International Journal of Computer Applications in Engineering Sciences
[VOL I, ISSUE II, JUNE 2011] [ISSN: 2231-4946]

Safe Semantic Web and Security Aspect Implication for Social Networking

Devendra Kumar Sloni[#], V. K. Sharma[*]

[#] *Bhagwant University, Ajmer (Raj.) India -305 001*
[*] *Bhagwant Institute of Technology, Muzaffarnagar (UP) India -251 315*

[1]devansloni@yahoo.com
[2]viren_krec@yahoo.com

***Abstract*-- Web 3.0 is one of the terms used to describe the evolutionary stage of web that follow 2.0. World Wide Web is a system of interlinked hypertext documents accessed via the internet. The last few years have seen the rise of a new trend on the Internet: online social networks, educational semantic web etc. Social and educational networks represent a new opportunity to online uses and a challenging scenario to security community. A user demands the acceptance of new tools and techniques, which are the object of this paper. Here we describe ways of semantic web security implementation through layers. These layers are represented in XML security, RDF security and in an idea of semantic web security standardization. And we are focusing on its security suggestion with point of view in the near future.**

***Keywords* – Social network and future, Aspect Security, Ontology, XML Schema, RDF Schema**;

I. INTRODUCTION

One of the most prized assets in today's world course information. Information, as the foundation of web today, usually appears on the form of documents or data (articles, reports, texts, pictures etc). That can be searched, browsed and combined in various ways. It is difficult extract desired information in a reasonable time. The beginning of the World Wide Web has resulted in even greater demand for managing data, information and knowledge effectively. New tools and techniques are needed to effectively manage this data. Therefore, to provide interoperability as well as warehousing between the multiple data sources and systems, and to extract information from the databases and warehouses on the web, various tools are being developed. Therefore the web is developing into what is now called the semantic web. The semantic web [1] is visions of an Internet in which web resources are improve with machine-processable metadata that describes their meaning. This will enable computers to interpret and extract web content much more effectively and precisely than today's XML-based approaches to allow interoperability. Tim Berners Lee, the father of WWW, realized the insufficiency of current web technologies and subsequently struggles to make the web more intelligent.

A semantic web can be thought as a web that is highly intelligent and sophisticated and one needs little or no human involvement to carry out tasks such as scheduling appointments, coordinating activities or nearby devices, searching for complex documents as well as integrating disparate databases and information systems. While much progress has been made toward developing such an intelligent web there is still a lot to be done. For example, technologies such as ontology matching, intelligent agents, trustful information, and markup languages are contributing a lot toward developing the semantic web.

The last few years have seen the rise of a new trend on the Internet: online social and educational networks. Social and educational network is the grouping of individuals into specific groups, like small rural communities or a neighborhood subdivision [2]. Such networks quickly became a global and cultural phenomenon by adapting the concept of real-life social groups and interactions to cyber space. Web 2.0 technologies have been authorize social network platforms by making them more interactive, and the majority of online users are already attached to one or more social – n – educational networks. These kinds of networks are changing the way users interact, share information (personal data, opinions and news) and do business online, turning the communication-focused Internet that we know into a new social Web platform.

Social networks have their drawbacks. In the face of the specific security risks related to their normal usage (information disclosure and privacy issues), they have become an attack vector for phishers, fraudsters and sexual predators. Cyber criminals are adapting their strategies and tools to target social network users and are improving their attack technologies to target Web 2.0 applications. From the user perspective, trust and privacy on the social Web remains a hot, yet unresolved topic.

As the web progress into the semantic web, there are more and more possibilities for security breaches as we introduce new technologies. Therefore, it is critical that security is considered right from the beginning of development of the semantic web. For the semantic

web to be secure we need to ensure that all of the layers of the semantic web are secure. This includes secure XML, secure RDF, secure ontologies, and ensure the secure interoperation of all these technologies.

II. MODERN STATUS OF SOCIAL NETWORK

A. History

SixDegrees.com was the first recognizable social networking site, launched in 1997. It allowed users to create profiles, list their friends, surf the friends' lists and send messages, representing the first provider to combine the most popular social networking features. From 1997 to 2001, a number of community tools began supporting various combinations of profiles and publicly spoken friends, such as AsianAvenue, BlackPlanet, MiGente and LiveJournal [3] (see Figure - 1.1).

