INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY (IJCET)

ISSN 0976 – 6367(Print)
ISSN 0976 – 6375(Online)
Volume 4, Issue 2, March – April (2013), pp. 198-212
© IAEME: www.iaeme.com/ijcet.asp
Journal Impact Factor (2013): 6.1302 (Calculated by GISI)
www.jifactor.com

IJCET
© I A E M E

HIS: HUMAN IDENTIFICATION SCHEMES ON WEB

Hemprasad Badgujar, Dr. R.C.Thool

Department of Information Technology SGGS IE&T Nanded, Maharashtra, India.
Head of dept., Department of Information Technology SGGS IE&T Nanded, Maharashtra, India.

ABSTRACT

We address the present and future possibilities of Automatic Reverse Turing Tests for distinguishing between human users and software bots on the web, comprised of pre-proposed & existing techniques which are generally required to pass the Human Interaction and observation Proofs (HIOPs). Inevitable methodology to relieve drawbacks of current human identification techniques to protect web services from abuse by software programs masquerading as human users. We arrived at the proposed new concrete identification techniques by evaluating each of the most prevalent and new Human Identification Techniques (HIT). A survey has been conducted to find the advance characteristics of the each technique. Each technique was evaluated in three categories: Full, Hybrid and Non interactive. By gathering data to determine a numerical score for each technique based on a rubric. We proposed new technique by removing inherent drawbacks and with merging and overlapping benefits of the top scoring Human Identification Scheme's (HIS) layers. To examines and discuss to make them more productive and persistent without annoying common users as potential solutions that allow identification systems to test human users.

Keywords: Reverse Turing Tests, Human Interactive and observation Proofs (HIOPs), Human Identification Schemes (HIS), Human Identification Techniques (HIT).

I. INTRODUCTION

There are many risks posed by bots and other types of malicious axiomatic web crawlers. These are the software programs which crawl through the various web sites, system applications to gather information and abusing different services, for example 1) Make auto registrations service accounts like email /social network/cloud/etc. 2)Mimic legitimate clients to change rank of websites popularity.3) Bogus comments on blogs/forums/chats.4)

Distribution spams/malwares/mount phishing attacks/other malicious programs pose a serious threat to online users [1]. That ensures an arms race between services providers and bot programmers that have made it extra challenging for such test schemes to identify correctly the humans user while blocking only software bots. Despite all preventive measures taken, certain bots are able to break the best defenses. Due to hazardous activities of automated bots, it is important to distinguish between these two classes. One of the schemes to thwart such bots is to use which are used to test challenge & check response that is easy for humans but hard for computers to solve. Existing interactive HIS having different challenges that require a significant conscious effort by the human user interaction by input devices. Many time it distract and interrupt human users from accessing further services, since the challenge is perceived as an irrelevant intrusions, but one of the standard tasks of registering with modern web Human Identification Schemes services is the demonstration that we truly are human beings and not wicked computer programs set on causing transgression [2] [3].

To provide reliable security the effective detection and isolation techniques for bots is in great demand but is still missing. While much research had its focus on the development and testing of human identification techniques and schemes, but there are not a significant efforts that can perform a comprehensive comparison of these different techniques. The data was populated in each category for each technique to identify through a local hosted web-based testing platform and users survey, as well as a rudimentary user survey review. The final rankings were determined according to an equation 1 we calculated the numerical score of each technique as a weighted sum of each relevant criteria.

II. HUMAN IDENTIFICATION BACKBONE

There are different types of human identification & registration techniques that are used in web services and the others that are used in online or offline system applications. All the identification services are managed either by Administrator or by Server process automation that depends on their design of the services. Fig.1 Shows Network architecture required for the user identification & registration Different Identification required Activity are processed at Server Side and client side[4].

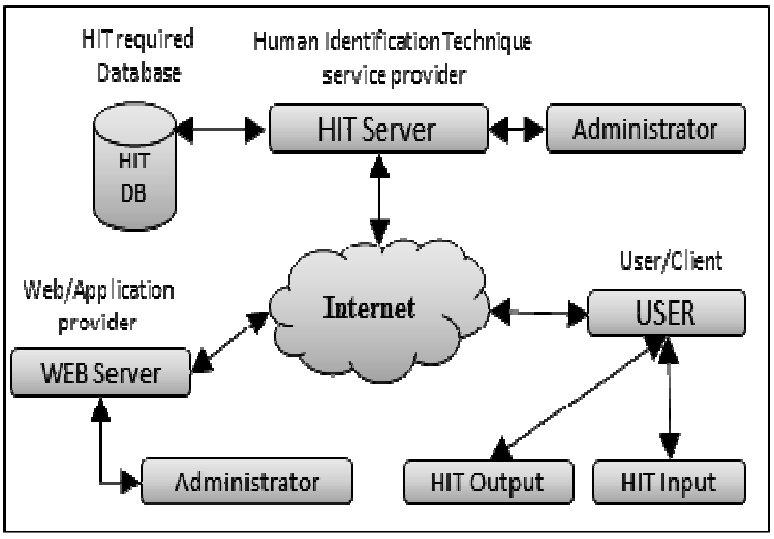

Figure 1 HIT Network Component Diagram

1) Server side Activities: They are manage with help of server administrator or server process automation. Some are required active participation of administrator and some are not. Server side activities are Database formation and analysis, Query generation & automation, Validation & Verification, Confirmation, Banning services, application scripting, etc. web services

