Volume: 03, Issue: 01, Pages: 978-983 (2011)

Current Security Considerations for Issues and Challenges of Trustworthy Semantic Web

Akhilesh Dwivedi
Department of CSE, Ambedkar Institute of Technology, GGS IP University, New Delhi, India
Email: dwivedian5@gmail.com
Suresh Kumar
Assistant Professor, Department of CSE, Ambedkar Institute of Technology, GGS IP University, New Delhi, India
Email: sureshpoonia@yahoo.com
Abhishek Dwivedi
Assistant Professor, Department of MCA, Raj Kumar Goel Engineering College, Ghaziabad, India
Email: dwivediabhi@gmail.com
Dr. Manjeet Singh
Associate Professor, Department of CE, YMCA University of Science & Technology Faridabad, India
Email: mstomer2000@yhaoo.com

----------ABSTRACT----------

The advent of the web has resulted in even larger demand for managing privacy, quality and security of information, info and data effectively. This can be because of the fact that these days information on the web represents the biggest body of knowledge ever accessible to any person. Semantic web technologies have several applications because of their expressive and reasoning power. In today's world, security is one in all the foremost vital quality attributes in Semantic web. Semantic web proposes new security requirements; so, previous security mechanisms offer insufficient support for an in-depth treatment of security in trustworthy Semantic web. Many issues need being handling efficiently to appreciate trustworthy Semantic Web.

Keywords : Privacy, Quality, Semantic Web, Security, Trust

Date of Submission: March 06, 2011 Date of Acceptance: May 03, 2011

I. INTRODUCTION

In a row with the extraordinary growth of internet, it is increasingly troublesome to produce useful results. To manage this explosively large amount of web documents, automatic clustering of documents and organizing them into domain dependent directories became highly regarded. The terrific increment of the net has created the evolution of the net itself. From web 1.0 (first generation of internet– 1990 – 2000), web 2.0 and currently has become to web 3.0. Web 1.0 refers to web at its rising stage, with corporate and institutional websites occupying 90 % of the cyber space, with a one-way mode. Therefore, web access serves useful purpose, and other people may read and extract data from the websites. Web access was achieved usually} through telephone dial-up at that point} [1]. “Web 2.0” is remodeling the net into an area that permits anyone to make and share data online—a space for collaboration, conversation, and interaction; an area that is highly dynamic, flexible, and adaptable [2]. Web 3.0 is the terms used to explain the evolutionary stage of the net that follows web 2.0. Generally, it refers to aspects of the net that, though probably attainable, do not seem to be technically or practically possible at this point [3]. We can see differences between web 2.0 and 3.0 in table 1. From the figure 1, it shown that web 1.0 is a one-way platform, web 2.0 is a two-way platform where participation is a key word. Whereas the web 3.0 shows additional intelligences the "web machine" learns, suggests and anticipates what individuals like and would like to induce [4].

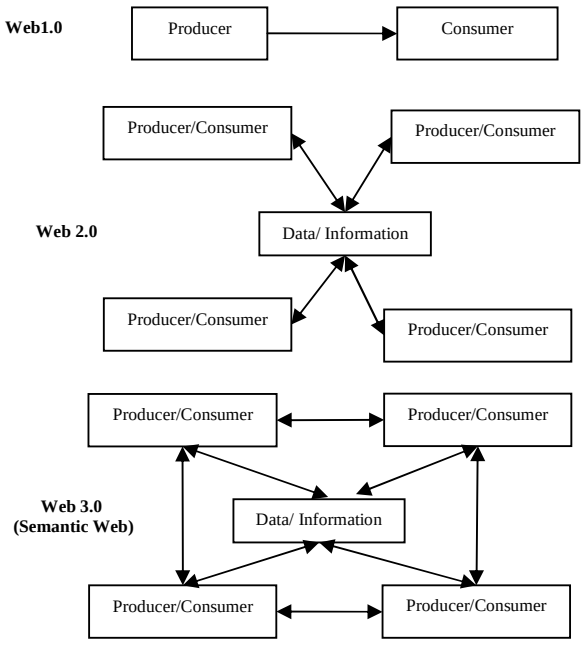

Fig.1 Evolution in web 1.0, web 2.0 and web 3.0 [4]