The first business-oriented network site, Ryze.com, launched in 2001, was followed by Tribe.net, LinkedIn and Friendster. Friendster gained grip among early adopters and grew to 300,000 users through word of mouth before gaining attention from traditional press media, building the road to MySpace and Facebook. From 2003 on, several social networking sites launched and became popular, proliferating worldwide.

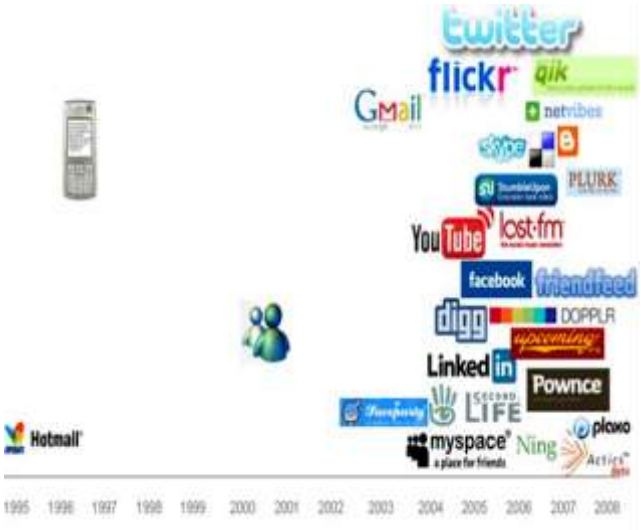

Figure -1.1

B. Social Network Folksonomy and Theorical Model:

Online social networks introduced a new organizational framework for online communities, and a exciting new research context. Web 2.0 applications and folksonomies1 have led to new user experiences and give up rich materials that are demanding appropriate representations to be efficiently studied and mapped.

Social Tagging / Folksonomy are present in the current social networking sites and applications by the adoption of shared tagging capabilities. Social network analysis (SNA) forms a family of methodologies to map and evaluate relationships and data flows between people, groups, communities or any type of social structures. This includes theories and abstract models as the "small world property," social graphs and semantic Web.

1. Digital Identities

Social identities are the names, nicknames, or aliases that users create to identify themselves on online social networking sites. Users adopt different nicknames or aliases in groups they belong to and usually each one of these groups has different privacy concerns; there are public profiles and private or closed profiles. The possibility of having different social information listed on different groups is one of the key characteristics of social identities. Depending on the nature and scope of a social network, users' identities have different purposes and might not be associated with a user's real identity.

2. Representing Social Data with Semantic Web

Research in Semantic Web has provided models to leverage the richness of the online social interactions that the social networks represent. Semantic Web researchers provide models to capture such activities and turn the information into collective intelligence. Researchers see social data as a two-fold structure: data that describes the social network and data that describes what their members produce. There are several ontologies that are well suited for linking together data across various social networks include Friend of a Friend (FOAF) and Semantically-Interlinked Online Communities (SIOC). FOAF represents a profile about an individual and links data from one social network to another. SIOC aggregates data from various Web-based media (including wikis, and blogs) and presents information to users in the most appropriate representation. [4] In addition, the Simple Knowledge Organization System (SKOS) offers a way to organize manipulated concepts and to link them to SIOC descriptions. SKOS provides a standard way to represent knowledge organization systems using the Resource Description Framework (RDF). Encoding information in RDF allows it to pass between computer applications in an interoperable way. An RDF-based description of social data forms a rich-typed graph and offers a powerful way to represent online social networks. Semantic Web technologies are appropriate means for modeling and formalizing to extract the knowledge produced by online social interactions (see Figure 1.2). Indeed, by connecting social networks to FOAF and social activities such as blogs comments to

SIOC, Semantic Web provides a complete interlinked graph on top of existing networks.

http://foaf-project.org
http://sioc-project.org
4 http://www.w3.org/2004/02/skos
5 http://www.w3.org/RDF