2) Client side Activities: In client side, the presentations of UI through HIS APIs and the user interaction through HIS APIs take place. The users interact with the presented UI to understand identification schemes through the web applications if using online HIS or standalone desktop applications for offline HIS. HIT presents through Output devices like display devices, audio devices, sometime printers, etc. through which user can sense identification criteria because after understanding the identification criteria, the human users can interact with HIS [5] [6].

Table 1 : Elucidation of User-Input Actions

Actions	Action Elucidation
Keystroke	Press and release of a key.
Point	A series of continuous mouse cursor position changes with no mouse button pressed; the time- stamps for each pair of cursor position changes
Pause	A period of time fragment or longer with no actions.
Click	The press and release of a mouse button
Point & Click	A point followed by a click within time fragment. [5]
Drag & Drop	The press and release of a mouse button; the cursor Changes pixels between the press and release.
Gesture	Continuous movement of cursor while pressing of a mouse button / hand front of camera
Present	Presenting Biological & physical characteristics to sensors
Event flow	System tasks & events (copy, paste, select, etc.)
Touch	Multi touch / single Touch on touch screen

Input to HIT API given through Input devices such as Keyboard, Mouse, Touch Screen panels, Sensors, Camera Devices, etc. by which human Users can interact. The output schemes to the human users include the devices through which HIS interaction task can be easily recognized by various human senses like sight, hearing, touch [7].

To make HIS presentation hard to understand for software bot, different changes can be integrated with the output API text, image, video, animation and Audio by noising, rotating and occlusions, obfuscation, distorting, warping, curving, deviating, fragmenting, shredding, overlapping, scrambling, anamorphosis, reformatting, disorientation, variation coloring, twisting, Scattering, varying, irregularity, Optical Illusion, degradations, legibility of text, segmentation, Gestalt perception, style-consistent recognition trajectory, EZ-gimpy, confounding, demoralization, disarranging, discomfiting, discomfiture, distraction, disturbing, dither, dumbfounding, perturbation, interfaces color, noising segmenting, Baffling, random arcs extracting pixels , randomization , glyph ,visual similarity, decoying, Splitting ,Rotating etc. [8-18].

Table 2 : Elucidation of Outputs schemes for User

Schemes	Schemes Elucidation
Text	to display schemes / task description in text form [19]
Image	to display schemes / task description image form [20]
Video	to display schemes / task description in Video form [21]
Audio	to present schemes / task description in audio form [21]
Animation	to display schemes / task description in image form [21][22]
Touch sense	to present schemes / task description in touch sense form

III. MOTIVATION

Computers are used by many people to avail different online and offline services, e.g., cloud services & applications, e-commerce, blogs, forums and system applications etc. In all of these services, the user has to register with the system by filling out a form. However, bots, pose as humans for signing up for these free services. Preventing online services from these automated-bots is a challenge. The extant methods for combating bots are not successful in the protection of web & system applications. The approaches based on Human Interactive and observation Proofs (HIOPs), most commonly used to distinguish bots from humans. However, the inherent interactive requirement makes HIP-based approaches inadequate.
In this paper, we introduce approaches based on Human Interaction and observation Proofs (HIOPs) use to create HIS to avoid bots. HIOPs offer distinct advantages over HIPs & HOPs. The approach that we were following is the enumeration of the behavior of human users along multiple different axes, and setting thresholds that distinguish human users from bots. Unfortunately, no reliable data may be available in order to understand more about bot behavior and to cross-validate our outcomes. We suggest using two mechanisms, the first is to employ two thresholds for each criteria, enabling the identification of users who are most possibly human or most possibly bots according to need, to avoid ambivalent cases.

IV. RELATED RESEARCH

For human Identification &Registration there are different schemes. Some of them are still used by different web & system applications, and some of them are in phase of proposal & proposed. The schemes for identification criteria's for human identification presents to human in the form of multimedia techniques & by different human sense of sight , hear , touch.

A. Human & Bots

Human: Human behavior is more complex than computer automated program behavior due to human senses and intelligence. Humans beings different in various aspects from the computers, they are capable of making decisions on their own and assuming suitable data when necessary.
Bots: Bots are nothing but software robot, refers to automated computer programs that partially require a human operator if needed. Bot is a program with the unique purpose that interacts with an online or offline services to automate different undertaking illegal activities or achieving goals not always in line with the ethic and habits. Single bot operators can controlling a few hundred bots. Potential abuses of software bots include spreading malware, phishing, booting and other malicious activities; but several situations where the use of automated tools are mandatory, due to the large quantity of data to process to facilitate human user.

