**IOSR Journal of Engineering (IOSRJEN)** **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 4 (April. 2019), ||S (I) || PP 10-17

# A Prototype Description Relates to Security Mechanisms on Web Semantic data

Naseema Shaik[1], Dr. E. Sreenivasa Reddy[2]
[1]*Research Scholar, Acharya Nagarjuna University, Guntur, AP, India.*
[2]*Dean, Faculty of Engineering, Acharya Nagarjuna University, Guntur, AP, India.*
*Corresponding Author: Naseema Shaik*

**Abstract:** Interaction between computers and humans in Web Semantic data, describes high security definitions to explore data from web server and enable automatic sophisticated privacy in Web Semantic data analysis. Once any two persons communicate with each other then automatically data to be does and hold by others present in web. Web Semantic data shares overall data into different users present in throughout the world then main challenge behind web data sharing gives possible communications whether it is possible or not possible based on users with server communication. So that security is the main factor to provide efficient privacy to data on web. There are different types of security approaches/methods were introduced conventionally. In this paper, we give brief description about security mechanism used for web data, discuss about hash based security procedures and also describe major contributions relates to digital artifact concept on web for security to data with hash based mechanisms. We also discuss comparative analysis of different security mechanism used for web data. Also discuss about innovation of digital artifact making on web.

**Index Terms:** Digital Artifact, Web Semantic data, Trusty URI, RDF, and Web of trust, Security, privacy and Digital Technology**.**

---

Date of Submission: 26-03-2019 Date of acceptance: 09-04-2019

---

## I. INTRODUCTION

Data provide in the current Web is for the most part human arranged. For instance, HTML script are not accessible to reasonable however a personal computer can't comprehend the substance and concentrate the privilege ideas spoke to there, the importance of the information. The Web Semantic Data [1] is a circulated situation is defined by methods for all around characterized semantics, that is, machine justifiable, in this manner giving web based business and computerization (e.g., in inquiry). In such a domain, substances which are not cooperation may now have the capacity to consequently collaborate with one another. For instance, envision an operator arranging a trek for a client. It's describes to define clients time table which are need to define. At the point when the client's specialist contacts lodging's site, the last needs to advise the previous which require the end goal to affirm a reservation. Be that as it may, the client may presumably need to limit the conditions under which her operator naturally uncovers client individual data. Because of such trade of conditions and individual data, and additionally its computerization, security and protection turn out to be yet more important and conventional methodologies are not appropriate any longer. From one viewpoint, one-sided get to control is presently supplanted by reciprocal insurance. Then again, character based access control can't be connected any longer since clients are not known ahead of time. Rather, elements' properties assume a focal job. Different properties and conditions are expressed based on satisfied with third party which is reasonable for well defined semantics relations to process different elements. Improve the procedures relates to security approaches to control different data relevant assets and assess to dependable properties described in [2]. Disseminating to control main portion of lacked issues organized by the web scripts. Role based access control (RBAC) doesn't meet Web Semantic data descriptions for selected client jobs which are not associated with time efficiency. For efficient client security instance, Privacy for Platform Preferences (P3) gives vocabulary to portable web server security strategies. In any case, it is not sufficient to expressive and it is not take account implementation instruments with update described in [3][4][5][6][7]. Security based approaches defines expressive, effort and versatility and analyzability. These approaches can be substances on security related Web Semantic data utilized with around estimated semantic relations. The approach dialects recorded above vary in expressivity, sort of thinking required; highlights and usage gave, and so etc. So that in this paper, introduce basic security approaches used to provide privacy for web data with suitable parameters, and also discuss about discriminative analysis of different hash based mechanism used to provide security for web related data.

## II. REVIEW OF RELATED WORK

In this section, describe past research relates to Web Semantic data security, properties of Web Semantic data security itself which are used to describe research on privacy of Web Semantic data security foundation. Web Semantic data security approach defects access control with ontology based cyber security and issues with privacy in web based semantic information.

