A COMPARATIVE ANALYSIS TO OBTAIN UNIQUE DEVICE FINGERPRINTING

Theertha Babu, Kiranmayee Narhari, Yash Agrawal, Abhishek Karan

ABSTRACT

The main focus of this paper is on obtaining Unique Device Fingerprint using JavaScript specifically Angular JS and Client JS techniques which together can make the comparative analysis more efficient and valuable. The term 'Device Fingerprinting', is a phenomenon to collect information such as Device name, java installed and its version, user agent, browser version, etc of an individual computing device for the purpose of identification. Through this technique even if the cookies are turned off we can obtain individual device fingerprints. Device Fingerprinting is often immutable and tends to rapidly change, making it challenging to get a unique one. The majority of solutions available to obtain a unique device fingerprint are complex, and most solutions don't have the sufficient efficiency to obtain the required. Thus, this Comparative Analysis to obtain Unique Device Fingerprint using JavaScript techniques simplify this challenge and create an opportunity in analysing and obtaining the data in much more efficient way.

Keywords: *Device Fingerprinting, Unique Identification, Unique Fingerprint, PC Fingerprinting.*

INTRODUCTION

Device Fingerprinting uses JavaScript techniques which includes Angular JS and Client JS along with Spring MVC and Restful Webservice as backend technique's for the comparative analysis. Device fingerprinting is about collecting information or data, its wider usage in different applications, and obtaining efficient fingerprint. That can be examined and hence used deeper by new applications in a timelier way to increase efficiency or to enable new business models. Today, Device Fingerprinting is becoming a business initiative through which new applications use this unique fingerprint to ensure security, prevent fraudster, easy and user-friendly environment to users. It also enables organizations to accomplish several objectives:

- Apply the analysis done to detect anomaly beyond the traditional analysis to provide first unique fingerprint. Use cases using this first fingerprint will lead and support real-time applications to obtain unique fingerprint anytime anywhere.
- We can create velocity filters based on the fingerprint that will give a way to minimize the costs of fraud when details like names, personal card details and Internet Protocol addresses are changed.
- Allow people in all roles to explore and analyse information related to transactions in order to have a secure transaction.

- Detect all types of illegally involved or wrongly involved accounts or subscriptions, that are made by fraud experts or automated systems.
- Improve big business outcomes and manage risk of detect risk which comes from customers that share same device network, i.e. they are backlisted.

In short, Device Fingerprinting provides the capability for an organization or individual to ensure data security and individual identification to have efficient enterprise, an organization that dynamically adapts to the changing needs of its individual customers by using information from the fingerprint obtained. Although it is true that many businesses use device fingerprint to manage the growing capacity requirements of today's applications such as advertisements, customers' personalised search to enable SEO techniques. Enterprise uses Device Fingerprinting to enhance revenue streams by using the fingerprints the way that they give all the information about the customer that helps in enhancing business solutions. Device Fingerprinting uses techniques which are available to also work on mobile phones and extract data from an individual mobile phone. Device Fingerprinting means for performance and capacity because of the following listed below: Uniqueness- how confidently and specifically one can identify a computer and differentiate it from the others on the web. It relies on the entropy or data that the fingerprint possesses. Persistence-to uniquely identify a device based on our unique technique to obtain fingerprint. For example, the OS would be a persistent attribute if the fingerprint. Resistance-It tells how appropriate the Device Fingerprinting technique is made to tamper by a hacker or a fraud. For example, a cookie of a browser may be unique but it is easily deleted or copied. Fit-This measure tells us how the integration of the Device Fingerprinting technology is done with our business and technology requirements. Ideally the Device Fingerprinting method should be transparent to the end user. Existing fingerprinting system is of two types:

Client Based- These methods require installing a software executable on an end computer. Its advantages are that they have permission to all the hidden OS information such as the HD serial number and MAC address of the network. This information is highly unique, persistent and harder to tamper with. Its disadvantages are that the process requires some action or permission on behalf of the user. The other issue which is raise is course that most corporate computers won't allow anything to get installed from an external source. Server-based- These methods on the other hand rely on information that can be measured remotely via a profiling server. Advantages-this method has zero impact to the user's customer experience and their privacy and does not require registration. this is often the only practical method available to e commerce, online media and retail financial businesses. Disadvantages-the protected individual attributes such as MAC address or HD serial number are not available. Recent advances in TCP protocol and OS profiling are now able to enable a device to be uniquely identified in spite of various and obvious browser characteristics such as browser type and version.

