International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Policy based Security Framework in Semantic Web

Jyoti Malik, Suresh Kumar

Abstract-Semantic Web (SW), an extension of Web2.0 which can integrate various application and system such that data can be processed by machine instead of human using RDF, SPARQL, OWL technologies. With the passage of time advancement made in technologies which can provide dynamic support and interactions such as DAMLS [13], RDF AND RDF-S, OWL, SWRL.As we are shifting towards making a system which is user interaction free, meet new security challenges [14]. Security is becoming prime important and a crucial factor in making an autonomous system, who will able to provide dynamic support and interaction of various clients and agents on a large scale? Success of Semantic Web depends on the way security is handle at various layers. Here, we are providing a policy based security framework containing Knowledge base, Distributed policy Management. Moreover, we have also provided a table with key points of SW and problem addressed in each research article.

Index terms: Agents, security framework, machines, web resources, web services, semantic web.

I. INTRODUCTION

Initially the first steps toward the development of secure SW is to analysis each and every layer of it
along with detailed description of technology needed for achieving the goal of secure semantic. PKI, X.509 are the convential technologies, used to provide security in web2.0 but become insufficient for web 3.0 because of the dynamic nature of web3.0[14]. Technologies used in web 2.0 are based on XML which can efficient for authentication and accountability but lack in authorisation as very much needed for SW. There are two types of threats inherits by SW that is from networks and the internet namely Eavesdropping wire-trapping, impersonates, phishing, masqueration and denial of services etc. As the SW provide autonomous and dynamic behaviour between clients and service providers or Between two clients which is bringing new security challenges at an alarming rate. Therefore, XML based existing security standards such as XML Encryption Signature. Mechanisms to be used for making semantic web secure are 1. use of TLS by the URL in the semantic web so that document host at this URL does not remain vulnerable to being intercepted and altered by third party.2 SOAP header Message format is to be used to transport the contents securely at the application layer.

Revised Manuscript Received on April 18, 2020.
* Correspondence Author
Dr. Suresh kumar*, Phd, Faculty of Engineering and Technology, Maharshi Dayanand University, Rohtak, Haryana, India
Jyoti Malik, Student, M.tech, Information Security, Department of CSE, Ambedkar Institute of Technology, GGS IP University, New Delhi, India

Trust Ontologies and Trust rules are defined in the agent interaction protocol so that authorization, authentication problem can be solved. The Semantic Web review is followed by overview of security framework. Section II contains work which includes Semantic web –architecture and technologies in section. In section III Semantic Web security aspects which contain detail of Semantic web assets-AGENTS, RESOURCES AND WEB SERVICES and their respective security mechanism, along with a table containing list of research paper along with their respective key point and problem addressed. Section IV contains security framework based on distributed policy management approaches, semantically risk and enforces security policies. Section V contains conclusion and future work.

II. LITERATURE REVIEW

A. Semantic Web

With the passage of time, amount of data on the web is increasing exponentially with a very alarming rate, which makes it difficult to manage such a big amount of data on the web therefore different technologies are developing day after day in order to manager data effectively, to provide interoperation ability, warehousing among different sources, for extracting information. As a result vision of web3.0 comes into force which is also called Semantic Web. Initially Lee gave a vision of SW, as a web which can be processed by machines not by humans, therefore regarded as an integrator of different content, applications and systems provide the result to the user. For the realisation of SW various technologies and languages have been developed.

B. Architecture And Its Technologies

According to the B. lee[16] A web that can be processed by machine rather than human and known to integrate web content, services and application . According to Danker[23] ,agents and search engine in the Web 3.0 can work more quickly and accurately as compared to the web 2.0 as it integrate the data of different source more intelligently and collected data can be used for knowledge access, communications, applications. After fully understanding the architecture of SW, the property of interoperation ability can be known. The architecture of the SW is basically a layered stack having semantic language technologies and languages used for interoperation among different layers and different applications. Finally, the status model proposed by Gerber[25] was adopted as shown in figure1. This architecture is based on language hierarchy which extended and exploits the