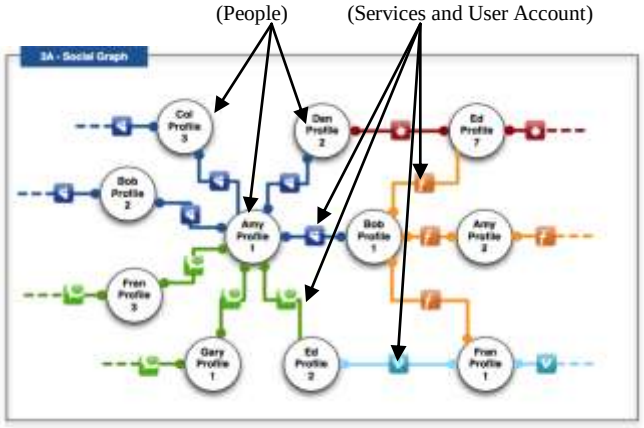

Figure -1.2: Social Graph Representation Using Semantic Web

C. *Current Problems*

Most of social networking sites provide very little interaction with external online services. They operate as "walled gardens," where the users' content is exclusive to the site and there is no way to share it with outside Internet applications. The reason for this lays behind the fact that sites' business models center on having the largest possible user base, and user lock-in is a major part of that strategy. There is a great desire by many users to have an interoperable format that allows them to transport their social interactions across different sites. In addition, as a user struggles to gain reputation within one site, he or she wants to take that reputation to another world. As things are now, in order to switch to a new social networking site, a user would have to start from scratch, making new contacts and creating their online identity.

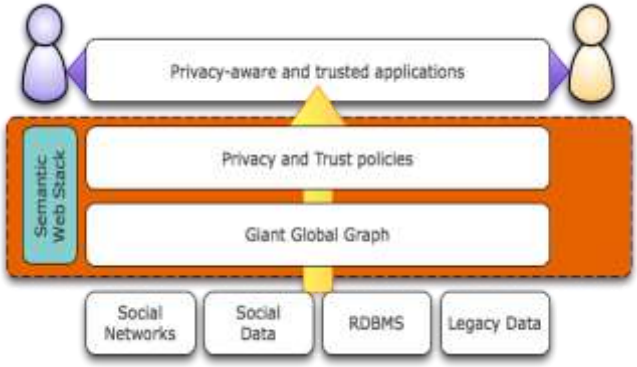

Figure 1.3 Interoperability with semantic web

1) *Trust Management*

Trust is a key concept to determine when to establish relationships with profiles from known people or strangers, much like in the real world. To build new relationships, users must be confident that are connecting to whom they expect. Reputation management and tagging technologies help users to assess trustworthiness of third-party information online. Global tagging and aggregation is a great way to build trust on the web and to find resources within a trusted social network.

2) *Privacy*

Privacy means that user profiles should never give out any information not explicitly slated to be publicly available. People tend to publish personal information on the Web, be it Pictures, opinions, videos or personal home pages, comprising sensitive information such as birth dates, home addresses and personal phone numbers. Since online users are usually querying and searching profiles, groups and forums about other users' information, protection needs are always on the side of everyone's personal privacy.

III. FUTURE OF SOCIAL NETWORK

Social networking sites are a relatively new phenomenon, and as with any other technological innovation, they will continue to have a long period of both technical and social adjustments and improvements to fit in people's needs and behaviors. People will also adjust their online practices in the light of the new social networking technologies.

A. *Meta-Social Networks and User-Centric Social Universes*

With users occupying multiple roles and having dynamic social networks that can grow and shrink, an important aspect in the future of social networks is that users will be able to manage their profiles and connections using meta-social network tools. In this scenario, the user will become the center of his or her social network, adding a cross-network friendship in its virtual centralized profile.

B. *Social Web Bill of Right*

As a response to the endless discussion on data and privacy rights, on September 2007, Open Social Web group11 promoted the "Bill of Rights for the Social Web,"12 a straightforward document put out by four Web 2.0 pioneers. It outlines how companies should treat the data they collect from users of social network

sites, as personal data, who the user is connected to, and users' content.

C. Virtual Currency

Wikipedia defines virtual economy as the emergent economy existing in virtual worlds, usually by the exchanging of virtual goods in the context of an Internet game [5]. Each virtual world has its own virtual economy and virtual currency based on the exchange of virtual goods.

D. Mobile Social Networking

Essentially, since both social networking and mobile usage are ubiquitous and growing, the overlapping demographics will generate plenty of new opportunities to mobile social networking in the coming years. The benefits that mobile social networking can bring in terms of enhanced location awareness and availability need to be balanced with the responsibility inherent of these features and the specific user's requirements for personal privacy.

