International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-141 PAGE NO: 836-842

Novel Decentralized systems for data publishing by trusty URI links

N.RAMYA[1],Shyamal Telkar[2] & Dr.K.Ramakrishna[3]

[1]M-Tech Dept. of IT Sridevi Women's Engineering College Hyderabad

[2]Assistant Professor, Dept. of IT Sridevi Women's Engineering College Hyderabad

[3]Professor & HOD, Dept. of IT Sridevi Women's Engineering College Hyderabad

***Abstract*—** To make digital artifacts (undesired or unintended alteration in data introduced in a digital process by an involved technique and/or technology) such as datasets, code, texts, and images verifiable and permanent. Digital artifacts that are supposedto be immutable, there is moreover no commonly accepted method to enforce this immutability. To solve this problem, we proposetrusty URIs containing base 64 encryption values.Base64 encoding can be helpful when fairly lengthy identifying information isused in an HTTP environment. For example, a database persistence framework might use Base64 encoding to encode a relativelylarge unique id (generally 128-bit UUIDs) into a string for use as an HTTP parameter in HTTP forms or HTTP GET URLs. Itmakes the contents of the data trustworthy which is sent as a URI to the user and it make sure whether it is trusted or not We showhow trusty URIs can be used for the verification of digital artifacts, in a manner that is independent of the serialization format inthe case of structured data files such as nanopublications .Our goal is to achieve a data security and make the content present isimmutable thereby extending the range of verifiability to the entire reference tree. Even the file with large content it becomespossible to implement in enhancing data's on the web and it is fully compatible with existing standards and protocols.

Keywords: Decentralized systems, data publishing, Semantic Web, linked data, resource description framework, nanopublications.

1. Introduction

In many areas and in particular in science,reproducibility is important. Verifiable, immutable, andpermanent digital artifacts are an important ingredient formaking the results of automated processes reproducible, butthe current Web offers no commonly accepted methods toensure these properties. Endeavors such as the Semantic Webto publish complex knowledge in a

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-141 PAGE NO: 836-842

machine-interpretablemanner aggravate this problem, as automated algorithmsoperating on large amounts of data can be expected to beeven more vulnerable than humans to manipulated orcorrupted content. Without appropriate counter-measures,malicious actors can sabotage or trick such algorithms byadding just a few carefully manipulated items to large sets ofinput data. To solve this problem, we propose an approach tomake items on the (Semantic) Web verifiable, immutable,and permanent. This approach includes cryptographic hashvalues in Uniform Resource Identifiers (URIs) and adheres tothe core principles of the Web, namely openness anddecentralized architecture. It directly follows that trusty URIartifacts are immutable, as any change in the content alsochanges its URI, thereby making it a new artifact. Again, youcan of course change your artifact and its URI and claim thatit has always been like this. You can get away with that if thetrusty URI has not yet been picked up by third parties, i.e.linked by other resources. Once this is the case, it cannot bechanged anymore, because all these links will still point tothe old trusty URI and everybody will notice that the newartifact is a different one.

Third, trusty URI artifacts are permanent if weassume that there are search engines and Web archivescrawling the artifacts on the Web and caching them. Inthis situation, any artifact that is available on the Webfor a sufficiently long time will remain available forever.If an artifact is no longer available in its original location(e.g. the one its URI resolves to), one can still retrieve itfrom the cache of search engines, Web archives, ordedicated replication services. The trusty URI guaranteesthat it is the artifact you are looking for, even if thelocation of the cached artifact is not trustworthy or it wascached from an untrustworthy source.

2. Related Work

2.1 EXISTING SYSTEM

In many areas and in particular in science, reproducibility is important. Verifiable, immutable, and permanent digital artifacts is an important ingredient for making the results of automated processes reproducible, but the current Web offers no commonly accepted methods to ensure these properties. Endeavors such as the Semantic Web to publish complex knowledge in a machine-interpretable manner aggravate this problem, as automated algorithms operating on large amounts

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-141 PAGE NO: 836-842

of data can be expected to be even more vulnerable than humans to manipulated or corrupted content. Without appropriate counter-measures, malicious actors can sabotage or trick such algorithms by adding just a few carefully manipulated items to large sets of inputdata.

Disadvantages of Existing System:

- Web content corrupted by human beings.
- In existing, no methods to make web content immutable.

2.2 PROPOSED SYSTEM

We propose an approach to make items on the (Semantic) Web verifiable, immutable, and permanent. This approach includes cryptographic hash values in Uniform Resource Identifiers (URIs) to the core principles of the Web, namely openness and decentralized architecture. Our proposed approach boils down to the idea that references can be made completely unambiguous and verifiable if they contain a hash value of the referenceddigital artifact. Our method does not apply to all URIs, of course, but only to those that are meant to represent a specific and immutable digital artifact.