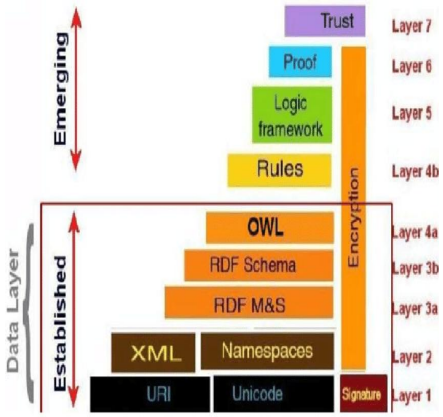

Fig1. Semantic architecture

features of layer below it by extending the syntax and semantic of the language under it. Languages accept by W3C for the SW are Unicode, XML, RDF, RDF-S, OWL. Overall SW architecture is divided into three parts-Established technology, Emerging Functionality and vertical layers. Established technology-All the technologies which are recommended and adopted by W3C are established technologies as these technologies have been used in layer 1(URI and UNICODE),layer2(XML),layer3(RDF) and layer 4(RDFS). Emerging Functionality-The top three layers defines the functionalities rather than technologies hence they are called emerging functionality. Vertical layer-It consists of Encryption and Signature, used to provide security mechanism to the languages and SW.

C. Semantic Web Layers

i. Uri And Unicode

Both URI and UNICODE reside in the first layer of the SW. URI is used to identify a resource over the web [29] anything having URI is consider to be on web and stands for uniform resource identifier. URL, a subset of URI identifies resources with the help of network locations.URI specification as provided by IETF provides specifications known as RFC-2396. UNICODE is used to identifies the character rather the resource for all languages by specifying a global character encoding mechanism such as UTF-8, 16, 32 as provided by UNICODE consortium

ii. Xml,Xml Schema And Namespace

All these three comes under 2nd layer of SW[16] and provide a mechanism for interoperationablity by defining and describing syntax for layer above them[25].XML is a markup language with markup tags that defines the logical structure for a document, set of rules and for encoding contents. These contains can be read by both human as well as by processed by machine.XML also define standards for exchanging data over web so as to provide interoperationablity in order to access any XML document[17].

iii. Rdf And Rdf Schema

[17] It provides a metadata description framework for the layer above it. [25] It describe declarative statements for web resources by using data model[17].RDF is an important part of SW for defining the security framework as it define and declare metadata which can be processed by machine. It represents resources information in the form of graph and consists of Subject Predicate Object expression [3] triplets. Here resources are represented by subject, Properties or attributes are define in term of predicate and object defines values . RDF defines common vocabularies by using metadata statements and also enhances interoperationablity. RDF schema defines vocabulary of RDF model and used to provide applications specific classes and properties of resources in term of set of primitives such as class, domain range, sub property, property-of[3]. It also assigns specified semantics for resources [17][29].It is also describe various mechanism in order to define relationship of their resources.

iv. Ontology Vocabulary

Ontology and its rule resides at layer 4 [17]. Ontologies use common knowledge to represent RDF with the help of technologies, its formalisation and understanding of domain knowledge.[25].Ontologies play an important role in processing and representation of the knowledge between different programs on the SW. Ontologies is define in terms of natural, domain and instance and helps in representing machine processing information on the web. It also provide computation task by defining properties and methods used in computation. It also defines reasoning properties used by machines in processing knowledge.

v. Logic Framework

Logic Framework provide formal semantic to logic statements [19] on the top of ontology language .It allow rules declare for specific knowledge domain to be written for different web application [3].

vi. Proof

The proof layer involves actual deductive processes, representation of proofs in web language and also provides mechanism for proof validation [3].

vii. Trust

Trust lies at the top of the SW and provide a mechanism to establish trust among all the items and entities by using Knowledge base recommendations as provided by trusted agents, certificates agencies through Digital Signature [3].

viii. Vertical Layer-Signature And Encryption

The vertical layer consists namely of signature and encryption .This layer provide security mechanism to the SW and its different languages [25]. Encryption provides end to end encryption of XML document, which is used for information storage, transfer and also for authentication. XMLENC is a standard mechanism used for encryption as well as decryption of various XML data objects. Signature is enforce by XML Digital Signature[12] used for verifying entities and to sign the documents ,for authentication, retrieval based on the public key security and trust systems mechanism .XMLDSIG is a standard of both W3C AND IETC for signing the document digitally and provide verification of these signature for XML data objects.

III. RELATED WORK

According to [21] tools and security models should be develop for technologies such as RDF,OWL,XML and security requirement must be driven by the needs of functionality, collaborations and organisation.