SPRING MVC FRAMEWORK

Spring MVC helps in building versatile and around coupled web applications. The Model-see controller setup design helps in separating the business legitimization, introduction technique for considering and course present. Models are in charge of tending to the application information. The Viewpoints render reaction to the client with the assistance of the model request. Controllers are responsible for continuing through the demand from the client and coming back to the back-end affiliations. Obviously when a demand is sent to the Spring MVC Structure the running with change of occasions happen. The Dispatcher Servlet first gets the demand. The Dispatcher Servlet actuate the Handler Mapping and sums up the Controller which is related with the demand of the user. The Controller approach the urgency by calling the right association structures. The ModelAndView challenge contains the model information and the view name. The Dispatcher Servlet sends the view name to a View Resolver to locate the true-blue View to summon. Over the long haul the Dispatcher Servlet will pass the model request the View to render the outcome. The View with the assistance of the model information will render the outcome back to the client.

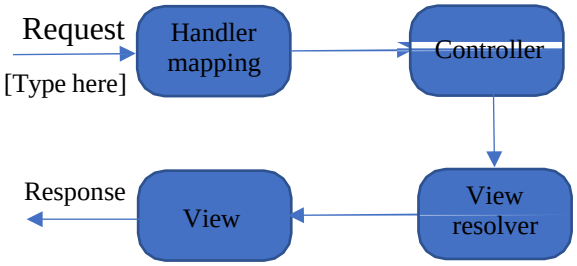

Figure 1. Spring MVC Framework

RESTFUL WEB SERVICE

Restful web administrations are worked to work best on the Web. Illustrative State Transfer (REST) is an engineering style that determines limitations, for example, the uniform interface, that if connected to a web benefit incite alluring properties, for example, execution, versatility, and modifiability, that empower administrations to work best on the Web. In the REST engineering style, information and usefulness are thought about assets and are gotten to utilizing Uniform Resource Identifiers (URIs), normally connects on the Web. The assets are followed up on by utilizing an arrangement of straightforward, very much characterized tasks. The REST structural style compels an engineering to a customer/server design and is intended to utilize a stateless correspondence convention, regularly HTTP. In the REST design style, customers and servers trade portrayals of assets by utilizing an institutionalized interface and convention.

CHARACTERISTICS OF DEVICE FINGERPRINTING

There are various variables you should consider while executing a Device Fingerprinting innovation. Zero effect Device Fingerprinting arrangement must have zero effect arrangement on both your client encounter and additionally your IT basics. A client to need to download programming or utilize an equipment token that will prompt disappointment and deserted framework, while requiring your operational staff, who are regularly incanted on up-time and reachability, to introduce add on programming on your web servers can likewise prompt some pushback. Establishment adaptability the gadget fingerprinting innovation can be executed as a web administration to diminish establishment, upkeep and adjustment costs. An all around characterized web-API will empower straightforward and financially savvy blend of Device Intelligence into your current association rules motors, hazard based access control frameworks. Continuous Settlement motor Knowledge is just as profitable as it is auspicious. Search for Device Fingerprinting arrangement that is fit for computing Device Risk continuously as opposed to minutes, hours or days. Fluffy coordinating One way to deal with producing a Device Fingerprinting is to play out a basic hash of estimated characteristics. The impediment of such an approach is, to the point that it takes just a single parameter to change, for instance swapping the program utilized from Internet Explorer to Firefox, and a completely new Device Fingerprint is created. Search for a Device Fingerprinting arrangement that uses a fluffy coordinating method to give a more precise and constant Device Fingerprint. Estimation Diversity The present programs bolster advancements, for example, Flash and JavaScript that are equipped for social occasion broad Device Fingerprinting data. Be that as it may, such innovations are likewise ready to be promptly impaired by fraudsters and protection cognizant web surfers alike. To have the capacity to separate between a fraudster and a significant client, search for a Device Fingerprinting innovation that does not depend solely on either JavaScript or streak and can exceptionally distinguish a gadget notwithstanding when these advancements are handicapped. Gadget Fingerprint Depth Much the same as an ice sheet, what you can't see could sink you. All web servers and web examination organizations give essential program techno designs, for example, program compose, program dialect and the sorts of mixed media and dialects that are upheld. Notwithstanding, this data additionally simple to control by an educated fraudster and is likewise ignorant concerning cautioning signals that lie underneath what the program is letting you know. Search for a Device Fingerprinting approach that looks past the program and can perform Operating System, Protocol and Connection Fingerprinting continuously. The advantage of these advancements is that they can perceive a fraudster notwithstanding when the program traits change or when treats are erased, and would more be able to precisely aware of when a high hazard intermediary is being utilized. 7.7 First-time assurance: Device Analytics and Anomaly Detection For most web based business sites, the lion's share of their exchanges and extortion endeavours are from new clients. For these organizations, perceiving an arrival fake gadget isn't as helpful as having the capacity to distinguish a misrepresentation endeavour the first-run through, progressively. Search for a Device Fingerprinting arrangement that can give first-time extortion insight, for example,