B. Past and Present Research

Most human identification techniques have been variations on the ideas of HIS. These include Full Interactive, Hybrid Interactive and Non Interactive Identification systems in that again have two factors, as user side and server side Interactions. These are the scheme's criteria to user to understand & follow steps to get identify. Commonly these schemes are presented by text, images, videos, animation, audio, etc. through the output devices such as that can only understand by human user to get identify and to register.

1) Recognition Base : The identification of something as having been or interpreted from previously seen, heard, known, etc. to imply on graphical, text, audio authentication technique for human identification. Users need to recognize / reproduce / remind their choice among reminder, hints and gestures set of schemes. [15][23][24]
2) Task Base: Asking a visitor to complete a simple task takes almost no extra time. Includes both a visual task; such as typing words displayed in an image, and an audio task, such as typing letters spoken in an audio file. Task interaction results from humans usually performing well and machines generally do not. Use of different interactive tasks as clicking, dragging, dropping, scrolling, sliding, drawing, etc. to identify human interaction within computer or web services. [5][25]
3) Puzzles Base: To use human intelligence to solve Puzzlement from that identifies the presence of human. Syllogism is another aspect wherein advanced computer programs lag behind the human users, so the user is needed to solve a puzzle and provide the answer. [28]
4) AI Questions Base: Questions based on pure logic are ask in such a way that multiple questions have the same answer. The bots will not be able to solve them in stipulated amount of time and humans are aboriginal to such questions. [26][27][22]
5) Small Games Base: Programmed bots cannot play games for which they have not been programmed. Simple twist in the game can make the source code of the game playing obsolete, on the contrary, the human users of the game are able to pass the test as they do not have to scratch their heads on anything nor does it involve any hard understanding part. [31][32]
6) Native System Tasks Base : This include creating new files, copy , paste , delete ,update of data or other normal tasks we perform daily in the operating system, user is instructed to perform such a task in the application itself so bots are not able to perform that tasks.
7) Hybrid HIS Base: Combination of available and new human identification techniques discussed mentioned above. [28]
8) Server & User Management: Various users are identified uniquely and the administrator has total access to the data or other aspects of the user's information. User authentication and identification manage by administrator or by server automation systems.
9) User Defined & Abstracting Function components: Bots are programmed for capturing information on the internet, they identify a component on the basis of the name which is given to it, so while creating the website, the developer abstracts the common name of the object into a unique and special name, and as the bot mines the source code for the page, it wouldn't be able to identify the components itself.
10) Conformational &Tokens Services: Multilayer authentication is performed by passing tokens at the end user side, to verify the human users. The bots may be able to retrieve the information sent from token, but due to the multilayer nature of token, they cannot input the information into the conformational page, neither understands how to interact.

11) Biometric Data recognition: Bots do not have any biometric identification information, so this is a reliable mode of identification of bots and distinguishing them from human users of the system, if the human operator gives his ID to every bot, we can recognize the pattern.
12) Single sign-on: Single sign-on ID is use for authentication. Like the OPEN ID. In this way, the user is redirected to the host website for authentication and then after confirmation of the usage of data the account is given access. Bots are not able to process all such information.
13) Biometric Data Analysis: Analyzing biometric data such as form completion time, clicking style, mouse gesture style, etc. Human beings are different and unique in nature, so this method captures data and analyses it to model the response of the user that is later compared for differentiate bot and human, a bot being a computer program, has very different interaction with the system than the human user.
14) User-Agent header: User agent is the characteristic identification string used by a software& hardware agent while operating in a network protocol. All software and hardware have a standard user agent, and thus human users will be using the web application whose user agent is well defined, but it is not true in case of bot.
15) Browser fingerprinting: Identifying characteristics of browser configurations, because every web page on the Internet at a call leaves a kind of "fingerprint". This relatively new form of identification shall be illuminated scientifically in order to subsequently develop protective measures. Web activity without your knowledge, One place where generating digital fingerprints is very useful is in combating transaction frauds.
16) Unusual Form Interaction: Prompting the user to inter- act with a web form in a typical manner, such as un-checking an already-checked checkbox.
17) Hidden Form Elements : The form with which the user interacts contains some hidden elements, the human users are not cognizant of these elements on the contrary the bots submit information even for the hidden elements as they browse the source code of the web page and fail to understand it. Hiding form elements from users (e.g. through CSS and/or HTML attributes), with the assumption that if information is entered into the element, the form was submitted by bot which does not understand the aforementioned website source code attributes
18) JavaScript Detection: Bots normally have JavaScript turned off, so this method can be used to identify bots from users, but the effectiveness of this technique is not known. Detection of human user if the user has JavaScript enabled but bots do not typically implement JavaScript engines.
19) Bot Response: This is a criteria for HIT that does not require human interactions as they are hidden from user sight .They are merged with website source code or system application code. Some of above schemes used either user side or server side as per their merging practice with deployed applications [29]

C. Future Research

Clearly, there is a wide variety of techniques available. However, very little is known about their relative effectiveness. For identification scheme there is not any boundary to create new techniques to identify Human user but there is limitation due to empirical and limited physical senses of humans to accept data for perception.