### 2.1. Access Control based Web Semantic data

Main research with respect to access control done in Web Semantic data security, for example Rei [20] describe the relations of utilization in [4] with respect to World Wide Web for web access control (WAC). These methodologies display consents and commitments between operators worked for information usage on Web Semantic data [10], with the objective to keep up some security approach amid a conveyed movement, for example, Web Semantic data Service structure. Practically speaking these methodologies are for the most part helpful for inter-operation between different access control arrangements. Approach dialects are ordinarily utilized with obligatory access control (perhaps reached quality with respect to access control), which depends on a focal confided in gathering, for example, an OS to really implement the entrance control [15], and such a brought together believed gathering is absent on Web Semantic data from on the dimension of personal visit of web. The essential advancement in using web semantic information for approach dialects is circulated get to access control policies. As opposed to arrangement dialects, a significant part of whatever is left of the Web relies upon an abilities based methodology by given authorized security web [14]. Research described on arrangement dialects have been wellspring advancement however is symmetrical to privacy problems of web semantic information itself, whereupon these strategy dialects depends on user derivation.

### 2.2. Cyber-security Ontologies Descriptions

Another implementation methodology describes which describes privacy related vulnerabilities into semantic ontology web script relations in [24]. Albeit defined joined with provenance based Web Semantic data information based on security goals, for example, Division home and get data about digital artifact attacks. This methodology describes about privacy issues using ontologies inside an antagonistic situation

### 2.3. Open Data Security Relations

Distributing open information utilizing Web Semantic data norms may have all the earmarks of being an open decent, even harmless open information, for example, street information may serve to deanonymize clients thus uncover individual or delicate information, running from regardless of whether a property is deserted to empowering the disclosure of sexual inclination [10]. With the end goal to keep these issues, the distribution and inquiry of scrambled RDF information has been proposed [11], and differential protection [16], however so far neither have been actualized. In spite of the fact that which can be expanded to support by Lee-Burners for the utilization of Web Semantic data models to "decentralize the Web" and give individual information [2], the specific same utilization of the Web Semantic data for information combination can be utilized by outsiders with the end goal to manufacture FBI Fusion Centers in the USA.

### 2.4. Web Semantic data Security

Albeit past research described on abnormal state "anchoring RDF is substantially more difficult" than customary extensible markup and hyper text markup based models as "we additionally need to guarantee that security is saved at the semantic dimension", so examination toward this path that go past the negligible "thought of Web Semantic data security institutionalization" [13]. Big government business clients just trust which is best to "get to privacy for access control happens and conventions on HTTP security relations, and not at the connected information layer.

## III. PRIVACY ISSUES IN WEB SEMANTIC DATA

In this section, describe various privacy and security issues which can be relevant to XML related privacy and discuss about RDF privacy for information on web semantic data.

### 3.1. Security Issues Overview

As communicated previously, method of reasoning, check and trust are at the most shocking layers of the Web Semantic information. That is, by what means may we trust in the information that the web gives us? Immovably related to trust is security. At any rate security can't be considered in control. That is, there is no one layer that should focus on security. Security cuts over all layers and this is a test. For example, consider the most insignificant layer. One needs secure TCP/IP, secure connections, and secure HTTP. There are at present security traditions for these distinctive lower layer traditions. One needs start to finish security. That is, one can't just have secure TCP/IP dependent on un-believed correspondence layers. That is, we require sort out security.

Next layer is XML and XML mappings. One needs secure XML. That is, get to must be controlled to various bits of the file for examining, scrutinizing and adjustments. There is ask about on securing XML and XML designs. The resulting stage is securing Resource Description Framework RDF. Directly with RDF notwithstanding the way that we require secure XML, we moreover require security for the understandings and semantics. For example under certain one of a kind circumstance, parts of the file may be Unclassified while under certain other setting the report might be characterized. For example one could declassify a RDF record, when the war is done. Some portion of work has been finished security prerequisites getting ready for social databases. One needs to choose if these results could be associated for the Web Semantic information (see [THUR95]). Whenever XML and RDF have been tied down the accompanying stage is to take a gander at security for ontologies and interoperation. That is, ontologies may have security levels joined to them. Certa in parts of the ontologies could be Secret while certain distinctive parts may be Unclassified. The test is the way by which does one use these ontologies for secure information coordination? Investigators have done some work on the protected interoperability of databases. We need to come back to this examination and subsequently make sense of what else ought to be done in that capacity that the information on the web can be administered composed and exchanged securely. Solidly related to security is assurance. That is, certain bits of the report may be private while certain diverse portions may be open or semiprivate.