E. Sensor Network

An increasing amount of portable devices are supporting sensor-based interactions, from peripherals (Nike and iPod) to integrated sensors (the iPhone's accelerometer). Sensors are becoming more prevalent in mobile devices in recent years. By supporting Bluetooth and WiFi communication, mobile phones have now become sensor gateways for individuals. A wide range of Bluetooth sensors, such as heart monitors and environmental monitors, can be associated with these mobile phones, enabling a new paradigm—the personal sensor network—in which the individual becomes the sensor hub.

F. Social TV

Internet protocol television (IPTV) comes up in the market as next generation for television, where users are able to watch television wherever they are. Social networking brings many favorable social services to television watchers based on IPTV technology and the ability of people to share their experiences and opinions.

G. E-Learning through Networking

Schools and higher education foundations are increasingly using social networking as a communications and collaboration tool of choice. As such, in the near future, it would be beneficial for schools to promote online interaction through social networking sites.

IV. SECURITY ASPECTS OF SOCIAL NETWORKING

A new paradigm provides a lot of opportunities, but when it is done without the necessary security requirements kept in mind, it serves as a deterrent to growing and user adoption. In addition, since social networks attract thousands of users who might represent potential victims, social networks represent a very desirable target to mass attackers.

A. Current Security Threats

As the popularity of social networks started to increase, hackers, fraudsters and malicious users started using them to run illegal activities, either by using the social networks as attack vectors to traditional cyber crimes, by creating specific threats to social networking users or by running direct attacks to disrupt social networking sites.

Social networks have by nature some intrinsic properties that make them ideal to be exploited by an online criminal: a huge and highly distributed user-base made of clusters of users sharing the same social interests, thus developing trust with each other.

B. Privacy

The availability of personal information on social networks provides ideal conditions for actors to abuse such information and leverage it. The inappropriate exposure of sensitive information might represent a good opportunity for criminals and terrorists to conduct "criminal data mining." Bad actors could use unflattering material or personal information from social networks to select their targets, profile their victims, and plan and execute their activities.

C. Malicious Code, Viruses and Worms

Malicious code utilizes infected users' social network accounts to collect friend information and use it to proliferate. In addition, many attackers use social networks to create fake profiles and publish fake links that lead to sites infected with malicious code. Banner ads, video content and fake social network profiles have become a pipeline for stealing personal information as more consumers jump online. There are malicious codes distributed through pop-up ads, and not all of them require a click by the user.

In January 2009, iDefense investigated attackers utilizing the my.barackobama.com website, a social network for President Obama supporters, to spread malicious code. The attack utilized fake images trying to convince users to install a malicious executable file through fake Flash codec errors. Attackers injected the same URLs into many different websites and forums, suggesting that attackers utilized automatic forum crawling and account creation programs.

D. Sexual Crimes and Child Safety

Social networking environments represent a serious risk to teenagers and younger children, as they

can be victims of several threats as cyber bullying, online harassment and sexual predators. Usually, children who are at risk online are those who are also at risk offline. The most frequent threats to children on social networking sites in general come from their peers, young adults and predatory older adults.
Social network providers have a hard time keeping their sites entirely clear of sex offenders, given the huge number of users and the fact that not all of them use their real identities.

E. Social Networks under Attack

Social network providers, as with any other Web application, might be vulnerable and become the target of a direct attack. Security vulnerabilities could provide hackers with a means to attack providers and cause service failures unauthorized access to users' credentials (followed by disclosure of private information) or could be used by a virus to be spread amongst user accounts. Cross-site scripting (XSS) or SQL injection vulnerabilities on social network applications could cause huge problems to millions of users.

V. LAYERS FOR THE SEMANTIC WEB

Tim Berners Lee has specified various layers for the semantic web (Figure 1.4).

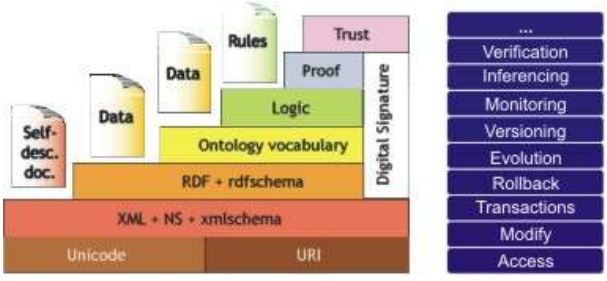

Figure 1.4

A. Layer 1: URI and Unicode:

Unicode is considered as the universal standard encoding system [6] for computer character representation [7]. Web pages can use a variety of character encoding such as ASCII, Latin-1 or Unicode. Most encoding systems represent only few languages while Unicode represents all languages such as Arabic, English and Chinese. While URI which stands for Uniform Resource Identifier (URI) provides a simple and extensible way for identifying resources. A resource can be anything that has an identity such as a web site, a document, an image and a person [8]. Protocols that exist on this layer are TCP/IP, SSL and HTTP, as the protocols for data transmission. They are built on top of more basic communication layers [9]. With these protocols one can transmit the web pages over the Internet. At this level one does not deal with syntax or the semantics of the documents.