Advantages of Proposed System:

- We can make content on verifiable, immutable and permanent.

This approach includes cryptographic hash valuesin the Web URI's, especially acceptance anddecentralized architecture. Our proposed approachboils down to the idea that references can beverified if it contains a hash value of the referencedDigital artifact.

This method does not apply for every URIs, ofcourse, but only to those which is to show aspecific and immutable digital artifact.We also propose trusty URI’s for the web artifactsto be reliable and more secure.

2.3 **ALGORITHM**

Base64 encoding is used to identify the informationin an HTTP environment. For instance, a databasepersistence framework might use Base64 encodingto encode a relatively lengthy unique id into astring for use as an HTTP parameter in HTTPforms or HTTP GET URLs. Also, manyapplications need to encode binary data in a waythat is convenient to be included in URLs or hiddenweb form fields, and Base64 is a convenientencoding to render them in a compact way.Thealgorithm which is used in this module is convertsthe ASCII value to base64 String which givessecurity to the data that is to be sent as a reliabledata. This prevents from unauthorized decoding ofdata.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-141 PAGE NO: 836-842

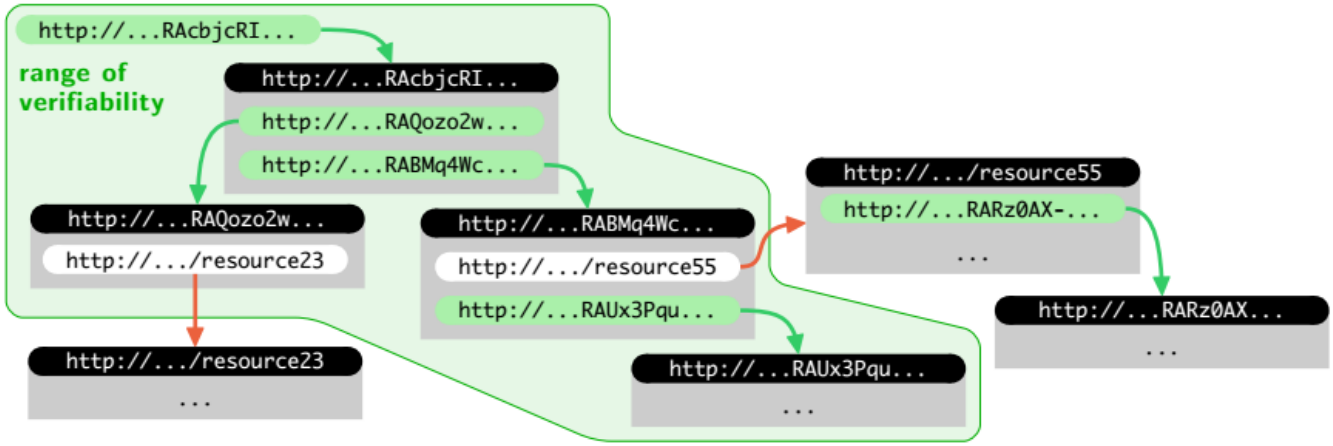

Fig1. Schematic illustration of the range of verifiability for the trusty URI on the top left. The green area shows itsrange of verifiability that covers all artifacts that can be reached by following trusty URI links (green arrows).

3. Implementation

3.1Authentication & Authorization:

Authentication is a process in which the credentialsprovided are verified to those on file in a databaseof authorized users' information in a local databaseor within an authentication server. Authorization isthe function of specifying access to resourcesrelated to information security and computersecurity in general and to access control.In this project authentication is done to providemore security for the users to have their owncredentials to log in. The admin approves the userswho are registered and provide rights to login to the process.

3.2Cache of the data:

Cache which is widely used and very stable, buthas not changed in years and is no longer activelydeveloped.The Cache is designed to assist a developer inpersisting data for a specified period of time.In this project, it is used as the collection of data tostore which is used for various processing.

4.3Secured Distribution (Encoding &Decoding):

Encoding is the process of making a sequence ofcharacters such as letters, numbers, punctuation,and certain symbols etc. into a specialized formatfor efficient transmission or storage. Decoding isthe inverse process -- the conversion of an encodedformat back into the original sequence ofcharacters.In Encoding, the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-141 PAGE NO: 836-842

data which are to be published isbeing encoded and it is being transformed intoencoded values and stored it in the database. InDecoding, the converted data is being decodedback only if the valid user enters otherwise, itshows that you cannot access the file.