Volume: 03, Issue: 01, Pages: 978-983 (2011)

II. THE SEMANTIC WEB

The advent of WWW in the mid 1990s has resulted in even bigger demand for managing information, data and knowledge effectively. There is currently such lot information on the net that managing it with typical tools is turning into nearly impossible. New tools and techniques are required to manage effectively this information.

Therefore, to produce interoperability similarly as warehousing between multiple knowledge sources and systems, and to extract data from the databases and warehouses on the net, numerous tools have been developed. One among the recent developments with the internet is the semantic web by Tim Berners Lee, Jim Handler and others [6].

The semantic web is regarding machine understandable web content. In the article on semantic web by Sir Tim Berners Lee et al., the semantic web is described to be a web that may perceive and interpret web content and manage activities for people. These activities might be maintaining appointments, giving recommendation, and primarily creating the life of the human as simple as possible. If the semantic web is to be effective, then we want to make sure that the information knowledge on the net is timely, accurate, and precise [9].

Table.1 Differences between web 2.0 and web 3.0 [5]

	Web 2.0	**Web 3.0**
Main task	Focus the power of community to create dynamic contents and interaction technology	Linked devices and data, people across the web
Linking	Walled gardens inhibit interoperability	Data and devices linked more easily and in new ways
Content	Individual and organization create content	Individual, organization, machine create content which can be reused
Technology	AJAX	Resource Description framework (RDF)
Website	Google, Face book, Wikipedia, e-bay, You-tube	dbpedia, sioc-project.org

Note that with bad information one cannot build smart choices. Therefore, we want to develop ways in which to include quality parameters into the technologies for the semantic web. These technologies embody XML, (extensible Markup Language), RDF (Resource Description Framework), and agents (see [8]). There is very little work reported on knowledge quality, security and integrity for the semantic web. We want to begin investigating the problems where we have a tendency to conduct analysis on the semantic web. We mentioned some preliminary concepts in [9] for dependable semantic web. If data quality, integrity and security are added as an afterthought, then it will be very tough to make sensible systems. Here we will undergo the developments with the semantic web and then discuss a number of the work described in [9] for dependable semantic web. This may compromise quality as data may originate from untrusted sources and be passed from one to another. We tend to focus more on the security issues and challenges for the trustworthy semantic web.

III. KEY SECURITY CONSIDERATIONS AND CHALLENGES

We are going to discuss some aspects of security here. We will elaborate on some issues. First of all the technologies that structure the semantic web need to be secured. These embody XML, RDF, agents, the infrastructures as well as the data management and knowledge management technologies.

3.1 Semantic Web Dependability Aspects

While the semantic web as an idea continues to be evolving, there are several developments in this area. These embody RDF, Ontologies, Agents, and Databases. One may envisages publish and subscribe model for the net where producers publish the services while customers subscribe for the services. Agents act on behalf of users. There are numerous kinds of agents including brokers. These brokers negotiate the most effective deals for their customers. These services might be managing schedules and appointments as well as giving recommendation and primarily managing all of the activities for a client. By Dependability, we mean security, fault tolerance, integrity, data quality, and real-time processing. It will be troublesome to make sure that all the constraints should meet. The challenge is to develop quality of service constraints for the semantic web. For instance, the agents that interact with one another ought to be secure and meet the timing constraints. We want to make sure that they are fault tolerant. The information being exchanged like XML documents have to be compelled to be of prime quality. Varied access management policies have to enforce for XML documents. Trust issues also are important. As an example, to what extent do you trust your source? The remaining sections concentrate on two aspects, data quality for the semantic web and real-time services for the semantic web.