V. CLASSIFICATION CRITERIA

To classify human identification schemes we create three criteria as Full Interactive, Hybrid Interactive & Non-Interactive as shown in table 3. In all criteria, there are two sub-type of schemes at user side &Server side. These techniques are classified according to the level of dependency on the user in the process of HIS.

1) Full interactive: This type of identification technique uses full interaction with the user, the user has to perform the tasks and input the necessary data wherever needed.
2) Hybrid interactive: The dependency on the user for the process is reduced to some extent, the system assumes the other necessary data, like a image HIS along with a mouse motion analyzer implemented in the system, which will get half input from the textbox and the rest from the analyzer.
3) Non-interactive: This method is completely automatic here the user does not need to input anything; unlike the previous two methods, thus the system analyzes the way in which the user is using it. It may use any suitable method for identification of the users which may include one or more of the following methods for data collection from the user by the touch screen, mouse, web camera, and or the mic, thus the user can be easily identify from bots who can't possibly fake all such implicit information. Table 3 shows classifications of identification schemes as per interactions experienced by human user.

Table 3 : Classification of identification schemes for User to avoid bots

Full Interactive		**Hybrid Interactive**		**Non Interactive**	
USER SIDE	**SERVER SIDE**	**USER SIDE**	**SERVER SIDE**	**USER SIDE**	**SERVER SIDE**
• Tasks • Puzzles • Questions • AI Questions • Small Games • Multi factor HIS • System Tasks	• Confirmation Services • Key Tokens Services	• Recognition Questions • Puzzles • AI Questions • Multi factor HIS	• User Management • User Defined Functions • Biometric Data recognition • Centralized Sign-on	• Biometric Data Analysis • User-Agent header • Browser fingerprinting	• Unusual Form Interaction • Hidden Form Elements • JavaScript Detection • Web Server Management • Bot Response

VI. ANALYSIS FRAMEWORK

To perform absolute analysis and comparison for all consonant aspects of identification schemes, We use grading system to grade HIS in several category, like experience resulted by server side, administrator side and user side at the process of differentiate human from software bots . In the way of analyze Non-interactive schemes it is hard to analysis& compare grades as criteria ,because they are not experienced by user or administrator side , only server side criteria experience gain by server automation system , hence it will going to take in mind as factor to evaluate further analysis for Non-interactive schemes. Table 4 shows categories with criteria including their weight to identification schemes

Table 4 : Schemes comparison analysis framework with weight

Category	Criteria	Notation	Weight (W_i)
System/Server	Penetration Rate	$[PR]_s$ =Y_1	5
	System platform	$[S']_s$ = S'	4
	Complexity	$[C]_s$ =X_1	3
	Time to response	$[T]_s$ =Y_4	2
Administrator	Database	$[DB]_A$ =X_2	3
	Automation	$[A]_A$ = X_3	3
User	Understandability	$[US]_U$ =X_4	2
	Recognition Rate	$[RR]_U$ =X_5	1
	Time to Interact	$[TI]_U$ =Y_3	2
	Success Rate	$[SR]_U$ =V	1
	Skip Rate	$[SR]_U$ =Y_2	1

A. Progression of the Analysis

To get result we evaluate scores of each category of each identification schemes. Final score of each schemes was calculated by assigning overall performance using following equation 1, Where $HIS_{(S)}$ is Final Score of human identification scheme "s", calculated as normalized weighted sum over the criteria X_i and Y_j. Weight was assigned to each criteria by considering relative impact of those criteria on complete factors of usability experienced by user, administrator &server.

$$\boldsymbol{HIS_{(S)} = V\left\{S'\left[\left(\sum_{i=1}^{5} W_i X_i\right) - \left(\sum_{j=1}^{4} W_j Y_j\right) \Big/ HIS^{\alpha}_{(S'\to 1)}\right]\right\}} \quad \text{..(equation1)}$$

In analysis some of defined criteria are as in table 5 which we taken severalcriteria as shown in table 5. These criteria are likeSystem Penetration Rate, System Platforms, HIS Complexity, HIS Database, Time To Response by User and Server, Time To Interact HIS by User, HIS Layer Automation, Understand Rate of User, Recognition Rate, HIS Skip Rate by User, Success Rate of HIS. The final score is computed by summation of each criteria scores. In criteria score [X_1, X_2…] series shows positive impact on final score and [Y_1,Y_2..] series shows negative impact, for calculation V & S shows multiplicity in schemes criteria factors in $HIS_{(S)}$ shown in equation 1 for scheme '**s**' (small s) calculated as $\boldsymbol{HIS_{(S)}}$.

