Context Analysis for Web Applications

In the beginning, the mental set of the web was decentralized and global as there were no central reference structures in the aspect that no one could control and restrict the web.To create web connections without a doubt for everyone without differing social, political and cultural qualities, it was assumed that there should be an extensive communication dialect between web applications and computers. Despite the fact that the web has become an unparalleled financial opportunity in the later past, it has unfortunately been reshaped in a number of ways. [1]

A few businesses decide to build their claim centralized settings inside the web. It's great for ensuring device compatibility to have a universal language for computer communication [1]. However, driving their clients into a company-owned and operated atmosphere with constrained information groups and application interfaces is more advantageous for benefit suppliers. By preventing information movement so that clients can continue working with the knowledge that is already available, it makes a difference to keep clients within the same ecosystem [2]. A single substance controls both information groups and application interfaces, therefore it has the power to change both at any time, potentially making outdated apps that enable simple information sharing. When a customer shares their information with another benefit provider, it creates a situation of weakness where modern rivals hardly have a chance to enter the market. As a result, it promotes greater centralization and the development of benefit-imposing business models, providing a few firms greater control over client information and the means through which clients connect with and access information. Clients' essentially nonexistent control over their own information has given rise to serious security concerns and initiatives to re-decentralize the web, including SoLiD [2].

To provide their own utility, web apps frequently have to rely on outside data and their administrations. It is crucial to convey a concept similar to human trust to those intelligent, notwithstanding the possibility that interaction partners may stand to gain from mistreating or abusing these individuals. Web apps have the option to choose their interaction partners and manage their usefulness thanks to Trust [3]. In a centralized framework, both parties must think that connections between possible interaction partners are directed and made by a central specialist. Based on the validity of predetermined plans or manually granted, human-given authorizations, this specialist determines whether or not third parties are trustworthy [4]. In an intuitive setting, confirmation tools are used to verify the identity of third parties. [5]

Ready to enable more control over how people's data is accessed and used by services and applications by maintaining information security. This could be accomplished by re-decentralizing the web using widely used, open application interfaces and conventions while allowing the client to be independent of central experts or substances [1, 2, 4]. Clients will give access to their information to applications based on a fine-grained widespread access control framework, allowing the client to square from any application, and store their information on their own devices or in a decentralized pod-like structure, as suggested by SoLiD [2], for example. accessing their data whenever you want. The benefit of storing data in a comprehensive format is that users can switch to another application if they aren't satisfied with one for whatever reason without having to transfer their current data from one service to another. More information sources will be available on a decentralized web, and they can be added, removed, or updated at any moment. Some information providers might be hidden or only accessible through devious means, and some might have malicious or predatory intentions. Web applications should, nevertheless, nonetheless be able to connect with a subjectively large number of interaction partners without sacrificing security or utility. To do this, those online applications need a grasp of trust as well as a decentralized trust administration framework that makes use of a trust demonstration that evaluates trust more effectively than coordinate or reputation-based trust models.

In Content Trust Evaluation For Web Applications, authors proposed a Trust Framework to give web applications a mechanism to use substance trust-based, computerized, and decentralized trust assessment as seen in Substance trust. Without any human interaction, this system should function [6]. I'll focus on the Context Analysis part, one of the components of the conviction appraisal, in my thesis proposal. Creating guidelines using establishing research and combining these measures with trust assessment to get trust value results is the idea behind this proposition.