Assurance has gotten a significant proportion of thought starting late for the most part in light of national security concerns. Insurance for the Web Semantic information may be an essential issue, That is, how might one adventure the Web Semantic information and still keep up security and every so often lack of definition. We moreover need to dissect the derivation issue for the Web Semantic information. Finding is the path toward showing request and inferring new information. It transforms into an issue when the determined information is something the customer is unapproved to know. With the Web Semantic information, and especially with data mining instruments, one can make a wide scope of findings. That is the Web Semantic information intensifies the deduction issue (see [THUR98]). Starting late there has been some examination on controlling unapproved deducing on the Web Semantic information. We need to continue with such research (see for example, [FARK03]). Security should not be a less than ideal thought. We have frequently heard that one needs to embed security into the framework ideal from the earliest starting point. Thus security can't be reconsideration for the Web Semantic data. Nonetheless, we can't likewise make the framework wasteful on the off chance that we should promise 100% security consistently. What is required is an adaptable security arrangement. Amid a few circumstances we may require 100% security while amid some different circumstances say 30% security (whatever that implies) might be sufficient.

### 3.2. Security relevant to XML

There is different security related approaches has been introduced for XML related privacy issues (see for instance, [BERT02]). We quickly talk about a portion of the key focuses. XML records have diagram structures. Main principle is to control access control with respect to XML reports which are relevant to security in basic related reports. Bertino et al describe innovative models relates to security approaches for XML related privacy. Different approaches predict XML relevant security relations with respect to clients organized by semantic web data. Benefits incorporate read, compose, attach, appropriate, and peruse. For instance, if a client approaches the base of a report at that point should his entrance, say read, and proliferate to every one of the relatives or the quick kids? In [BERT02] calculations for access control and also processing perspectives of the outcomes are likewise exhibited. Furthermore, designs for anchoring XML reports are likewise talked about.
In [BERT03] the makers go further and illustrate how XML information might be allocated on the web. The idea is for owners to spread information, topics to ask for accessibility to information and distributers to provide the topics the viewpoints of the reviews they are accepted to see. The idea is for the distributers to be untrusted. This is the owner indicates the entry control techniques. The distributer will then maintain the entry control preparations. Protection computations and furthermore Merkel hash can be used to ensure that the distributer is untrusted. Bertino et al provide the authenticity and end result of the results prepared by the distributer and sent to the topic.

W3C (World Wide Web Consortium) is too identifying standards for XML security. The XML security project (see [XML1]) is focusing on providing the performance of security standards for XML. The attention is on XML-Signature Format what are more, planning, XML-Encryption Format and Preparing and XML Key Management. W3C furthermore has various operating events such as XML Trademark operating collecting (see [XML2]) and XML encryption operating collecting (see [XML3]). While the indicators are focusing on what can be implemented in the close phrase part of research is required on anchoring XML information. The work specific in [BERT02] is a good begins.

### 3.3. Security based RDF

RDF is the businesses of the Web Semantic information. While XML is restricted in providing machine sensible information, RDF manages this confinement. Consequently, RDF gives better help for interoperability and therefore looking for and identifying. It shows material of information and therefore relationships between different components in the review. While XML gives syntax and information, RDF products this by offering semantic information consistent. The fundamental RDF display has three sorts: they are resources, qualities and details. Resource is anything represented by RDF articulations. It could be a page or a set of pages. Rentals are a particular credit used to illustrate a resource. RDF claims are resources together with a known as residence along with the evaluation of the exact residence. Connection sections are topic, predicate and demonstration. So for example, on the off chance that we have a phrase of the shape "John is the manufacturer of xxx", at that point xxx is the topic or asset, Property or predicate is "Maker" and demonstration or tight is "John". There are RDF maps especially like say ER maps or demonstration describes to talk to claims. Vhere are different viewpoints particular to RDF language framework. Iis vital that the organized knowing be used for RDF phrases. This is efficient by RDF blueprints. Structure is kind of a vocabulary and has translations of different terms found in phrases. RDF and XML namespaces to determine situations in semantics.