They also emphasised on the development of flexible model for the web access controls that support fine grained granularity of data which can accommodate large range of policies which are suitable for decentralization and must be for dynamic and open environment so that it preserve the consistency, illegal interference. Hence to achieve the goal of secure SW its components should be secure, integration of information must be secure and issues related to the trust must be examined. DENKER[23] raised the issues of services descriptions along with security requirement and capabilities, ensuring that clients and service provider meet each other requirement. Kagal proposed a policy engine which is used to identify policies for privacy, security and also suggested semantic web languages policies requirements along with distributed policy management. Ashri[14] proposed the use of conventional security solutions at the semantic level with the ability to reason to achieve a secure semantic web. Kagal, Bhargavan, Fournet and Gordon [26] suggested that security policies are define to describe capabilities related to security and infrastructure is defined for defining descriptive reasoning and infrastructure capabilities. Along with these Other program aim at security in semantic as describe : XMLENC- provide encryption mechanism for XML document., XMLDSIG[15] a mechanism to digitally signing and verify it, XKMS[24] a mechanism for key distribution verification, P3P define policies related to privacy to enable services on websites and also define reasoning to check whether these policies matches user preferences[27], SAML: SAML provide security framework for XML document related to authentication and authorisation.

A. Semantic Web Security Aspects

The prime goal of security is to attain standard security goal of integrity, availability, confidentiality by using different security mechanism such as authentication, authorisation, audit log etc to determine the threats like interception, interruption, fabrication, modification of resources firstly computing asserts to be identified for the protection and evaluation of the asserts must be done to achieve the security goal. Table1 shows security mechanism for agents, resources and services to be protected along with security goal affected and respective security threat each may have.

Table 1: table show asset to be protected

ASSET TO BE PROTECTED	Threat related to Security	Security goal affected
Web services	Session hijacking	Confidentiality ,integrity
	Eavesdropping	Confidentiality
	Wire-tapping	Confidentiality , integrity
	Impersonation	Confidentiality , integrity
	Spoofing	Confidentiality
	Phishing	Confidentiality, integrity, non-repudiation
	Masquerading	Non-repudiation
	Denial-of-service	Availability
Web resources	Eavesdropping	Confidentiality
	Wire-tapping	Confidentiality , integrity
	Impersonation	Confidentiality , integrity
	Denial-of-service	Availability
	Deletion of resource	Availability
	Phishing	Confidentiality, integrity , non-repudiation
	Illegal inference	Confidentiality
Agents	Information modification	Integrity
	Masquerading	Non-repudiation
	Cloning	Confidentiality , integrity
	Denial-of-service	Availability
	Eavesdropping	Confidentiality

B. Semantic Web Assets- Agents, Resources And Web Services

KAGAL[6] identify the assets namely resources, agents and services that need to be protected and required to define security functionality for them. All these Agent, Resources and web services must be include in security framework because all these are participants in various interaction[22][23].

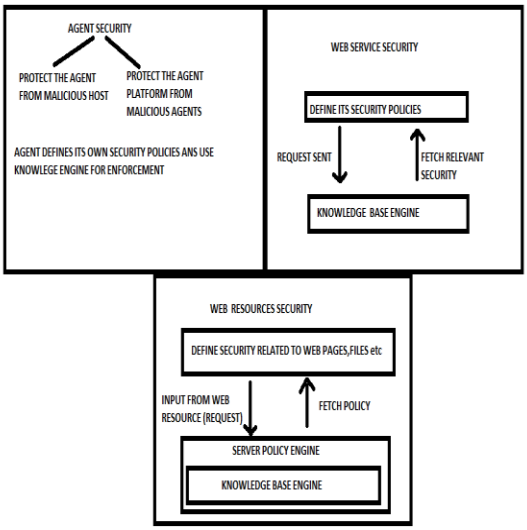

Fig2. : Security mechanism for Agent, Web Service, web resources

a. Agents And Agents Security Aspects

SOFTWARE agents ,an autonomous software which interacts with the environment having different attributes such as adaptively , coordination's, mobility etc.2.MOBILE AGENTS, representing user on the network by interacting and performing computational task with other web agents and services. Agents security include protecting agents against malicious hosts and network communication as shown in fig 2 above. Difference of communication among agents or between agent and users must be protected. They could be eavesdrop, manipulate, impersonates entities which are participating in communication

b. Web Services And Ecurity Issues

A web services are identifying by a URL, where interface are defined by XML. XML message can be exchanged using various XML protocol between different software agents. Web services will automatically discover, execute various logics required by different organisation A web service uses XML based different message exchange protocols to interact with other users and agents [18].

c. Web Resources

[29] Resource is an entity name by URL and defined by RDF. RDF defines properties and respective values of web resources and used these values among different applications such as for authentication and access control.