Table 5 : Identification Schemes evaluation chart

Criteria	Weight	Range	Description (With Example)		Hypothesis
$[PR]_S$ =Y_1 Penetration Rate	(W_1) = 5	1-3	1	No Penetration	Crucial point where penetration rate of HIS is evaluate by hackers, bots or any other mean to evaluate
			2	Partially Penetration	
			3	Complete Penetration	
$[S']_S$ = S System Platform	(W_2) = 4	1-∞	1	Only one Layer	No. of layers used to implementing Identification Schemes including web technology as PHP, ASP, JAVA, etc for designing & deploying of complete system .
			<∞	No. of System layers	
			∞	No. Layers (developed)	
$[C]_S$ =X_1 Complexity	(W_3) = 3	1-5	1	Simplest Level	level of difficulty in implementing of Identification Schemes' deployment of design & development function's factors & layers
			2	Simple Level	
			3	Moderate Level	
			4	High Level	
			5	Highest Level	
$[DB]_A$ =X_2 Database	(W_3) = 3	1-3	1	No DB Availability	Availability of database which will be used to raw functions design identification technique to manage HIS
			2	Partial DB Availability	
			3	Complete DB Availability	
$[T]_S$ =Y_4 Time to response	(W_4) = 2	1-∞	1	Moderate skipping (1-5)	Time taken by server or system to response to user interaction to accept as human or discard as bot Leaving or request for new HIS functions in Sec.
			2	Moderate skipping (7-12)	
			3	High Skipping (>12) Time	
$[A]_A$ = X_3 Layers Automation	(W_3) = 3	1-3	1	No Automation	Level of administrator participation required to manage and schemes maintenance requirement of HIS by automation
			2	Partial Automation	
			3	Complete Automation	
$[US]_U$ =X_4 Understand Rate	(W_4) = 2	1-5	1	Very Difficult	Level of understanding ability of human user while user interact with HIS user interface
			2	Difficult	
			3	Medium	
			4	Easy	
			5	Very Easy	
$[RR]_U$ =X_5 Recognition Rate	(W_5) = 1	1-3	1	No Recognition	User response level after understanding HIS by using experience, knowledge and remembrance level of user
			2	Partial Recognition	
			3	Complete Recognition	
$[TI]_U$ =Y_3 Time to Interact	(W_4) = 2	1-∞	1	Moderate time (1-10)	Time required to solve HIS Tasks & to get response from HIS server in seconds.time taken by user to interact with identification schemes including time required to understand the way of interaction style
			<	Less than (5 in min)	
			∞	Time Limit (5-10) in Minutes	
$[SR]_U$ =Y_2 Skip Rate	(W_4) = 2	1-3	1	Low Skipping (0-6) Time	no. of time user skips or rejecting HIS due to hard difficulty or complex to recognize
			2	Moderate skipping (7-12)	
			3	High Skipping (>12) Time	
$[SR]_U$ =V Success Rate	(W_5) = 1	0-1	0	No Success	percentage of success for human while trail to gain access from HIS get access to secured services
			1	Complete Success	

B. Grading a Classification

In grading we Classify HIS as Full Interactive, Hybrid Interactive and Non-Interactive. To calculate HIS score , we have criteria as shown in table 5, but few HIS's criteria are never fits into static rubric due to several limitations and difficulties to gain accurate data from server and administrator interaction, so some information assumption is made regarding sever automation system and administrator interactions.

VII. DATA ACQUISITION

Initially we had a set of several promising examples for Identification & Registration technique to differentiate humans from bots, as listed full and hybrid identification schemes in table 6 and non interactive identification schemes in table 7. In retrospect, some of these are websites of HIS provider, some are names of identification schemes and some are methods and Ideas, that proved more efficient than others. The main problem is that several criteria proved to be intrinsically not well separated from each other. Regardless of how we obtained a putative partitioning of the users into humans and bots, there was always considerable overlap between different identification techniques as Multifactor HIS so several assumption are taken in consideration.
Table 6 shows full and hybrid interactive type schemes with technique used with examples. Surveyed from websites and Research papers as follow.