B. Layer 2: XML, *XML* schema and namespaces:

Layer 2 consists of XML, XML Schema and Namespaces. XML is a language used to represent data in a structural way. It describes what is in the document, not what the documents looks like, while XML Schema provides grammars for legal XML documents [10]. This is one of the significant developments of the WWW. Without some form of common representation of documents, it is impossible to have any sort of meaningful communication on the web. XML schemas essentially describe the structure of the XML documents. Both XML and XML schemas are the invention of Tim Berners Lee and the W3C [11].

C. Layer 3: RDF and RDF schema:

Layer 3 consists of the Resource Description Framework (RDF) and the Resource Description Framework Schema (RDF Schema). RDF is a way for representing, exchanging and reusing of metadata [12][13]. RDF uses URIs to identify web resources and uses a graph model for the purpose of describing the relationship between different resources [7]. RDF Schema is a simple modeling language introducing classes of resources, properties and relations between them [7].

D. Layer 4: Ontology vocabulary:

Ontology is considered the backbone for the semantic web architecture provides a machine-processable semantics and a sharable domain which can facilitate communication between people and different applications. Next layer is the Ontologies and Interoperability layer. Now RDF is only a specification language for expressing syntax and semantics. The question is what entities do we need to specify? How can the community accept common definitions? To solve this issue, various communities such as the medical community, financial community, defense community, and even the entertainment community have come up with what are called Ontologies. One could use Ontologies to describe the various car models of the world or the different types of aircraft used by the Military. Ontologies can also be used to specify various diseases or financial entities. Once a community has developed ontologies, the community has to publish these ontologies on the web.

E. Layer 5: Logic:

There is no specific definition for the Logic layer in the semantic web, not only the Logic layer, but for Trust and Proof layers. There are attempts to reach to their full meaning, status and functions of these layers,

because Tim Berners Lee propositions and presentations did not describe these layers in details. The Logic layer is placed above the ontology layer. It is supposed that information will be extracted from the web according to this logic.

F. Layer 6: Proof:

Proof is the layer placed above the Logic layer. It is assumed to be a language used in a manner that describes for agents why they should believe the results. This will be a useful semantic web service.

G. Layer 7: Trust:

A lot of efforts have been exerted to reach the trusted web, but this is very complicated and difficult task and has not become a reality. Trust has many meanings in the semantic web. Trust is the final layer in the semantic web architecture. It depends on the source of information as well as the policies available on the information source which can prevent unwanted applications or user from access to these sources.

H. The vertical *layer*:

Digital signature: Digital Signature is the only vertical layer in the semantic web architecture. It begins from layer 3 and ends at layer 6. Digital Signature is a step towards a web of trust. By using of XML digital signature, any digital information can be signed [14]. There are specific elements in XML syntax used for this process such as Signed Info, Reference and Digest Value [15]. -based approaches and proof theories are being examined for enforcing trust on the semantic web. Note that the layers as evolving as progress is made on the semantic web.

VI. SECURITY IN SEMANTIC WEB

A. Semantic web security

As stated earlier, logic, proof and trust are at the highest layers of the semantic web. That is, how can we trust the information that the web gives us? Closely related to trust is security. However security cannot be considered in isolation. That is, there is no one layer that should focus on security. Security cuts across all layers and this is a challenge. That is, we need security for each of the layers and we must also ensure secure interoperability as illustrated in Table I.