- Whether the Device is holing up behind an intermediary and precisely decide the hazard related

with the intermediary.

• The True IP and not only the Proxy IP that the gadget is association from.

• The True Geo that the association began from, and not only the area of the intermediary utilized.

Regardless of whether a gadget has been bargained by malware and has a place with a botnet.

DEVICE FINGERPRINTING MECHANISM

Device Fingerprinting is becoming an important component of identification in the age of new tools and applications. As the uniqueness, persistence, fit and modularity of unique identification of individual remote computing device grows, device fingerprinting will also be become more important tobe used in different application including security.

Dealing with unique fingerprint id obtained and integrating it to various systems will increase efficiency and usability if the system. The mechanism used consists of implementation of a client js system using spring mvc framework. Analysing it to obtain unique fingerprint by testing it on different systems. Followed by implementation of angular js system using restful web services. Interpreting both the systems in various test cases we obtained unique fingerprint.

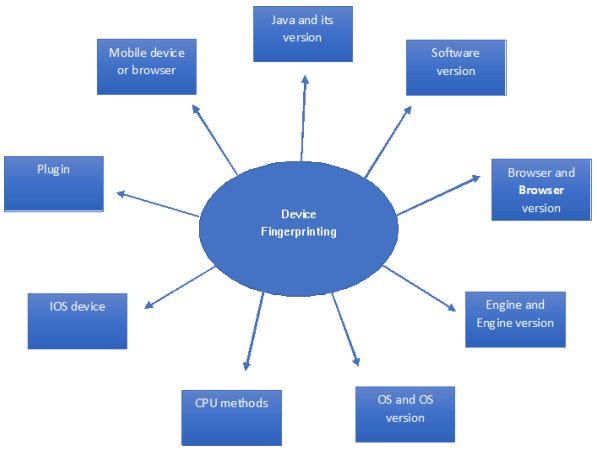

Figure 2: Device Fingerprinting Attributes

The above figure 2 describes a user's individual device fingerprint attributes. The attributes consists of Browser and its version, Java installed and its version, Plugins installed, Engine and its version, CPU methods, OS and its version, IOS device, software versions, etc. Thus the existing systems which are used to obtain fingerprint are based on two methods:

- Client Based method which uses a software to be installed in the remote computing device and hence obtain data.
- Server Based method which uses JavaScript techniques to obtain fingerprint using different frameworks suitable.

Here we are using Server based method to implement our system. Instead of Client based technique in which user privacy or integrity is not maintained. Here the server based have a drawback which is MAC address is not obtained in the unique fingerprint as MAC address is the main key to fraudster or even the violation of the user privacy. This can also be called as a drawback or data security key to user friendly system. We consider pairing Device Fingerprinting with different application to enhance security, prevent fraudster, generate easy or automated system of you own. The information obtained from the device fingerprint can be used entirely and can provide an automated help in selecting the best ways to present the data. Thus Device Fingerprinting can also be made in a way to easily deploy the entire data in a much approachable way of presentation. For an easier understanding, consider your data to be great and unique information in terms of fingerprinting.