Table 2 contains the list of research paper along with their respective key point and problem addressed .

S .no	Authors and Publication year	Title of paper	Key point discussed	Problem Addressed	Conclusion
1	M.Troya, I.Yague Mariemma, Mana Antonio,2003	Applying the semantic web layers to access control[2]	Application of SW and technologies used to the access control, provide SAC model and use of Semantic Policy Language	Work of semantic web layers infrastructure in different fields such as access control and authorization fields	SAC approach different components of access control systems, metamodel of SOAD
2	Pranav Parikh B.Thuraisingham,2008	Trustworthy semantic Web Technologies for secure Knowledge Management[11]	technologies are provided to make secure knowledge management	Secure Knowledge Management, information sharing , Integration , collaboration	XACML,SAML could be applied for enhancing secure knowledge management
3	A.Medic, A.Golubovic,2010	Making Secure Semantic Web[6]	Describe different way of security implement through different layers	Security in XML, Security in RDF	Define security of XML, RDF, Ontologies, inference algorithm for security, trust and privacy management.
4	Asok De, Prajapati, Rakesh kumar, Manjeet Singh, Suresh Kumar,2010	Realisation of threats and countermeasure in semantic web[7]	Semantic Web services must implement security solution at different layers for including Security Goal	Semantic Web Services Threats, respective countermeasures, SOAP,XML X-KRSS, Digital Signature, XML encryption, decryption	Use of XML encryption Decryption and SOAP technique at application level and also Digital certificate
5	Manjeet Singh , Akilesh Dwivedi,Abhishek Dwivedi, Suresh kumar[2011]	Current security consideration for issues and challenges of Trustworthy Semantic Web[8]	XML Signature , web service security problem	Key security considerations of different layers, SSL certificate Problem, SWS-Security	More Security standards like SAML, XACML need to be develop
6	Bruce Barnett[2011]	A semantic Model for Cyber Security[4]	SADL language is used to develop semantic web application as it allow Ontologies to be expressed in English	Component of the ontology for describing ,measuring and comparing physical and network – specific risks	Semantic Reasoners can provide useful benefit in measuring security of complex system

7	Rashmi Mishra,Gopal Gupta,Amrita Jyoti,2013	Secure Agent in the Semantic Web[9]	Security of an agent as it play different roles on different platforms	Provide agent framework on the Semantic Web, provide a mechanism of interaction of an agent with a site using SAML	Agent security is an important factor in order to make semantic web secure
8	Tanjim Rahman , Shamim Ripan, Sumaiya Kabir, Mamunur Rahman ,2014	Knowledge-Based Data Mining using Semantic Web[10]	Propose an approach to map data through Ontologies and accessing data through intelligent agent	web mining model is proposed under semantic agent framework, provide ontology based searching, OWL ontology Components	Knowledge based data mining required Ontologies so that only relevant search can be provided against the user query
9	Rashmi Bakshi,Abhishek Vijhani,2015	Semantic Web –An Extension Literature Review[3]	Explore the field of semantic Web and scope of data mining, information retrieval, language processing and bio –informations	Literature view is presented by categorizing into semantic Architecture and Security Semantic Mining and Context aware	Comparative Analysis is done by Categorizing the previous research paper .
10	Aamir JUNAID Ahmad,Sabina Priya Darshini,2017	Accessing Social Networking Sites Using Semantic Web[5]	Use of Semantic tool and techniques for making searching meaningful	A model is provide which contain RDF data store, Reasoner ,RDF/QWL engine to make a layer on the top of network application	It address some limitations of accessing network data and use of semantic web approach to overcome it
11	H. Halpin,2017	Semantic Insecurity :- Security and Semantic Web[12]	Currently, TLS is not appropriately used for majority of URLs on the Semantic Web	Security Properties of the SW, analysis of WebID +TLS, fixing the security for the SW	SW has not fully moved from http to https, Semantic Web Tools and Vocabularies should switch to use TLS – encrypted HTTPS URLS
12	Mathieu D' Aquin, Serena Villata, Sabrina Kierrane	Privacy, Security and Policies : A review of problems and Solutions with Semantic Web Technologies[1]	Privacy ,policies related challenges of SW technologies	Analysis the working of semantic web security, privacy and policies,	It provide strong focus on information collection, processing policies and access control

IV. SECURITY FRAMEWORK

A. Security Framework Components

Main components of security framework and their functionality can be categorized into 3 domains.