TABLE I. SECURITY LAYERS FOR THE SEMANTIC WEB

Layer 5	Logic, Proof, Trust
Layer 4	Secure Ontologies
Layer 3	RDF Security
Layer 2	XML Security (Secure XML Schemas)
Layer 1	Secure TCP/IP, HTTPS, Secure Sockets

For example, consider the lowest layer. One needs secure TCP/IP, secure sockets, and secure HTTP. There are now security protocols for these various lower layer protocols. One needs end-to-end security. That is, one cannot just have secure TCP/IP built on untrusted communication layers [9]. That is, we need network security. Next layer is XML and XML schemas. One needs secure XML. That is, access must be controlled to various portions of the document for reading, browsing and modifications. There is research on securing XML and XML schemas. The next step is securing RDF. Now with RDF not only do we need secure XML, we also need security for the interpretations and semantics. For example under certain context, portions of the document may be Unclassified while under certain other context the document may be classified. As an example one could declassify an RDF document, once the war is over. Lot of work has been carried out on security constraints processing for relational databases. One needs to determine whether these results could be applied for the semantic web [16].

Once XML and RDF have been secured the next step is to examine security for ontologies and interoperation. That is, ontologies may have security levels attached to them. Certain parts of the ontologies could be Secret while certain other parts may be Unclassified. The challenge is how does one use these ontologies for secure information integration? Researchers have done some work on the secure interoperability of databases. We need to revisit this research and then determine what else needs to be done so that the information on the web can be managed, integrated and exchanged securely. Closely related to security is privacy. That is, certain portions of the document may be private while certain other portions may be public or semi-private. Privacy has received a lot of attention recently partly due to national security concerns. Privacy for the semantic web may be a critical issue, That is, how does one take advantage of the semantic web and still maintain privacy and sometimes anonymity. Note that W3C is actively examining privacy issues and a good starting point is P3P (Platform for Privacy Preferences) standards, P3P 1.0 Specification [17].

We also need to examine the inference problem for the semantic web. Inference is the process of posing queries and deducing new information. It becomes a problem when the deduced information is something the user is unauthorized to know. With the semantic web, and especially with data mining tools, one can make all kinds of inferences.

That is the semantic web exacerbates the inference problem [18]. Recently there has been some research on controlling unauthorized inferences on the semantic web. We need to continue with such research [1].

Security should not be an afterthought. We have often heard that one needs to insert security into the system right from the beginning. Similarly security cannot be an afterthought for the semantic web [19]. However, we cannot also make the system inefficient if we must guarantee one hundred percent security at all times. What is needed is a flexible security policy. During some situations we may need one hundred percent security while during some other situations say 30% security (whatever that means) may be sufficient.

1) Security in XML

Researchers they have focused on access control policies as well as on dissemination policies. They also considered push and pull architectures. They specified the policies in XML. The policy specification contains information about which users can access which portions of the documents. As in reference [19] is stated algorithms for access control as well as computing views of the results are also presented. In addition, architectures for securing XML documents are also discussed. Bertino et al. go further and describe how XML documents may be published on the web. The idea is for owners to publish documents, subjects to request access to the documents and untrusted publishers to give the subjects the views of the documents they are authorized to see. W3C (World Wide Web Consortium) is also specifying standards for XML security. The XML security project is focusing on providing the implementation of security standards for XML. The focus is on XML-Signature Syntax and Processing, XML-Encryption Syntax and Processing and XML Key Management. W3C also has a number of working groups including XML-Signature working group [20] and XML-Encryption working group [21]. While the standards are focusing on what can be implemented in the near term lot of research is needed on securing XML documents.

2) Security in RDF

RDF is the foundations of the semantic web. While XML is limited in providing machine understandable documents, RDF handles this limitation. As a result, RDF provides better support for interoperability as well as searching and cataloging. It also describes contents of documents as well as relationships between various entities in the document. While XML provides syntax and notations, RDF supplements this by providing semantic information in a standardized way.

The basic RDF model has three types: they are resources, properties and statements. Resource is anything described by RDF expressions. Property is a specific attribute used to describe a resource. RDF statements are resources together with a named property plus the value of the property. Statement components are subject, predicate and object. RDF- and XML-namespaces resolve conflicts in semantics. More advanced concepts in RDF include the container model and statements about statements. The container model has three types of container objects and they are Bag, Sequence, and Alternative. A bag is an unordered list of resources or literals. It is used to mean that a property has multiple values but the order is not important. A sequence is a list of ordered resources. Here, the order is important. Alternative is a list of resources that represent alternatives for the value of a property. Various tutorials in RDF describe the syntax of containers in more detail. RDF also provides support for making statements about other statements. Now to make the semantic web secure, we need to ensure that RDF documents are secure. This would involve securing XML from a syntactic point of view.