Table 6 : Full and Hybrid HIS Examples

Type	Techniques By	Examples
Full Interactive	Task	peoplesign.com, keycaptcha.com , Captcha ,Arbitrary Instruction, etc.
	Puzzles	areyouahuman , Trivia Puzzle, etc.
	Questions	bestwebsoft , MathGuard , etc.
	AI Questions	VouchSafe, Textcaptcha , Skill Testing, Zhang's CAPTCHA [30]
	Small Games	Sweetcaptcha ,tic-tac toe game, etc.
	Multi factor HIS	Identipic, etc.
	System Tasks	minteye, slider DISTCHA , Drag & Drop CAPTCHA ,
	Confirmation Services	OSE email masking , Google , Yahoo
	Key Tokens Services	Google Via SMS Verification, Temporary Tokens vie Email ,etc.
Hybrid Interactive	Recognition	captcha.net , captchas.net , NuCaptcha ,hellocaptcha.com, phpcaptcha , etc.
	Questions	bestwebsoft.com, Confident Caaptcha
	Puzzles	textcaptcha.com, Math Puzzle , etc.
	AI Questions	areyouahuman.com , Friend recognition
	Multi factor HIS	Theymakeapps, etc.
	User Management	NI-Guardian, Quest IdM , Aveksa , CA Tech IdM , EmpowerIDIdM ,etc.
	User Defined Functions	Escape Output,etc.
	Biometric Data recognition	Face , eye , gesture recognition,etc.
	Centralized Sign-on	OpenID ,Shibboleth , SmartSignin ,Pubcookie ,JOSSO ,SAML ,CoSign single sign on ,OpenAM , Ubuntu Single On , etc.

Table 7 shows Non- interactive type schemes with technique used with examples, that are mostly user observation and interactions proofs shown at server side.

Table 7 : Non Interactive HIS examples

Type	Techniques By	Examples
Non Interactive	Biometric Data Analysis	Typing speed, time to interact & response ,etc.
	User-Agent header	Google Chrome, Firefox, IE,Opera, Safari,etc system use .
	Browser fingerprinting	Google Chrome , Firefox, IE , Opera , Safari,
	Unusual Form Interaction	Confirmation Screens, fields
	Hidden Form Elements	using CSS (cascading style sheets , Honeypot Trap ,
	JavaScript Detection	GrowMap anti-spambot,
	Web Server Management	Automated Banning , Checking Emails and IPs , Third Party Verification , Akismet, Mollom and SBlam
	Bot Response	Detect & Validate content within a hidden form element the submitted

VIII. RESULT

The description of examples given above of the progression of the interactive and non-interactive analysis included only a brief manual part of the whole evaluation process. In addition, we conducted automated as well as manual tests for thresholds that lead to good separations in results. In this section, we summarize the final results of evaluation process.

A. Useful Criteria Classification: Initially we had a set of several promising criteria for differentiate of humans from bots, as listed in table 5. In retrospect, some of these proved more efficient than others. The main problem is that some criteria proved to be intrinsically not well separated. Regardless of how we obtained a putative partitioning of the users into humans and bots, there was always considerable overlap between the two or more than two groups. It proved useful in the grading.

B. Thresholds and Results: The main results of the analysis are summarized from Table 6 and Table 7. The main schemes types used are listed across the table. For several identification schemes, we have the Full, Hybrid & Non interactive type's data collected at server side, admin side & user side. The best thresholds schemes that were found to identify humans and bots, using the full and hybrid interactive schemes are use of User Defined Functions, Biometric Data recognition, Multifactor HIS, AI Questions and Small Games and by using non interactive schemes like JavaScript Detection , Biometric Data Analysis , Bot Response .