1) Knowledge Management

In this different technologies such as data mining, multimedia require different sub domains namely metrics, processes and strategies [11] .To have secure knowledge management Strategies, metrics, process subdomain must be secure. Strategies subdomain contains all lists of security strategies that need to be implemented when required. Process subdomain contains list of secure operation and metrics subdomain contain support for security related information[11].

When knowledge domain is created the initial step is to specify the receiver, who will receive the data after the transfer is done and also to whom access control techniques must be provided .Lastly but most important is to make a secure knowledge management architecture.

2) Technology Domain

It contains language, Ontologies, Agent subdomain. Language subdomain contains various languages such as XML and SAML. XML Markup language used markup tags to define structure of document. It helps in building interoperationablity in order to access the contents of xml document. SAML abbreviated as Security assertion Markup Language is basically a standard define for exchanging authorization, authentication of information for XML languages .Ontologies sub domain contain conceptual knowledge about the object and store them in ontology library[10].When user make a call to the agent then it start searching ontology and its library to find all nodes which are need in order to obtain all information for user query.OWL ontology return the relationship between object in Subject + relationship + object format[10].In order to make ontology secure Attack/defence ontology model [4] can be taken into consideration. In ontology model only few classes and attribute are required to calculate metrics related to physical and network security. Classes are defined for device capabilities, attack mechanism, vulnerability, defence mechanism and the specific attacker design is model as instance of the class [4]. In the Semantic Web Agent subdomain consists of 5 type of reflex model namely simple, model, agent, goal , utility [9]. An agent system consists of a performance measure, actuator, sensor and an environment. In the security framework an agent must get security information dynamically and exchange information and attribute mutually in multidimensional environment system. An agent provides result against the requested query of the user.

3) Information Security Domain

It consists of threats, security services (goal) and countermeasure policies. Threats refer to anything that cause harm to a system if occur .In this domain keep all the possible list of threats that may harm a system or its resources in the form of vulnerabilities such as vulnerabilities related to Unauthorized access[7] ,also include taxonomy of activities led to privacy problem[1]. Countermeasure sub domain contains policies or mechanism that is required to eliminate the possible vulnerability of the threats sub domain. Security Service subdomain contains all the mechanisms which are used to make semantic web secure such as 1.)Use of TLS by the URL in the semantic web so that documents host at this URL does not remain vulnerable to being intercepted and altered by third parties[12].2.)SOAP header Message format is to be used to transport the contents securely at the application layer and defines XML standards like XML signature AND XML Encryption[8].Trust Ontologies and Trust rules are defined in the agent interaction protocol so that authorization, authentication problem can be solves[6].

B. Policy Based Security Framework In Semantic Web

It is a security framework based on policies which is using a distributed policy management approaches, semantically risk and enforces security policies**.** Ontologies are used for describing security information to have secure transaction over different domains. The security framework contains 4 components as shown in figure3. 1.The distributed policy management –policy engine ,policies ***2***.knowledge base-security Ontologies ,process ontology 3.security services 4.securitymechanism and standards as shown below in figure .

i. The Distributed Policy Management

It consists of policy engine and policies sub domain .Policy engine contains knowledge related to security services, security mechanism and standard and detail description of policies related to various threats.

a) Policy Engine

Policy engine is basically a reasoning engine must be consulted each and every time an request and action must be taken .It may be used for web services, web resources and for agents as shown in figure above .It draws rules and facts from knowledge base and make comparison of facts with the security policy of an application and draw out the result for the course of action to be taken against the request made to it.

b) Policies

In this framework security policies must be adaptive in nature and must be applicable for multiple domain environment, flexible .Here the policies are define for the subject such as Access, privacy, Transaction etc .Identification of resources, services, application, transaction policies, countermeasure policy against threats are the various list of content against which security policies are defined in the above security model.

ii. Knowledge Base

It has a relationship between protected entities and mechanism. KB has two domains-Security Ontologies and Process Ontology Models.

a. Security Ontology

In this security terms, their relations, specialisation is defined and also define automatic reasoning annotation .Languages used in security Ontologies are-OWL, RFDS. It consists of three classes. .a.)Security services defining security mechanisms and protocols. b.) Security Policies-defining languages c.)Protected entity- Credential threats, and security requirement security capabilities. Knowledge Base with Ontology is used for access control mechanism where security policies are define as rules and encoded the security policies by means of ontology.