Further developed ideas in RDF integrate the section design and details about claims. The section display has three kinds of owner articles and they are Bag, Series, and Alternative. A bag is an unordered explanation of resources or literals. It is used to suggest that your home has different features yet the demand isn't important. A grouping is a rundown of requested assets. Here the request is vital. Elective is a rundown of assets that speak to choices for the estimation of a property. Different instructional exercises in RDF depict the language structure of compartments in more subtle elements.

## IV. TAXONOMY OF NANO PUBLICATION

Present days, because of increasing communication system, it is very difficult for specific scientific related statements to be identified and connected to text i.e nano-publications. We describe basic model relates to nanopublication associated with Graph/RDF serialization with text. the Web Semantic data is giving the stage in which individuals can all the more effectively create explanations, extricate proclamations from existing writing and offer them in a way that will permit computational specialists to find, total and translate these proclamations. The upsides of this are clear, and in a perfect world, the ideas in an announcement and the announcement itself will have a few one of a kind character that interfaces each case of an announcement over the snare of (formally and additionally casually) distributed material. It tends normal that the quantity of frameworks that encourage the making of articulations will increment. These will come in the shape of the two procedures intended to create articulations from existing material, and frameworks that encourage all over again articulation creation. More current guidelines like RDF's likewise encourage this and coordinate with current html docs with titles, statements and others presented in figure 1.

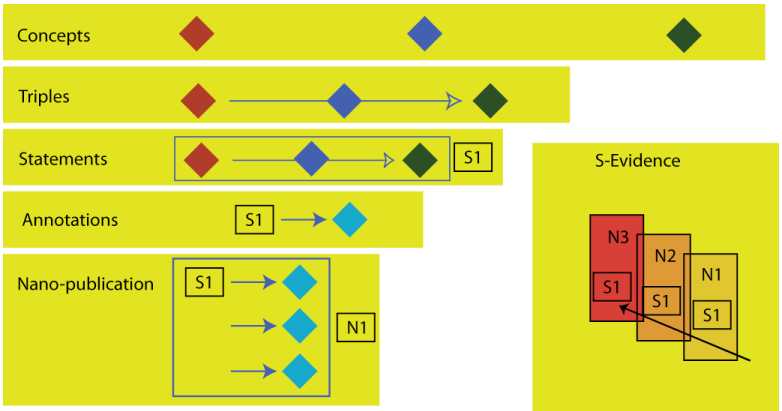


**Figure 1. System description with nano-publication model.**

The test currently progresses toward becoming; what should be done to put the setting back in to an explanation that was in the past given by a archive. In this paper we investigate the additional segments that would should be accessible to fortify the estimation of an announcement to the point where it could in itself be viewed as a distribution. This is named a nano-distribution. We separate out objectives from executions and think about the materialness of current models to necessities. Nano publications are associated with text on web using Annotation concept, structure relates to nanopublication on web shown in figure 2 designed by SWAN ontology.

```
@prefix swan: <http://swan.mindinformatics.org/ontologies/1.2/pav.owl> .
@prefix cw:   <http://conceptwiki.org/index.php/Concept>.
@prefix swp:  <http://www.w3.org/2004/03/trix/swp-1/>.
@prefix : <http://www.example.org/thisDocument#> .

:G1  = { cw:malaria cw:isTransmittedBy cw:mosquitoes }

:G2  = { :G1 swan:importedBy cw:TextExtractor,
         :G1 swan:createdOn "2009-09-03"^^xsd:date,
         :G1 swan:authoredBy cw:BobSmith }

:G3  = { :G2 ann:assertedBy cw:SomeOrganization }
```