3.2 Data Quality for the Semantic Web

Data quality attributes would come with data like timeliness, accuracy and precision. We anticipate that the semantic web would require techniques to manage the standard of knowledge on the net. A lot of the interest in data quality is attributable to attempt to integrate knowledge from previously unconnected systems, typically in a data warehouse. The semantic web can be described as a virtual integration of knowledge and services on the net.

The semantic web enables relationships between information from previously unconnected sources, and propagation of information from one organization to a different. Therefore, users of the semantic web will want a way to work out the standard of knowledge used. In

Volume: 03, Issue: 01, Pages: 978-983 (2011)

essence, it is necessary to know the standard of data if one is to attain semantic understanding of the knowledge. High quality data is essential for e-commerce transactions. These transactions may involve massive sums of cash, and if the information is of poor quality, the result is disastrous. Several of the companies that have studied data quality (within their internal systems) have found that quality issues can directly trace to vital loss of revenue. Some industrial tools currently address data quality problems; however, several of these specifically influence common issues with client names, addresses, and phone numbers. This tuning is not directly applicable to ecommerce and therefore the semantic web, where contact with customers is essentially electronic (although, one might imagine similar tools for email addresses). Some additional versatile tools are raising that use data mining techniques to spot statistically anomalous information.

Quality attributes like worth are subjective, and it is not usually necessary for others to understand their semantics. However, in the semantic web, the selections and business processes of one user will typically be used to make data products employed by others. The semantic web allows data supply chains (including long ones) by defining semantics for the products at each link in a chain. Like other forms of supply chains, a data supply chain using the semantic web can solely be as dependable as its weakest link. Therefore, the net will need to propagate quality attributes from producers to customers, and users will want ways to outline or derive quality attributes for product from those of the data they use to provide those product.

3.3 XML Security

Numerous analysis efforts are reported on XML security (see for example, [10]). We tend to discuss a number of key points. The main challenge is whether to offer access to entire XML documents or elements of the documents. Bertino et al have developed authorization models for XML [15]. They have targeted on access management policies as well as on dissemination policies. They conjointly thought of push and pull architectures. They specified the policies in XML [15]. The policy specification contains data regarding which users can access those parts of the documents. In [10] algorithms for access control as well as computing views of the results are presented. Additionally, architectures for securing XML documents also are mentioned. W3C (World Wide Web Consortium) is specifying standards for XML security.

3.4 RDF Security

RDF is that the foundations of the semantic web. Whereas XML is restricted in providing machine understandable documents, RDF handles this limitation. As a result, RDF provides higher support for interoperability as well as looking and cataloging. It additionally describes contents of documents as well as relationships between numerous entities within the document. Whereas XML provides syntax and notations, RDF supplements this by providing semantic information in a standardized manner. The fundamental RDF model has three types: they are resources, properties and statements. Resource is something described by RDF expressions. It might be an internet page or a set of pages. Property may be a specific attribute used to describe a resource. RDF statements are resources in conjunction with a named property and the worth of the property. Statement parts are subject, predicate and object. It is necessary that the supposed interpretation be used for RDF sentences. RDF schemas can accomplish this. More advanced ideas in RDF embody the container model. The container model has three kind of container objects and that they are Bag, Sequence, and different. RDF additionally provides support for creating statements concerning different statements. For any data on RDF, we check with the superb discussion in the book by Antoniou and van Harmelen [11]. Currently {to make the semantic web secure, we need to make sure that RDF documents are secure. this may involve securing XML from a syntactic point of view. With RDF, we have to be ensuring security is preserved at the semantic level. The problems embody the security implications of the ideas resource, properties and statements. That is, how is access management ensured? How can statements, properties and statements be protected [24]? How will one give access control at a finer grain of granularity? What are the security properties of the container model [24]? How will baggage, lists and alternatives be protected? Can we specify security policies in RDF? How can we resolve semantic inconsistencies for the policies? How can we protect RDF schemas? These are troublesome queries and we need to find answers (see also [12]).