B. Process Ontology

Defines workflow i.e. sequence of events takes place

C. Security Services

Various security goals provides by this are-CIA, authentication, authorisation and non repudiation.

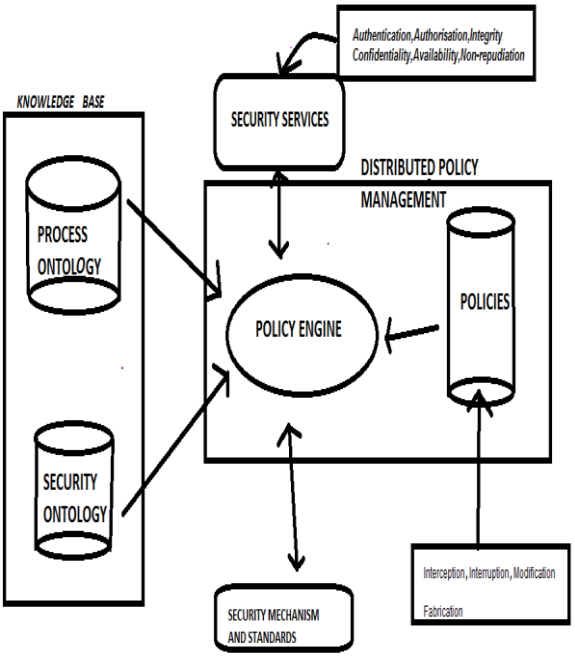

Fig 3- Security Framework

Protection against Interruption, modification provide by Integrity services applicable to web resources XML security technologies provide framework policies.

D. Security Mechanism And Standards

It includes security standards based on XML which are adopted by security applications like XML encryption, XML Signature, XAML and must be utilised by security framework.

V. RESULT AND DISCUSSION

Table1 is listed with the assets that need to be protected. Table2 contained the lists of research paper along with the respective key points and problem addressed in each research paper. Security mechanism for Agents, Services and web resources is discussed along with their individual security aspects. Security mechanism and its security framework components are discussed in details and show the interaction among the different component with the help of Distributive Policy Management.

VI. CONCLUSION

New security challenges emerge in the SW due to dynamic relationship between clients or clients and service providers. These security challenges must be deal with the help of security framework. A policy based security framework is described along with its component. Moreover along with framework a list of different research article is prepared highlight key point and addressed problem in each paper related to secure Semantic Web. In future Policy Based Security Framework will be implemented by using Protege tool. With the help of PROTEGE tool various Ontologies will be develop for Process and Security which are used in Knowledge Base.