**Figure 2. Sample representation of nano-publication.**

Comments give an instrument to portray data about a proclamation. For instance, who created the announcement, when was the announcement made, what programming was utilized in making the articulation et cetera. Be that as it may, in various cases it helpful to be ready to talk about a nano-distribution all in all, for instance, to guarantee attribution on it, enable a commentator to endorse it, or to give an approach to individuals to vote in favor of or refer to a nano-distribution. Here, we utilize attribution for instance. While the provenance cosmology from SWAN gives a sensible arrangement of data portraying the comments inside a nano-distribution. It doesn't yet give a decent instrument to asserting the substance of a nano-distribution. To help this, we propose to utilize the Web Semantic data Publishing ontology. This cosmology gives as asserted. By relationship, this relates a specific NamedGraph to a substance (i.e. an expert). In this way, a substance can express that they stated a nano-publication what's more, in this way guarantee. Besides, this cosmology gives the capacity to express computerized marks on every one of the diagrams. This mark capacity might be critical in confirming cases. There might be in excess of one nano-production about the equivalent proclamation. Through this affirmed by system, it winds up simpler to recognize the starting points of these distinctive records of the equivalent explanation. In reality, clients (programming or human operators) of a nano-publication may choose which accounts they trust and which they try not to dependent on any number of heuristics. This thought of various perspectives or records of a similar articulation is enlivened by the Open Provenance Model [7]. We trust that attribution is a basic part to nano-publications; in any case, the network may choose that other metadata on nano-productions might be fundamental, for instance audits or institutional affiliation. Different utilizations might be to empower the development of accumulations of nano-publications. Nano-publications are associated with digital artifacts for security to web text data.