3.5 Secure Ontologies

Ontologies are representations of varied ideas to avoid ambiguity. Varied ontology is developed. Agents use this ontology to grasp the online pages and conduct operations like the mixing of databases. Furthermore, RDF or special languages like web ontology language (OWL) are used to represents ontology. Now, ontology need be secure. That is access to the ontology must be controlled. This suggests that different users may have access to different components of the ontology. On the other side, ontology could also be used to specify security policies simply as XML and RDF are used to specify the policies. Later on, we discuss ontology and security. That is, we describe how ontology can be secured and how ontology can be used to specify different policies.

3.6 SSL Certificate Problems

Secure Sockets Layer (SSL) is a protocol that establishes secure communications for such activities as internet browsing, e-mail, instant messaging and different information transfers. An SSL certificate issued by a third party provides privacy and security to transmissions between two computers on a public network by confirming that a message truly did come from the person identified. Issues with SSL certificate will cause several internet browsers to block users from accessing web site, or to show a security warning message when web site is

Volume: 03, Issue: 01, Pages: 978-983 (2011)

accessed. The host name of web site (the URL) should match the topic name(s) of your SSL certificate. Netscape in 1996 has introduced transport Layer Security [16], having common name "Secure Sockets Layer (SSL)". It consists of two main parts: The Record Layer encrypts/decrypts TCP data streams using the algorithms and keys negotiated in TLS Handshake, which is additionally used to authenticate the server and optionally the consumer. These days it is the foremost vital cryptographic protocol worldwide, since it is implemented in each internet browser. TLS offers various choices for key agreement, encryption and authentication of network peers, however most often the subsequent configuration is used: the online server is configured with a X.509 certificate that features its domain name. This certificate should be issued from a "trusted" certification authority (CA), where "trusted" means that the foundation certificate of this CA is included in nearly all internet browsers [22]. During the TLS Handshake, the server sends this certificate to the browser. The browser checks that the certificate comes from a "trusted" CA, which the domain name within the certificate matches the domain name contained within the requested URL. If each check succeeds, the browser continues loading the online page. If there is a haul, the human user is asked for a (security) call. The browser itself remains anonymous inside this TLS configuration. To authenticate the user, typically a username/password is requested by the server through an HTML form. This TLS configuration worked fine for all internet applications, until the primary Phishing attacks surfaced in 2004. In an exceedingly Phishing attack, the attacker lures the victim to a pretend website (either using spoofed emails or attacks on the DNS), where the victim enters username and password(s). This is possible even with TLS, since the human user fails to verify the authentication of the server via TLS [17].

3.7 SWS-Security

SWS-Security is defining the way to give integrity, confidentiality and authentication for SOAP messages. WS-Security defines a SOAP header (Security) that carries the WS-Security extensions [23]. Additionally, it defines how existing XML security standards like XML Signature and XML Encryption are applied to SOAP messages. XML Signature permits XML fragments to be digitally signed to make sure integrity or to proof authenticity. The XML Signature component has the subsequent (slightly simplified) structure:

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethodAlgorithm="..."/>
     <SignatureMethod Algorithm="..."/>
     <Reference URI="..." >
     <DigestMethod Algorithm="...">
     <DigestValue>...</DigestValue>
    </Reference>
    </SignedInfo>
   <SignatureValue>...</SignatureValue>
</Signature>
```

The signing method works as follows: for each message part to be signed a Reference component is formed and this message part is canonicalized and hashed. The ensuing digest is added into the DigestValue element and a reference to the signed message part is entered into the URI attribute. Finally, the Signed information part is canonicalized and signed. The result of the signing operation is placed within the Signature worth part and the Signature part is added to the security header. XML Encryption permits XML fragments to be encrypted to ensure information confidentiality. The encrypted fragment is replaced by an Encrypted information part containing the cipher text of the encrypted fragment as content. Further, XML Encryption defines an Encrypted-Key element for key transportation functions. The most common application for an encrypted key is a hybrid encryption: an XML fragment is encrypted with a randomly generated symmetric key, which itself is encrypted using the general public key of the message recipient. In SOAP messages, the Encrypted Key part should seem within the security header. Additionally to encryption and signatures, Security defines security tokens appropriate for transportation of digital identities, e.g. X.509 certificates [22].

3.8 Trust for the Semantic Web

Recently there has been some work on trust and the semantic web. The challenges embody how one trusts the data on the web. How does one trust the sources? How does one negotiate between different parties and develop contracts? How does one incorporate constructs for trust management and negotiation into XML and RDF? What are the semantics for trust management? Researchers are functioning on protocols for trust management. Languages for specifying trust management constructs are being developed. For instance, if X trusts Y and Y trusts Z, then will X trust Z? How does one share the info and knowledge on the semantic web and still maintain autonomy. How does one propagate trust [13]? For instance, if X trusts Y at say 50% of the time and Y trusts Z 30% of the time, then what worth does one assign for X trusting Z? How does one incorporate trust into semantic interoperability? What are the standard of service primitives for trust and negotiation? That's, for sure things one might have 100 percent trust whereas for different things 50% trust might suffice. Another topic that is being investigated is trust propagation and propagating privileges [21]. For instance, if you grant privileges to X, what privileges will X transfer to Z? How are you able to compose privileges? Is there an algebra and calculus for the composition of privileges? A lot of analysis still has to be done here. One in all the layers of the semantic web is Logic, Proof and Trust. This layer deals with trust management and negotiation between different agents and examining the foundations and developing logics for trust management [13].

IV. SECURE TRUSTWORTHY SEMANTIC WEB

We mentioned some aspects of security in earlier sections. First of all the technologies that form up the semantic web have to be secure. These embody XML, RDF, agents, the infrastructures as well as the data management and information management technologies. We need to make sure that security is preserved when integrating the technologies. For instance, one desires proper access to the XML documents. Furthermore, these documents should be encrypted for the applications. The agents that perform the processing should communicate securely. Numerous security technologies for the net do exist at the present. These technologies should be evaluated for the semantic web. There is the need to incorporate security semantics into semantic interoperability. The varied logics being developed for the semantic web should be examined and security properties should be incorporated. One example is logic for secure data and knowledge based systems known as NTML (Non-monotonic Typed Multilevel Logic) mentioned in [7]. We need to conduct similar analysis for the semantic web. Because of the opportunities for unauthorized inferences through data mining tools, the semantic web may exacerbate the inference issues. We need to look at this issue for the semantic web. We also need to sure that unauthorized intrusions are prevented and detected.