3) Standardization of semantic web security

Web resources and services need to be protected from unauthorized access and software agents want to be ensured about the privacy of data they disclose to services. Thus, a broad range of security-related notions, such as authentication, authorization, access control, confidentiality, data integrity, and privacy are relevant for semantic web technology. Currently, low-level encryption, digital signature mechanisms, certification, and public key infrastructures provide a good security infrastructure for web-based interactions.

4) Other viewpoint to semantic web Security

Trust is, usually, the last but not the least thing for people to concern when they build a system. So, why we worry about trust issue at this moment? Especially when the trust layer was declared as the top of layer on the semantic web layer cake. If we agree that proof and trust are applications rather than a new ontology language on the layer stack, then it will not hurt to explore the trust issues at current stage [10]. There are several important results on agent trust based on psychology and security viewpoints [22][23][24]. Trust and risk are complementary terms in social relations. An emphasis on risk is generally based on mistrust, whereas trust is associated with less doubts about security. Those who trust others do not look for high security before they act. Trust (or security) is also one of the important issues for web service and grid computing in the semantic web pyramid [25][26].

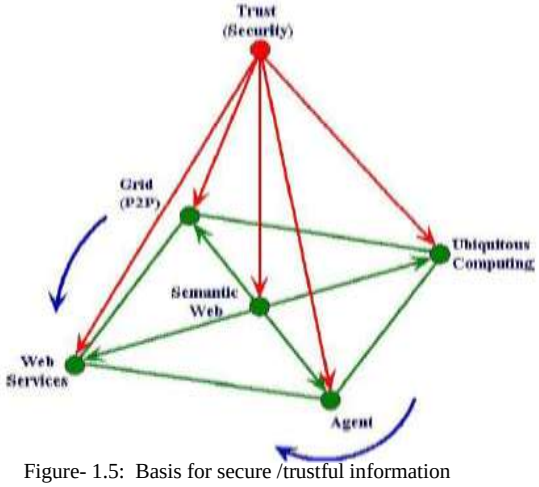

Figure- 1.5: Basis for secure /trustful information

When we compare with other emerging technologies, the research progress for the trusted semantic web is very slow and the results are scarce [27][28]. Trusted semantic web was defined as well-defined trust ontologies and trust rules in the agent interaction protocols so that agent's access control services, such as authentication, authorization, and delegation can be achieved. This approach not only solves the agent's authenticity and authority problems but also provides the possible capacity to resolve information propagation authenticity, ontology and rule integrity issues in the future. In the trust traversing path, d, b, c (Figure 1.5), the Ontology and rule techniques will be leveraged on agent trust control. In another trust traversing path, e, b, a, agent technology will be leveraged on the building and verifying of authenticity and integrity of ontology and rule.

VII. CONCLUSION

This paper has provided an overview of the semantic web and social or educational network system. Social networks are growing rapidly and users want to express their identities and share information in restricted virtual communities. The "way of communicating" has advanced from point-to-point message exchanges between isolated users to group-oriented activities. Social networking sites must recognize this basic aspect of human social interaction and find strong and intuitive methods for implementing it on a software level while providing the necessary level of protection, privacy and trust. Several hacking groups are attacking social networks, spreading key loggers, Trojans and other malicious tools. Governments and intelligence agencies will have to adopt new paradigms and technologies to use and manipulate the amount of information and interaction in a social Web.

We have discussed security standards and discussed the layered framework of the semantic web proposed by Tim Berners Lee. We discuss that security must cut across all the layers; we need to integrate the information across the layers securely.

We must start examining security for RDF. This is much more difficult as RDF incorporates semantics. We need to examine the work on security constraint processing and context dependent security constraints and see if we can apply some of the ideas for RDF-Security. Finally, we need to examine the role of ontologies for secure information integration. Standards play an important role in the development of the semantic web. W3C has been very effective in specifying standards for XML, RDF and the semantic web. The next step for the semantic web standards efforts is to examine security, privacy, quality of service, integrity, proof of information, trust and other features such as multimedia processing and query services.

Meeting this challenge requires realizing four high-level objectives: (1) to advance the theory and practice of security, privacy, and trust of web based interactions by providing technology for trust in the semantic web services; (2) to provide declarative policy representation languages, ontologies, and inference algorithms for security, trust and privacy management; and (3) to prototype software tools allowing system designers and end users to both specify and verify policies for trust and privacy.