3.3 Publishing the data:

Data publishing is the process of making the dataavailable on the Internet, so that they can beaccessed, analyzed and reused by anyone forresearch or other purposes.The data are being published where the appropriatelevel has the permission to access the file which isdetermined by the admin.

4. Experimental Work

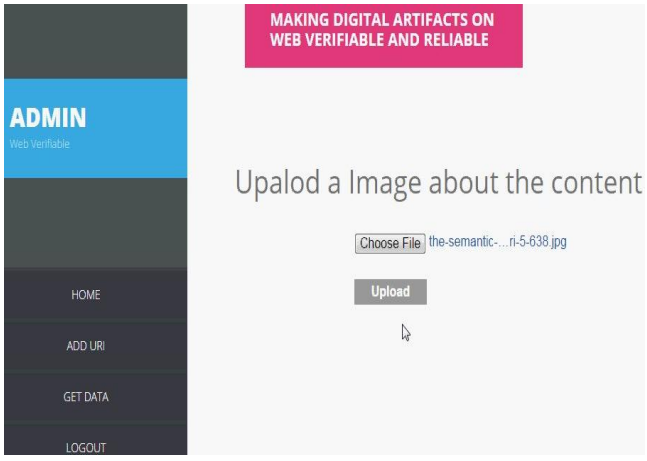

Fig 2: File uploading to cloud.

Fig 3: Java content along with URL's.

Fig 3: Content with URL based text values.

5. Conclusion

We have given a proposal for explicit URIreferences to make digital artifacts on the(Semantic) Web to be verifiable, immutable as wellas permanent. If adopted, it could have

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-141 PAGE NO: 836-842

aconsiderable impact on the structure andfunctioning of the Web, could enhance theefficiency and accuracy of tools using Webresources, which becomes an important technicalpillar for the Semantic Web, especially forscientific data, where provenance and verifiabilityare important. Further; we have started to develop adecentralized nanopublication server network.Nanopublications are distributed and replicatedamong such servers and identified by trusty URIs,thereby assuring that these artifacts remainsaccesable even if individual servers are terminated.In addition, we are working on the concept ofnanopublication indexes that allow for thedefinition and identification of small or large setsof nanopublications.

6. References

[1] T. Kuhn and M. Dumontier, "Trusty URIs:Verifiable, immutable, and permanent digitalartifacts for linked data," in Proc. 11th ExtendedSemantic Web Conf., 2014, pp. 395–410.

[2] P. Growth, A. Gibson, and J. Velterop, "Theanatomy of a nanopublication," Inf. Serv. Use, vol.30, no. 1, pp. 51–56, 2010.

[3] Farrell, Kutscher, C.Dannewitz, B.Ohlman,A.Keranen, and. Hallam-Baker, "Naming thingswith hashes," Internet EngineeringTaskforce(IETF),StandardsTrackRFC6920,Apr.2013

[4] R. Hoekstra, "The MetaLex document server,"in Proc. 10th Int. Conf. The Semantic Web, 2011,pp. 128–143.

[5] M. Altman and G. King, "A proposed standardfor the scholarly citation of quantitative data," DlibMag., vol. 13, no. 3, p. 5, 2007

[6] M. Bartel, J. Boyer, B. Fox, B. LaMacchia, andE. Simon, (2008, Jun.). XML signature syntax andprocessing. W3C, Recommendation. [Online].Available: http://www.w3.org/TR/xmldsig-core/

[7] J. Carroll, "Signing RDF graphs," in Proc. 2nd Int. Semantic Web Conf., The Semantic Web,2003, pp. 369–384.

[8] E. H€ofig and I. Schieferdecker, "Hashing ofRDF graphs and a solution to the blank nodeproblem," in Proc. 10th Int. Workshop UncertaintyReasoning Semantic Web, 2014, pp. 55.

[9] M. Bellare, O. Goldreich, and S. Goldwasser,"Incremental cryptography: The case

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 6, 2016. ISSN: 2348-6600
Reference ID: IJCS-141 PAGE NO: 836-842

of hashingand signing," in Proc. 14th Annu. Int. Cryptol.Conf., Adv. Cryptol., 1994, pp. 216–233.

[10] C. Sayers and A. Karp, "Computing thedigest of an RDF graph," Mobile and MediaSystems Laboratory, HP Laboratories, Palo Alto,USA, Tech. Rep. HPL-2003-235(R.1), 2004.

[11] R. Phan and D. Wagner, "Securityconsiderations for incremental hash functions basedon pair block chaining," Compute. Security, vol.25, no. 2, pp. 131–136, 2006.