Here, we are applying trustworthy semantic web technologies for guaranteeing that social networks maintain security and privacy. Researchers have done some work on the secure interoperability of databases [14]. We need to revisit this analysis and then confirm what else must be done in order that the data on the net is managed, integrated and exchanged securely. We conjointly need to examine the inference problem for the semantic web as inference is embedded into the descriptive logics for the semantic web. Inference is the method of posing queries and deducing new data. It becomes a problem when the deduced data is something the user is unauthorized to understand. A discussion of the inference problem for the semantic web is given in [18], [20], and [21]. While XML, RDF and OWL documents have to be secure, we can conjointly use these specification languages (e.g., XML, RDF, OWL) to specify policies. There has been plenty of work on specifying policies in XML. For instance, Bertino et al have used XPath expressions to specify policies [19]. These policies are then applied to secure XML documents. In addition to handling confidentiality policies, their work is also specializing in specifying privacy policies as well as trust policies in XML [15].

V. CONCLUSIONS

In this paper, we have presented a variety of problems with trustworthy semantic web security. we investigated ongoing problems with application of XML Signature and the web services security mentioned the importance and capabilities of browser security in the trustworthy semantic web security are various, and each of them needs an in depth analysis on their potential impact and relevance to real-world situations. As will be derived from our observations, a primary sensible place to begin for improving security consists in strengthening the protection capabilities of both web browsers and web Service, at best integrating the latter into the first. Thus, as a part of our ongoing work, we are going to still harden the foundations of trustworthy semantic web security that are laid by the underlying tools, specifications, and protocols used in the trustworthy semantic web scenario. Several efforts are under way to develop ontologies and mark-up languages for various information sorts and applications. However, security has not received much attention apart. Therefore, as we discuss the assorted standards, we would like to ensure that security problems are addressed totally. For more details, we refer to [13]. Whereas there are efforts like the work of W3C and OASIS to develop security standards like XACML and SAML specifications, much has to be done to deal with various security problems together with advanced confidentiality policies additionally to trust and privacy policies that are required for secure data management [15]. Furthermore, we would like to still develop ontologies in order that organizations can integration and share data to hold out effective collaboration in a very secure manner. Security cuts across every layer of the semantic web. One wants secure XML. That is, access should be controlled to numerous parts of the document for reading, browsing and modifications. There is analysis on securing XML and XML schemas. The succeeding step is securing RDF. Currently with RDF not only do we need secure XML, we additionally need security for the interpretations and semantics. As an example under certain contexts, parts of the document are also unclassified whereas under certain alternative contexts the document may be classified. One has to insert security into the system right from the start. Similarly, security cannot be an afterthought for the semantic web.

REFERENCES

[1] The Development of '.hk' with Internet Trends from Web 1.0 to Web 3.0, Available: https://www.hkdnr.hk/webupdate/article/pdfs/RTHK%20Article%20Final%20_Eng_%20revised.pdf

[2] Building a Library Web Site on the Pillars of Web 2.0.Available:http://www.infotoday.com /cilmag/jan07/Coombs.shtml, viewed on 22Feb 2011.

[3] Web3.0,Available: http://en.wikipedia.org /wiki/Web_3.0, viewed on 22 February 2011.

[4] From web1.0 to web3.0: get the point in a picture. Available: http://fredericmartin.typepad.com/myblog/2007/11/from-web10-to-w.html, viewed on 22 February 2011.

[5] Web3.0,Available: http://webuser.hsfurtwangen.de /~heindl/ebte-08ss-web-20-Suphakorntanakit.pdf, viewed on 22 February 2011.

[6] Berners Lee T. et al, "The Semantic Web", Scientific American, May 2001.

[7] Thuraisingham B., "NTML: Nonmonotonic Typed Multilevel Logic for Secure Data and Knowledge Base Management Systems", Proceedings of the

Volume: 03, Issue: 01, Pages: 978-983 (2011)

Computer Security Foundations Workshop, Franconia, NH, 1991.
[8] Thuraisingham B., "XML, Databases and the Semantic Web", CRC Press, 2002