REFERENCES

1. Mathieu D' Aquin, Serena Villata, Sabrina Kierrane, Security and Policies : A review of problems and Solutions with Semantic Web Technologies,IOS press, issue -1570-0844, 2018
2. Mariemma I.Yague, Antonio Mana, Javier lopez,Jose M.Troya, Applying the semantic web layers to access control,IEEE International Workshop on Web Semantic,p-622-626 ,2013
3. Rashmi Bakshi,Abhishek Vijhani, Semantic Web –An Extension Literature Review, Grid-Interop Forum ,2011
4. Bruce Barnett , A semantic Model for Cyber Security , International Journal of Advanced Networking and Application, vol-3,issue 01,page-978-983,2011.
5. Aamir Junaid Ahmad,Sabina Priya Darshini, Accessing Social Networking Sites Using Semantic Web ,IJARIIT ,ISSN: 2454-132X,2017
6. A.Medic, A.Golubovic, Making Secure Semantic Web,Universal Journal of Computer Science and Engineering Technology,vol-1,99-104, 2010
7. Asok De, Prajapati, Rakesh kumar, Manjeet Singh, Suresh Kumar,, Realisation of threats and countermeasure in semantic web,International Journal of Computer Theory and Engineering,Vol.2,no-6,1793-8201,2010.
8. Manjeet Singh , Akilesh Dwivedi,Abhishek Dwivedi, Suresh kumar, Current security consideration for issues and challenges of Trustworthy Semantic Web, International Journal of Advanced Networking and Application, vol-3,issue 01,page-978-983,2011.
9. Rashmi Mishra,Gopal Gupta,Amrita Jyoti, Secure Agent in the Semantic Web,International Journal of Innovation Research in Science,Engineering and Technology,vol.2,issue 3,2013
10. Tanjim Rahman , Shamim Ripan, Sumaiya Kabir, Mamunur Rahman, Knowledge-Based Data Mining using Semantic Web,IERI Procedia 7, Page no-113-114, ELSEVIER,2014
11. Pranav Parikh and B.Thuraisingham, Trustworthy semantic Web Technologies for secure Knowledge Management ,IEEE ISSUE-978-0-7695-3492-3,2008
12. H Halpin, Semantic Insecurity : Security and Semantic Web,HAL ,Halid:01673291,2017
13. Anupriya Ankolekar et.al, DAML-S: Semantic Markup For Web Services ,2001
14. Darren Marvin, Steve Taylor, Ronald Ashri, Mike Surridge , Terry Payne et.al, Towards a Semantic Web Security Infrastructure, AAI spring symposium on Semantic Web Services,2004
15. Donald Eastlake et al, XML Signature and Processing version 1.1 ,W3C Website. www.w3.org/TR/xmldsig-core1,2013
16. Tim Berners lee, Artifical Intelligent and the Semantic Web ,W3C Website http://www.w3c.org/2006/talks,2006
17. Deborah et.al ,EMMA: Extensible MultiModal Annotation markup language Version 2.0, http://www.w3.org/TR/emma20,2017
18. Bussler et.al ,A conceptual Architecture for Semantic Web Enabled Services, ACM SIGMOD ,2002
19. S Denker et.al ,The Semantic Web : The Roles of XML and RDF ,IEEE Internet Computing ,2000
20. Guozhu Meng et.al, Collaborative Security: A Survey and Taxonomy, ACM Computing Surveys,2013
21. Huhns and Farkas, Making Agents Secure on the Semantic Web,IEEE Internet Computing,2002
22. Finint and Joshi, Agents Trust and Information Access on the Semantic Web ,SIGMOD ,2002
23. Denker,G.NGUYEN, Semantic of Security Web Service:A Study, Springer-Verlag Berlin Heidelberg, 2004
24. Philip Hallam-Baker et.al, XML Key Management, http://www.w3.org/TR/xkms2,2005
25. Gerber et.al , A Semantic Web Status Model, IEEE Internet Computing ,2006
26. Kagal et.al ,A Policy Based Approach to Security for the Semantic Web, ISWC Springer-Verlag,2003
27. Klyne,Framework for Security and Trust Standards , http://w3.org/2002//SW/Europe,2002
28. Thuraisingham, Security Issues for the Semantic Web ,IEEE Computer Society,2003
29. Palmer ,The Semantic Web : An Introduction , http://Infomesh.net/2001
30. McGuiness et al ,OWL Web Ontology Language Overview, w3c Website, http://www.w3.org/TR/2004/REC-OWL-features,2004

AUTHOR PROFILE

Dr. Suresh kumar received Phd from Faculty of Engineering and Technology, Maharshi Dayanand University, Rohtak, Haryana, India and received the M.tech degree in Computer Science & Engineering from Department of Computer Science & Application , Kurukshetra University , Haryana, India in 2002. His major field of study is Semantic Web. His area of specialisation is Database Management System, Operating System, Semantic Web, Information Retrieval etc . He has more than 15.6 years of teaching experience .He is working as Associate Professor in the Department of Computer Science & Engineering , Ambedkar Institute of Technology, Govt of NCT Delhi, Geeta Colony, New Delhi, India. He is the author/co-author of more than 41 publications in International/National Journals and Conferences.

Jyoti Malik is pursuing M.tech in Information Security, Department of CSE, Ambedkar Institute of Technology, GGS IP University, New Delhi, India and has received B.tech in Computer Science & Engineering from GITM Gurugram, Maharshi Dayanand University, Rohtak, Haryana ,India. Her major field of study is Semantic Web, Cryptography, Trust , Privacy and Data Mining.