, Web Services and Grid Computing," HP (Hewlett Packard) White Paper, November 2006
17. A. H. Ouda, D. S. Allison and M. A. M. Capretz, "Security Protocols in Service-Oriented Architecture," 2010 6th World Congress on Services, Miami, FL, 2010, pp. 185-186
18. Mohamed Ibrahim B, Mohamed Shanavas A R, "Identifying SOA Security Threats using Web Mining", International Journal of Computer Applications, Volume 120 – No.4, June 2015.

AUTHORS PROFILE

Anurag Shashwat holds Bachelor of Technology in Information Technology from SRM University, Chennai and Master of Science in Computer Science from Manipal University, Karnataka. He is pursuing his Ph.D. in Information Technology from Amity University, Noida. He has many publications in national/international/journals and conferences. His research area includes enhancement of security and reliability for service-oriented architecture.

Deepak Kumar is an Associate Professor in the Amity University, Noida. He is earned his PhD from the University of Delhi, India and MTech in Computer Science from the Birla Institute of Technology, Mesra. He is an Associate Editor of International Journal of System Assurance Engineering and Management, Springer. He has delivered invited talk/guest lecturer in University of Maryland, USA, Fayetteville State University, USA, San Jose State University (California, USA) and published/presented more than 100 research papers in various international and national journal/conferences. He has filed three patents in software engineering. He has authored a book Software Reliability Engineering – A Brief Description.