REFERENCES

[1] T. Berners Lee, J. Hendler, O. Lassila, The semantic web, Scientific American; May 2001, 34 – 43.
[2] "What is Social Networking", http://www.whatissocialnetworking
[3] http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.
[4] Leveraging Social data with Semantics, http://www.w3.org/2008/09/ msnws/papers/ereteo_et_al_2008_leveraging.html.
[5] WikiPedia, http://en.wikipedia.org/wiki/Virtual_economy.
[6] Burleson, 2007. Introduction to the semantic web Vision and Technologies, http://www.semanticfocus.com/blog/entry/title/introduction-to-the- semantic-web-vision-andtechnologies-part-2-foundations.
[7] B. Matthews," semantic web Technologies. JISC Technology and Standards Watch," 2005.
[8] T. Berners Lee, 2006. Uniform Resource Identifiers, URI Generic Syntax. IETF. http://www.ietf.org/rfc/rfc2396.txt.
A. Medić, Criptography – Securing web Servers and web Applications, University of Bihać, Technical Faculty Bihać, engineer thesis, Bihać, Bosnia and Herzegovina, February 2008.
[9] Fensel, 2002. Layering the semantic web: Problems and Directions. In the Proceeding of 1st International semantic web Conference (ISWC, 2002). Sardinia, Italy, 9-12 June, pp: 476. ISBN: 3540437606, 9783540437604.
[10] S. St. Laurent, XML, McGraw Hill, New York, NY, 2000.
[11] S. Buraga and G. Ciobanu., 2002. A RDF- based model for expressing spatio-temporal relation between web sites. In The 3rd International Conference on Information Systems

Engineering. IEEE Computer Society. pp: 355. IEEE Computer Society Washington, DC, USA., ISBN:0-7695-1766-8.
[12] Description Framework", in D-Lib Magazine, May.1998; http://www.dlib.org/dlib/may98/miller/05miller.html.
[13] R. Cloran and B. Irwin, 2005. XML Digital Signature and RDF, http://icsa.cs.up.ac.za/issa/2005/Proceedings/Poster/026_Article.pdf
[14] T. Haytam, Al-Feel, M. Koutb and H. Suoror, semantic web on Scope: A New Architectural Model for the semantic web, Journal of Computer Science 4 (7): 613-624, 2008.
[15] B. Thuraisingham,W. Ford, Security constraint processing in a distributed database management system, IEEE Transactions on Knowledge and Data Engineering (1995) 274– 293.
[16] Ryan Naraine, "PlayStation Home virtual world hacked", ZDNET. Dec. 22, 2008. Available: http://blogs.zdnet.com/security/?p=2330.
[17] B. Thuraisingham, Data Mining: Technologies, Techniques, Tools and Trends, CRC Press, Boca Raton, FL, 1998.
[18] B. Thuraisingham, Secure Sematic web Services, Technical Report, University of Texas – Department of Computer Science, 2007.
[19] http://www.w3.org/Signature/.
[20] http://www.w3.org/Encryption/.
[21] Q. He, K. Sycara and T. Finin., Personal Security Agent: KQML-Based PKI. Proceedings of the Second International Conference on Autonomous Agents, (1998).
[22] Hu, Y.-J., Some Thoughts on Agent Trust and Delegation. The Fifth International Conference on Autonomous Agents, Montreal, Canada, May 28 - June 1, (2001), 489-496.
[23] H. C. Wong and K. Sycara, Adding Security and Trust to Multi-Agent Systems. Proceedings of Autonomous Agents '99 (Workshop on Deception, Fraud and Trust in Agent Societies), Seattle, Washington, (1999), 149-161.
[24] Security in a web Services World: A Proposed Architecture and Roadmap. A joint security white paper from IBM Corp. and Microsoft Corp., Version 1.0, April 7 2002. http://www-106.ibm.com/developworks/library/ws-secmap.
[25] N. Nagaratnam et al., The Security Architecture for Open Grid Services. Ver. 1, July 17 2002, http://www.globus.org/ogsa/Security/
[26] G. Jennifer, J. Hendler, and B. Parsia, Trust Networks on the semantic web. World Wide web Conference, Budapest, Hungary, May 20-26 2003.
[27] Y. Gil and V. Ratnakar, Trusting Information Sources One Citizen at a Time. The semantic web - ISWC 2002, (2002), 162-176.