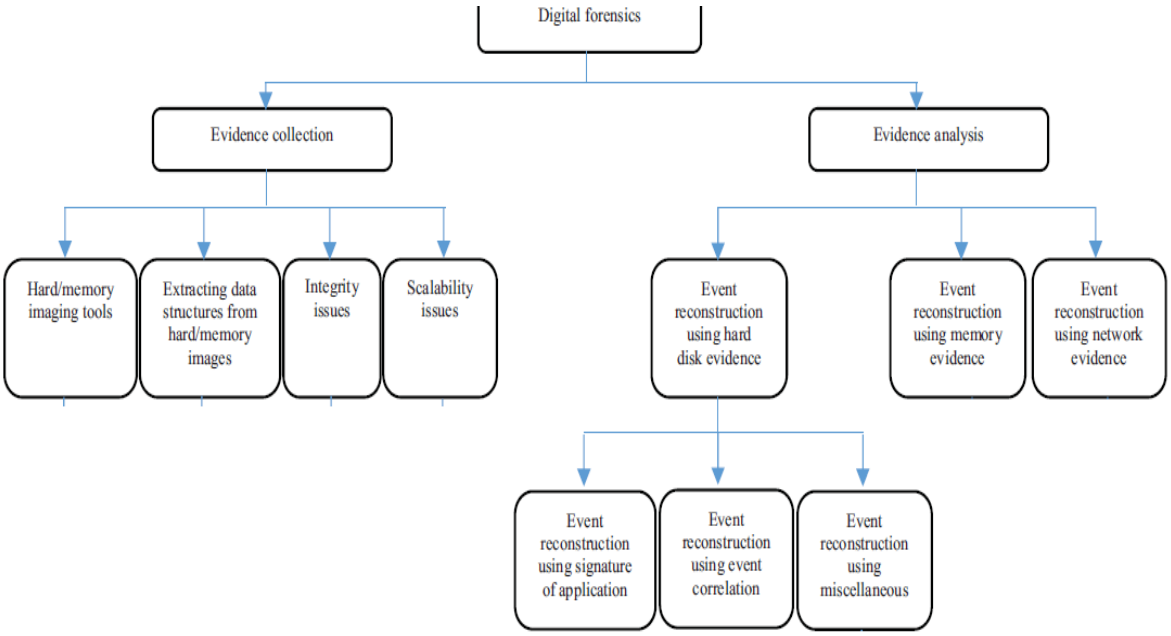


**Figure 3. Different types of digitized approaches used for security on web.**

## V. DIGITAL ARTIFACTS

The vision of the Web Semantic data is to make the substance of the web machine- interpretable, permitting, in addition to other things, for robotized collection thus sophisticated look methodology over a lot of connected information. As even human clients are some of the time simple to trap by spam and deceitful substance that can be found on the web, we ought to be considerably more worried on account of automated calculations that self-sufficiently break down Web Semantic data content. Without suitable counter-measures, noxious on-screen characters can damage or control such calculations by including only a couple of deliberately controlled things to huge arrangements of input information. To take care of this issue, we propose a way to deal with make things on the (semantic) web verifiable, unchanging, and perpetual. This methodology incorporates cryptographic hash esteems in Uniform Resource Identifiers (URIs) and holds fast to the center standards of the web, to be specific transparency and decentralized design. Different types of digital artifact techniques used for security in web shown in figure 3.

A cryptographic hash esteem (here and there called cryptographic process) is a short irregular looking arrangement of bytes (or, proportionately, bits) that are computed in a muddled yet superbly unsurprising way from a computerized relic, for example, a le. Similar information dependably prompts the very same hash esteem, though only a negligibly modified input prompts a totally different esteem. While there is an infinity of conceivable data sources that prompt a specific given hash esteem, it is unthinkable by and by (for solid best in class hash calculations) to remake any of the conceivable data sources just from the hash esteem. This implies on the off chance that you are given some information and coordinating hash esteem, you can make sure that the hash esteem was gotten from precisely that input. On this premise, this paper comes down to the possibility that references can be made totally unambiguous furthermore, verifiable on the off chance that they contain a hash estimation of the referenced computerized relic. Our technique does not make a difference to all URIs, obviously, but rather just to those that are implied to speak to a specific and immutable digital artifact.

## VI. SCOPE OF THE RESEARCH

The current Web has no broad instruments to make computerized relics —, for example, datasets, code, messages, and pictures — unquestionable and changeless. For computerized relics that should be unchanging, there is additionally no ordinarily acknowledged strategy to uphold this unchanging nature. To take care of this issue, we propose trusty URIs containing cryptographic hash esteems. We indicate how trusty URIs can be utilized for the check of advanced antiques, in a way that is autonomous of the serialization arrange on account of organized information documents, for example, nano-publications. We illustrate how the substance of these records wind up changeless, including conditions to outside advanced curios and subsequently broadening the range of undeniable nature to the whole reference tree. Our methodology adheres profoundly standards of the Web, to be specific transparency and decentralized design, and is completely perfect with existing benchmarks and conventions.

## VII. CONCLUSION

In this paper, we discuss about Web Semantic data security mechanisms relates to communication between different users in outside web environment. We also discuss about review of related literature relates to explore web data context for different applications. Privacy issues appeared in web data security also described in this document. How web data associate with nano-publications using annotations like HTML, hash codes and other privacy mechanisms. Introduce Digital artifact concept for security in web. Further improvement of our research is to continue create digital artifact on Web Semantic data verifiable, immutable and permanent. We have begun to build up a decentralized nanopublication server arrange [26]. Nano-publications are circulated and recreated among such servers and recognized by trusty URIs, in this manner guaranteeing that these curios stay accessible regardless of whether singular servers are ended. The current organize comprises of four servers in four unique nations facilitating 5 million nano-publications. Also, we are chipping away at the idea of nanopublication files that take into consideration the definition and recognizable proof of little or huge arrangements of nano-publications. Such files are nano-publications themselves and, obviously, are distinguished by trusty URIs.

## REFERENCES

[1]. Harry Halpin, “Semantic Insecurity: Security and the Web Semantic data”, In 2014 IEEE Symposium on Security and Privacy, pages 98–113. IEEE, 2017.