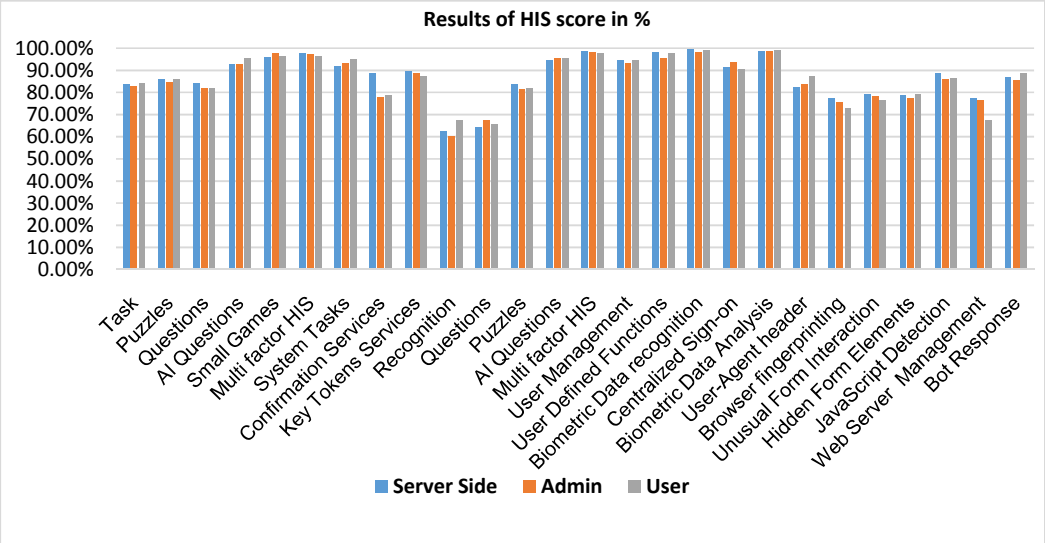

Figure 2 Result of Human I identification Schemes score in Percentage

IX. PROPOSED TECHNIQUE

We propose MARUTI (Multilayer Automated Randomized Reverse Turing Test to Unpropitious Program and Trustable User Isolation) [31] by Multilayering &Merging human identification techniques (HIT) for fusion of advantages & dissolve drawbacks. Which is combination of Interactive and non-interactive approach based on human interaction & observational proofs (HIOPs) for continuous bot detection. Defending system for human users from malicious attacks from abuse computer programs (soft-bots); Iterative &non-interactive process used of refining the thresholds to combine the results of multiple metrics in a mutually consistent manner. After ranking the techniques from highest to lowest, we analyze the combination of two or more techniques from different methods that complement each other's strengths & balance their vulnerabilities

C. Efficiency &Potency

Table 8 shows top Identification Schemes with their result at server side, administrator side and Client side technique used with examples

Table 8 Result of Top Identification Schemes

Type	Techniques By	Server Side	Administrator Side	User Side
FULL & HYBRID	User Defined Functions	98.54	95.38	97.54
	Biometric Data recognition	99.42	98.13	99.02
	Multi factor HIS	98.78	98.19	97.95
	AI Questions	92.67	92.68	95.67
	Small Games	95.84	97.55	96.34
NON	JavaScript Detection	88.94	85.95	86.37
	Biometric Data Analysis	98.94	98.65	98.97
	Bot Response	86.94	85.45	88.94
MARUTI	**Multilayering and Merging**	**99.97**	**99.90**	**99.97**

X. CONCLUSION

In human identification schemes, several techniques of recognition & registration of user identification & authentication are reviewed and surveyed. During our research, we identify several Human Identification Schemes with their overall security & usability score at server, administrator and user side shows their hardness of security wall while defending from several attacks. Therefore, it is concluded that removal of drawbacks from different identification techniques and combining the benefits of different techniques in one scheme will provide higher accuracy to identify human and to provide more security to web services.

ACKNOWLEDGMENTS

We are grateful to Suraj Patil and Sushil Kumar Yadav for proofreading this paper and many valuable comments. Many thanks to Identification, Registration & recognition services providers for making the web Secure

REFERENCES

[1] M. Xie, Z. Wiu and H. Wang , "Humans and Bots in Internet Chat: Measurement, Analysis, and Automated Classification," Networking, IEEE/ACM Transactions on, vol. 19, no. 5, pp. 1557-1571, Oct 2011.
[2] R. U. Rahman, "Survey On Captcha Systems," vol. 3, no. 3, pp. 1-5, june 2012.
[3] V. A. Luis, Manuel Blum and L. John, "Telling humans and computers apart automatically," Communications of the ACM - Information cities, vol. 47, no. 2, pp. 56 - 60 , 2004.
[4] M. moll, S. Y. wang, H. S. Baird and D. P. Lopresti, "A Highly Legible CAPTCHA that Resists Segmentation Attack," in Human Interactive Proofs: Proceedings of the 2nd Int'l Workshop (HIP2005), Verlag: Berlin, January 16-22, 2005.
[5] W. Roman and D. L. Alexander, "PassShapes: utilizing stroke based authentication to increase password memorability," in Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges, New York, NY, USA, 2008.
[6] M. K. Chong and G. Marsden, "Exploring the Use of Discrete Gestures for authentication," in INTERAC09 Proceedings of the 12th IFIP TC 13 International Conference on Human-Computer Interaction, Verlag Berlin, Heidelberg, 2009.
[7] MIT Media Lab; E15-392; 20 Ames St;, "Building HAL: Computers that sense, recognize, and respond sense, recognize, and respond," MIT Media Lab TR 532; Appears in Society of Photo-Optical Instrumentation Engineers. Human Vision and Electronic Imaging VI,, vol. VI, no. IS&T/SPIE9s Photonics West 2001, p. 20, 2001.
[8] F. I. Ibrahim, Y. Llker and B. S. Yucel, "Designing Captcha Algorithm: Splitting And Rotating The Images Against Ocrs," in International Conference on Convergence and Hybrid Information Technology, Daejeon / South Korea, 2008.
[9] M. moll and S. Y. Wang, "ScatterType: a Legible but Hard-to-Segment CAPTCHA," in IAPR 8th Int'l Conf. on Document Analysis and Recognition (ICDAR2005), Seoul, Korea, August 31 - September 1, 2005.
[10] J. Bentley, "Implicit CAPTCHAs," in IS&T/SPIE Document Recognition & Retrieval XII Conf, San Jose, CA,, January 16-22, 2005.