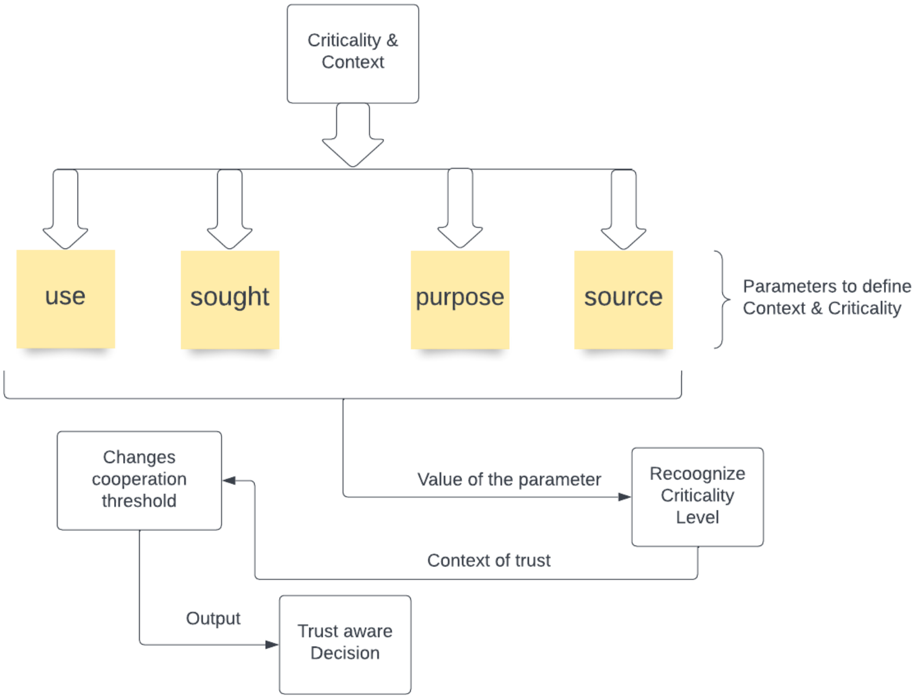
In order to determine the context of the system's operation, relevant examination involves the systematic research (discriminating, sorting, organizing, translating, synthesizing, and disseminating) of significant client work movement data. Web application setting investigation is really important in today's environment for obtaining data from web resources. It's more difficult to understand the context of an online resource, though. A web resource may occasionally contain unique settings, or certain resources may have settings with dual meanings. The literary composition of a web resource, nevertheless, may be the most challenging aspect of establishing investigation. There are several instances where online resources lack sufficient elements to distinguish the scene. precise evaluation of carefully gathered, significant client work movement information, including identification of evidence, sorting, organizing, translation, blending, and communication. investigation to establish the framework's operational environment. In the modern world, context analysis of online applications is quite important for removing data from web resources.

Content trust is a trust evaluation on a particular piece of information or some specific content provided by an entity in a given context and also it’s often subjective and there are many factors that determine whether content could or should be trusted, and in what context [5]. The use of the given interaction partner data, reason behind the information searched, purpose of the interaction partner data are mainly responsible to define the context of the web application [5]. These values will be used as a criticality parameter for each level of criticality which will be responsible for changing the cooperation threshold of the interaction.

As we already define the parameters of the context to recognize criticality level, now we need to determine how we can use these values to change our cooperation threshold, which means give weight to these parameters' value. For weight these values my idea is to mix the topics of the context along with the criticality level, because by doing that we will get the context of the trust and this will help to be more specific to give weight to our criticality parameters value. Based on the criticality level we will change the cooperation threshold value and finally the output after calling the co-operation threshold will be used for making the trust aware decision.

Throughout the process my challenge will be to maintain the accuracy of the context parameter value which means how relevant the found context parameter is with the context of input data. Along with this another challenge can be the number of information of the input data. Because it is quite obvious that sometimes the input data may contain less information or may be no information to get the context parameter of that.

On the basis of the knowledge I have or have obtained, I draw the below diagram for a better overview. I am confident enough that this process framework should be able to provide us the information which we are looking for making trust aware decisions.



Bibliography

[1] L.-D. Ibáñez, E. Simperl, F. Gandon, and H. Story, “Redecentralizing the Web with Distributed Ledgers,” IEEE Intelligent Systems, vol. 32, pp. 92–95, 2017.

[2] A. V. Sambra, E. Mansour, S. Hawke, M. Zereba, N. Greco, A. Ghanem, D. Za- gidulin, A. Aboulnaga, and T. Berners-Lee, “Solid: A platform for decentralized social applications based on linked data,” MIT CSAIL & Qatar Computing Re- search Institute, Tech. Rep., 2016.

[3] H. Yu, Z. Shen, C. Leung, C. Miao, and V. R. Lesser, “A survey of multi-Agent trust management systems,” IEEE Access, vol. 1, pp. 35–50, 2013.

[4] V. Siegert, M. Noura, and M. Gaedke, “aTLAS: a Testbed to Examine Trust for a Redecentralized Web,” in Proceedings of the 2020 IEEE/WIC/ACM Inter- national Joint Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT). IEEE, 2020, pp. 411–416.

[5] Y. Gil and D. Artz, “Towards content trust of web resources,” Journal of Web Semantics, vol. 5, no. 4, pp. 227–239, 2007.

[6] A. Kirchhoff, V. Siegert, M. Gaedke, “Content Trust Evaluation System For Web Application”, VSR, pp. 1–25, 2022.