[2]. Hadi Asghari, Michel Van Eeten, Axel Arnbak, and Nico Van Eijk. Security economics in the HTTPS value chain. In Twelfth Workshop on the Economics of Information Security (WEIS 2013), Washington, DC, 2013.

[3]. Vijay Bharadwaj, Hubert Le Van Gong, Dirk Balfanz, Alexei Czeskis, Arnar Birgisson, Jeff Hodges, Michael Jones, Rolf Lindemann, and J.C. Jones. Web Authentication: An API for accessing scoped credentials, 2016.
[4]. Karthikeyan Bhargavan, Antoine Delignat Lavaud, C´edric Fournet, Alfredo Pironti, and Pierre Yves Strub. Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS. In 2014 IEEE Symposium on Security and Privacy, pages 98–113. IEEE, 2014.
[5]. David Corsar, Peter Edwards, and John Nelson. Personal privacy and the web of linked data. In Proceedings of the 2013th International Conference on Society, Privacy and the Web Semantic data-Policy and Technology, pages 11–21, 2013.
[6]. Richard Cyganiak, David Wood, and Markus Lanthaler. RDF 1.1 concepts and abstract syntax, 2014. https://www.w3.org/TR/rdf11-concepts/.
[7]. Benjamin Heitmann, Felix Hermsen, and Stefan Decker. Towards the use of graph summaries for privacy enhancing release and querying of linked data. In Workshop on Society, Privacy and the Web Semantic data - Policy and Technology, 2016
[8]. Marios Isaakidis, Harry Halpin, and George Danezis. Unlimitid: Privacy-preserving federated identity management using algebraic macs. In Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society, pages 139–142. ACM, 2016.
[9]. Andreas Kasten, Ansgar Scherp, Frederik Armknecht, and Matthias Krause. Towards search on encrypted graph data. In Proceedings of the Workshop on Society, Privacy and the Web Semantic data-Policy and Technology, pages 46–57, 2013.
[10]. Essam Mansour, Andrei Vlad Sambra, Sandro Hawke, Maged Zereba, Sarven Capadisli, Abdurrahman Ghanem, Ashraf Aboulnaga, and Tim Berners-Lee. A demonstration of the solid platform for social web applications. In Proceedings of the 25th International Conference Companion on World Wide Web, pages 223–226. International World Wide Web Conferences Steering Committee, 2016.
[11]. Alessandro Oltramari, Lorrie Faith Cranor, Robert J Walls, and Patrick Drew McDaniel. Building an ontology of cyber security. In STIDS, pages 54–61. Citeseer, 2014.
[12]. Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel. Securing brokerless publish/subscribe systems using identity-based encryption. IEEE transactions on parallel and distributed systems, 25(2):518–528, 2014.
[13]. Lalana Kagal1 , Massimo Paolucci2 , Naveen Srinivasan, "Authorization and Privacy for Web Semantic data Services", Second Int. Web Semantic data Conference, Sanibel Island FL, October 2003.
[14]. Lalana Kagal, Tim Finin, and Anupam Joshi," A Policy Based Approach to Security for the Web Semantic data", D. Fensel et al. (Eds.): ISWC 2003, LNCS 2870, pp. 402–418, 2003.
[15]. Lalana Kagal. A Policy-Based Approach to Governing Autonomous Behaviour in Distributed Environments. PhD thesis, University of Maryland Baltimore County, 2004.
[16]. P. Bonatti and P. Samarati. Regulating Service Access and Information Release on the Web. In Conference on Computer and Communications Security (CCS'00), Athens, November 2000.
[17]. N. Li and J.C. Mitchell. RT: A Role-based Trust-management Framework. In DARPA Information Survivability Conference and Exposition (DISCEX),Washington, D.C., April 2003.
[18]. Jim Trevor and Dan Suciu. Dynamically distributed query evaluation. In Proceedings of the twentieth ACM SIGMOD-SIGACTSIGART Symposium on Principles of Database Systems, Santa Barbara, CA, USA, May 2001.
[19]. 25. Miguel Alves, Carlos Viegas Dam´asio, Daniel Olmedilla, and Wolfgang Nejdl. A distributed tabling algorithm for rule based policy systems. In 7th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2006), London, Ontario, Canada, June 2006. IEEE Computer Society.
[20]. Pranam Kolari, Li Ding, Shashidhara Ganjugunte, Anupam Joshi, Timothy W. Finin, and Lalana Kagal. Enhancing web privacy protection through declarative policies. In 6th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2005), pages 57–66, Stockholm, Sweden, jun 2005. IEEE Computer Society.
[21]. [21]. Steffen Staab, Bharat K. Bhargava, Leszek Lilien, Arnon Rosenthal, Marianne Winslett, Morris Sloman, Tharam S. Dillon, Elizabeth Chang, Farookh Khadeer Hussain, Wolfgang Nejdl, Daniel Olmedilla, and Vipul Kashyap. The pudding of trust. IEEE Intelligent Systems, 19(5):74–88, 2004.
[22]. Grit Denker, Lalana Kagal, Timothy W. Finin, Massimo Paolucci, and Katia P. Sycara. Security for daml web services: Annotation and matchmaking. In The Web Semantic data - ISWC 2003, Second International Web Semantic data Conference, Sanibel Island, FL, USA, October 20-23, 2003, Proceedings, Lecture Notes in Computer Science, pages 335–350. Springer, 2003.
[23]. Daniel Olmedilla, Rub´en Lara, Axel Polleres, and Holger Lausen. Trust negotiation for Web Semantic data services. In 1st International Workshop on Web Semantic data Services and Web Process