CONCLUSION:

Device Fingerprinting using Client JS techniques may not be a perfect solution for obtaining unique fingerprint but on the other side Device Fingerprinting using Angular JS techniques is providing the best solution by obtaining a unique fingerprint which includes Java and its version, Software Version, IOS device, CPU methods, Engine and its version, etc. All these together are giving us an identification mark of the individual computing device and hence can be used in many applications. Some applications in which this unique device fingerprint can be used are banking services, identification purposes, user friendly applications, automata system application. Through device fingerprinting, organizations or individuals can have access and can analyse the information of any individual computing device and can use it in the real time applications efficiently. Hence Unique Device Fingerprinting is a research in itself.

REFERENCES

1. Panopticlick: Is your program safe against watching and following? https://panopticlick. eff.org/.

2. Coreestimator. https://github.com/oftn- oswg/center estimator.

3. [wikipedia] once-finished of framing frameworks. https://en.wikipedia.org/wiki/List of shaping structures.

4. M. Ayenson, D. Wambach, A. Soltani, N. Mind blowing, and C. Hoofnagle, "Streak treats and security ii: Now with html5 and etag respawning," Available at SSRN 1898390, 2011.

5. K. Boda, A. M. Foldes, G. G. Gulyâ¨ as, and S. Imre, "Client watching and following on theâ' web through cross-program fingerprinting," in (game- plan of occasions) of the sixteenth Nordic Conference on Information Security Technology for Computer programs, ser. NordSec'11, 2012, pp. 31-46.

6. [github]AmIUnique?https://github.com/DIVERSI FYproject/amiunique.

7. M. Perry, E. Clark, and S. Murdoch, "The plan and execution of the tor program [draft][online], joined states," 2015.

8. S. Berger. You should exhibit two ventures. http://www.compukiss.com/web and-security/you-should-display two-browsers.html.

9. [graphicswikia]anti-(shield for)ing.http:// graphics.wikia.com/wiki/AntiAliasin g.

10. B. Krishnamurthy, K. Naryshkin, and C. Wills, "Confirmation spillage versus insurance measures: the making parceled," in Web 2.0 Security and Privacy Workshop, 2011.

11. B. Krishnamurthy, K. Naryshkin, and C. Wills, "Confirmation spillage versus insurance measures: the making parceled," in Web 2.0 Security and Privacy Workshop, 2011.

12. Wikipedia. Do whatever it takes not to Track Policy. http://en.wikipedia.org/wiki/Do Not Track Policy.

13. P. Eckersley, "How (like nothing else on the planet) is your web program?" in (strategy of occasions) of the tenth International Conference on Privacy Improving Technologies, ser. PETS'10, 2010.

14. F. Roesner, T. Kohno, and D. Wetherall, "Recognizing and protecting against outsider watching and following on the web," in (strategy of occasions) of the ninth USENIX Conference on Networked Systems Design and Putting into utilization, ser. NSDI'12, 2012, pp. 12-12.

15. Etienne and J. Etienne. Customary suzanne monkey from blender to kick your redirection off with threex.suzanne.

16. http://learningthreejs.com/blog/2014/05/09/custo mary suzanne-monkeyfrom-blender-to-kick your- preoccupation off with-threex-spot suzanne/.

17. X. Dish, Y. Cao, and Y. Chen, "I don't comprehend what you go by the past summer - shielding clients from outsider web watching and following with audit and followingfree program," in NDSS, 2015.

18. D. Fifield and S. Egelman, "Fingerprinting web clients through (game-plan of printed letters of a near style) numbers that measure things," in (identified with directing cash) (the examination of making riddle codes) and Data Security. Trapr, 2015, pp. 107-124.

19. Lerner, A. K. Simpson, T. Kohno, and F. Roesner, "Web jones and the hooligans of the lost trackers: An (identified with considering individuals who carried on quite a while back) examination of web watching and following from 1996 to 2016," in 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, 2016.

20. M. Mulazzani, P. Reschl, M. Huber, M. Leithner,
S. Schrittwieser, E. Weippl, and F. Wien, "Smart and solid program perceiving proof with javascript motor fingerprinting," in W2SP, 2013.

21. Soltani, S. Canty, Q. Mayo, L. Thomas, and C. J. Hoofnagle, "Streak treats and security," in AAAI Spring Symposium: Smart Information Privacy Management, 2010.