[11] G. Moy, N. Jones and C. Harkless , "Distortion estimation techniques in solving visual CAPTCHAs," in Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference, Washington, DC, 27 June-2 July 2004.
[12] A. A. Chandavale, A. M. Sapkal and R. M. Jalnekar, "Algorithm To Break Visual CAPTCHA," in International Conference on Emerging Trends in Engineering and Technology,ICETET-09, Nagpur, Maharashtra, India , 16th to 18th December 2009 .
[13] H. Gao, H. liu, D. yao, X. Liu and U. Aickelin, "An Audio CAPTCHA to Distinguish Humans from Computers," in Third International Symposium on Electronic Commerce and Security ISECS '10, Washington, DC, USA, 2010.
[14] El Ahmad, A.S. , Wai-Yin Ng and Yan, J., "CAPTCHA Design: Color, Usability, and Security," Internet Computing, IEEE, vol. 16, no. 2, pp. 44-51, March-April 2012.
[15] T. Farnaz and M. Maslin, "A Survey on Recognition Based Graphical User Authentication Algorithms," International Journal of Computer Science and Information Security, vol. 6, no. IJCSIS November 2009, pp. 119-127, November 2009,.
[16] M. Rao and S. Yalamanchili, "A Framework for Devanagari Script-based Captcha," International Journal of Advanced Information Technology, vol. 1, no. 4, pp. 47-57, 2011.
[17] J.-W. Kim, W.-K. Chung and H.-G. Cho, "A new image-based CAPTCHA using the orientation of the polygonally cropped sub-images," The Visual Computer: International Journal of Computer Graphics, vol. 26, no. 6-8, pp. 1135-1143, June 2010.
[18] N. A. Shah and M. T. Banday, "Drag and Drop Image CAPTCHA," in Proceedings of 4th J&K Science Congress 12th to 14th, Srinagar, India, Nov, 2008.
[19] S. S. Shahreza, and M. S. Shahreza, "Multilingual Highlighting CAPTCHA," Information Technology: New Generations (ITNG), 2011 Eighth International Conference on, pp. 447-452, 11-13 April 2011.
[20] T. Yamamoto, T. Suzuki and M. Nishigaki, "A Proposal of Four-Panel Cartoon CAPTCHA: The Concept," Network-Based Information Systems (NBiS), 2010 13th International Conference on, pp. 575- 578, 14-16 Sept 2010.
[21] Jing-Song Cui,, Jing-Ting Mei,, Wu-Zhou Zhang, and Xia Wang, Da Zhang, "CAPTCHA design based on moving object recognition problem," in Information Sciences and Interaction Sciences (ICIS), 2010 3rd International Conference on, June 2010, 2010.
[22] Y. Xu, G. Reynaga and S. Chiasson, "Security and Usability Challenges of Moving-Object CAPTCHAs: Decoding Codewords in Motion," in USENIX Security '12, Bellevue, WA, August 8-10 2012.
[23] H. Eiji and C. Nicolas, "Use your illusion: secure authentication usable," 4th. Symposium on Usable Privacy Pittsburgh, PA USA, vol. 4, pp. 35-45, july 2008.
[24] G. Mori and J. Malik, "Recognizing objects in adversarial clutter: break-ing a visual captcha," in IEEE Conference on Computer Vision and Pattern Recognition, http://www.cs.sfu.ca/~mori/research, October 11, 2007.
[25] N. A. Shah and T. B. M, "Drag and Drop Image CAPTCHA," in Proceedings of 4th J&K Science Congress 12th to 14th Nov, 2008, University of Kashmir,, Srinagar, India, 2008.
[26] R. V. Yampolskiy, "AI-Complete CAPTCHAs as ZeroKnowledge Proofs of Access to an Artificially Intelligent System," International Scholarly Research Network Artificial Intelligence, p. 6, 10 september 2012.
[27] J. a. C. L. F. Barr, "AI Gets a Brain," ACM Queue, vol. 4, no. 4(4), p. 24{29, 2006.

[28] T. Farnaz and M. Masrom, "A Survey on Recognition-Based Graphical User Authentication Algorithms," International Journal of Computer Science and Information Security, IJCSIS, pp. 119-127, USA Vol. 6, No. 2, pp. , , November 2009.
[29] O. Duskin and D. G. Feitelson, "Distinguishing humans from robots in web search logs: preliminary results using query rates and intervals," in WSCD '09 Proceedings of the 2009 workshop on Web Search, New York, NY, USA, 2009.
[30] Zhang and Wenjun , "Zhang's CAPTCHA architecture based on intelligent interaction via RIA," in Computer Engineering and Technology (ICCET), 2010 2nd , Beijing, 2010.
[31] Hemprasad Y. Badgujar,” Multilayer Parallel User Authentication System by Optimize Hardware use” SGGSIE & T Nanded , 2013.
[32] Ms.Shaikh Shabnam Shafi Ahmed, Dr.Shah Aqueel Ahmed and Mr.Sayyad Farook Bashir, “Fast Algorithm for Video Quality Enhancing using Vision-Based Hand Gesture Recognition” International journal of Computer Engineering & Technology (IJCET), Volume 3, Issue 3, 2012, pp. 501 - 509, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.