Composition (SWSWPC), volume 3387 of Lecture Notes in Computer Science, pages 81–95, San Diego, CA, USA, jul 2004. Springer.
[24]. Grid Security Infrastructure. http://www.globus.org/security/overview.html .
[25]. Andrzej Uszok, Jeffrey M. Bradshaw, and Renia Jeffers. Kaos: A policy and domain services framework for grid computing and Web Semantic data services. In Trust Management, Second International Conference, iTrust 2004, Oxford, UK, March 29 - April 1, 2004, Proceedings, Lecture Notes in Computer Science, pages 16–26. Springer, 2004.
[26]. Ionut Constandache, Daniel Olmedilla, and Wolfgang Nejdl. Policy based dynamic negotiation for grid services authorization. In Web Semantic data Policy Workshop in conjunction with 4th International Web Semantic data Conference, Galway, Ireland, November 2005.
[27]. P.A. Bonatti, C. Duma, N. Fuchs, W. Nejdl, D. Olmedilla, J. Peer, and N. Shahmehri. Web Semantic data policies - A discussion of requirements and research issues. In 3rd European Web Semantic data Conference (ESWC), Lecture Notes in Computer Science, Budva, Montenegro, jun 2006.
[28]. T. Kuhn and M. Dumontier, "Making Digital Artifacts on the Web Verifiable and Reliable," *IEEE transactionon knowledge and data engineering* Vol no 99 year2015.
[29]. O. S. Collaboration et al., "An open, large-scale, collaborative effort to estimate the reproducibility of
[30]. psychological science, "*Perspectives on PsychologicalScience, vol*. 7, no. 6, pp. 657–660, 2012.
[31]. T. Kuhn, C. Chichester, M.Dumontier, and M.Krauthammer,"Publishing without publishers: a decentralized approach to dissemination, retrieval, and archiving of data," *arXiv preprint arXiv*:1411.2749, 2014.
[32]. S. Farrell, D. Kutscher, C. Dannewitz, B. Ohlman, A. Keranen, and P. Hallam- Baker, "Naming things with hashes," Internet Engineering Task Force (IETF), Standards Track RFC 6920, April 2013.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Naseema Shaik. "A Prototype Description Relates to Security Mechanisms on Web Semantic data." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 04, 2019, pp. 10-17.