[9] Thuraisingham,.Hughes, Allen, "Dependable Semantic Web", IEEE WORDS 02, San Diego, CA, 2002
[10] Bertino, E. et al, Secure Third Party Publication of XML Documents, To appear in IEEE Transactions on Knowledge and Data Engineering, 2004.
[11] G. Antoniou and F. van Harmelan, "A Semantic Web Primier", MIT Press, 2003
[12] Carminati, B., et al, Security for RDF, Proceedings of the DEXA Conference Workshop on Web Semantics, Zaragoza, Spain, 2004
[13] B. Thuraisingham, Building Trustworthy Semantic Webs, CRC Press, 2007.
[14] B.Carminati, E.Ferrari, M.Kantarcioglu, Thuraisingham, Semantic web technologies for Secure social networking, UTD Tech Report, 2008
[15] E. Bertino et al, Secure Knowledge Management, IEEE Transactions on Systems, Man and Cybernetics, May 2006
[16] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," IETF RFC 5246, 2008, http://www.ietf.org/rfc/rfc5246.txt.
[17] R. Dhamija, J. D. Tygar, and M. A. Hearst, "Why phishing works," in Proceedings of the 2006 Conference on Human Factors in Computing Systems (CHI), Montr´eal, Quebec, Canada. ACM, 2006, pp. 581–590.
[18] Farkas, C. and A. Stoica, Correlated Data Inference, Proceedings data and Applications Security Conference, 2003
[19] Bertino, E. et al, Secure Third Party Publication of XML Documents, To appear in IEEE Transactions on Knowledge and Data Engineering, 2004.
[20] Thuraisingham B., "Security Standards for the Semantic Web", Computer Standards and Interface Journal, 2005
[21] Nathalie Tsybulnik and Bhavani Thuraisingham, "Administering the semantic web: cpt: confidentiality, privacy and trust management", Technical Report UTDCS-06-06 Department of Computer Science The University of Texas at Dallas, February 2006, pp. 1-19.
[22] Kumar, S. Prajapati, R.K. Singh, M. De, A., "Security Enforcement using PKI in Semantic Web", International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2010 ,pp. 392–397
[23] Suresh Kumar, Rakesh Kumar Prajapati, Manjeet Singh, Asok De," Realization of Threats and Countermeasure in Semantic Web Services", International Journal of Computer Theory and Engineering, Vol.2, No.6, Decr 2010, pp. 1793-8201
[24] Thuraisingham, B., Security Issues for the Semantic Web Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC'03) IEEE, 2003.

AUTHORS BIOGRAPHY

Mr. Akhilesh Dwivedi received the B.Tech degree in Electronics and Telecommunication Engineering from the MGM College of Engineering & Technology, Noida (U.P. Technical Univ., Lucknow) India, in 2009 and pursuing M.Tech in Information Security from Ambedkar Institute of Technology, Govt. of NCT Delhi, Geeta Colony, New Delhi (Guru Govind Singh Indraprastha University, New Delhi), India. His main research interests are in Biometric Security and Secure Semantic Web Services, Cryptography and Network Security, Data Storage Security in Cloud Computing. Mr. Dwivedi is the member of AIRCC, IAENG, IACSIT, and IAOE. He is the author/co-author of more than eight publications in International/National journals and conferences.

Mr. Suresh Kumar received the M.Tech degree in Computer Science & Engineering from Department of Computer Science & Application, Kurukshetra University, Haryana, India in 2002 and pursuing Ph.D from Faculty of Engineering & Technology, Maharshi Dayanand University, Rohtak, Haryana, India. His major field of study is Semantic Web. His current research interest includes Secure Semantic Web Services, Semantic Search, Cloud Computing, Cryptography and Network Security, Biometric Security. He has more than nine years teaching experience. He is working as Assistant 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 16 publications in International/National journals and conferences.

Mr. Abhishek Dwivedi, Master of Computer Application from Uttar Pradesh Technical University, Lucknow (U.P.), India. Pursuing Ph.D from Singhania University, Pacheri Beri, Rajasthan, India. His major fields of studies are Information security, Cryptography and Network security. His main research interests are in Cryptographic Protocol, Public Key Cryptography and its applications, Secure Semantic Web and Data Storage Security in Cloud Computing. He has more than four years of experience in teaching. He is working as Assistant Professor in the Department of MCA, Raj Kumar Goel Engineering College, Ghaziabad (U.P.), India. He is the author/co-author of more than 25 publications in International/National journals and conferences.

Dr. Manjeet Singh is currently working as an Associate Professor (CE) at YMCA University, Faridabad, Haryana, India. He has completed his M.Tech from GJU, Hissar and Ph.D from MDU University. Rohtak, Haryana, India. His areas of interests are Natural Language Processing and Internet Technology.