Ботоос хамгаалах загвар систем: MonCaptcha

П. Мөнхтулга*, Ч. Алтангэрэл*
*Монгол Улсын Их Сургууль. Хэрэглээний Шинжлэх Ухаан, Инженерчлэлийн Сургууль.
Мэдээлэл, Компьютерийн Ухааны Тэнхим
tulga_comp@yahoo.com

***Хураангуй*— Монгол улсын өсөн нэмэгдэж буй интернет хэрэглээг даган интернетээр дамжин орж ирэх робот-програмын халдлагаас веб-сайтууд хэрхэн хамгаалагдсан тухай, түүнээс хамгаалах системийг хөгжүүлэх судалгааг харуулна.**

Keywords*— *Бот - Ботнет - Веб робот програм; DOS - DDOS; CAPTCHA - КАПЧА; workflow - үйл ажиллагааны диаграм; ER-modeling - ER-модель; WAMP; MySQL server; PHP; Apache server; MVC;

I. Удиртгал

Монгол улсын интернет хэрэглэгчийн тоо 2013 онд 841100, 2014 онд 1962100, 2015 оны эхний хагас сарын дүнгээр 2121900 болон тогтмол өсөж байна [1].

Интернетийн өсөлтийг дагаж олон төрлийн хортой програмууд гарч ирж байгаа бөгөөд тэдгээрээс хамгаалах системгүй үед интернет урсгалаар дамжин халдварлаж хэрэглэгчдийн системд аюул учруулж байгаа нь вебийн аюулгүй байдлын чухал асуудлуудын нэг юм. Эдгээр хортой програмуудын нэг төрөл нь Бот юм [3].

Интернет халдлагын хор хөнөөл, давтамжийн талаарх дэлхийд антивирусын эсрэг үйлчилгээгээр тэргүүлдэг Касперски, Симантек - ийн тайлангаас дараах үр дүнг дурдав.

Касперски хямд төсөр серверийн үйлчилгээ үзүүлдэг орнуудаас халдлага хийгдэх нь их байгааг тогтоосон бөгөөд [4] интернет хэрэглэгчид нь халдлагад их өртсөн 20 улс орны зургадугаар байранд Монгол улс (38.27%) орсон [4].

2014 оны 4 - р улирлыг 2015 оны эхний улиралтай харьцуулахад ботнетыг хэрэглэсэн DDOS халдлагын урсгал 11% - аар буурсан боловч халдлагын шинж бүхий урсгал илэрсэн улсын тоо 66 - аар өссөн нь [5, 6] Монгол улс Ботын халдлагад өртөх өндөр эрсдэлтэй байгааг харуулж байна. Үүнд интернетийн урсгал дахь халдлагын шинж бүхий хандалт 2015 оны 10 сард 48924, 2015 оны 11 сард 34259, 2016 оны 1 сард 16815, 2016 оны 2 сард 18405 болсон [2] байгаагаас үзэхэд аюул занал учруулах тохиолдол өнгөрсөн онтой харьцуулахад буурсан боловч эргэн нэмэгдэх хандлагатай байна.

Бот нь сүлжээгээр дамжин автоматаар ажил гүйцэтгэх байдлаар сүлжээнд ачаалал учруулдаг хөнөөлт програм [3] бөгөөд түүнээс хамгаалах аргуудын нэг нь Капча юм [7].

Энэхүү судалгааны ажлын зорилго нь ботоос сэргийлэх MonCaptcha системийг хөгжүүлэх юм. Энэхүү өгүүллийн Хэсэг 2 -т холбоотой ажлуудыг, хэсэг 3 -т Системийн ерөнхий архитектур, технологийн талаар тусгасан. Хэсэг 4 -т цаашид хийж гүйцэтгэх ажлыг дурдав.

II. Холбоотой ажлууд

Энэ хэсэгт Капча, түүний төрөл, Монгол веб сайтуудын капча хэрэглээ, Капча сервисийн талаар ерөнхий мэдээллийг оруулав.

A. Монгол веб сайтын Капча хэрэглээний судалгаа

Капча бол "харилцагчаа хүн эсвэл компьютер гэдгийг тогтоодог бүрэн автомат нээлттэй тест" юм [9]. Анх Карнеги Меллон их сургуулийн Жон Лэнгфорд, Николас Ж. Хупер ба Луис Фон Ан нар 2000 онд бүтээсэн [8].

Капча нь зурган суурьт, текст суурьт, 3D, аудио, асуулт суурьт, таавар (puzzle) суурьт гэх мэт ангилалтай [3, 10].

Зур. 1. Капчаны хэлбэрүүд .

Капчаг ихэнхдээ веб сайтын хэрэглэгчээр автоматаар бүртгүүлэх, зохиомлоор санал өгөлтийн түвшинд нөлөөлөх, хэрэгцээгүй сурталчилгаан мэдээллийг илгээх, онлайн санал асуулгад бот халдахаас сэргийлэхэд хэрэглэж байна [11].

Монголын тогтмол үйл ажиллагаа явуулж байгаа 300 сайтын веб хэрэглэгчээр бүртгүүлэх, хэрэглэгчээр нэвтрэх, харилцах хэсэг, санал асуулга өгөхөд Капчаг хэрхэн хэрэглэсэн тухай хүснэгт 2 - т харуулав.

ХҮС I. МОНГОЛЫН 300 ВЕБ САЙТЫН КАПЧА ХЭРЭГЛЭЭ

№	*Хэсэг*	*Капчатай*	*Капчагүй*
1.	Хэрэглэгчээр нэвтрэх	4 (1%)	296 (99%)
2.	Хэрэглэгчээр бүртгүүлэх	7 (2%)	293 (98%)
3.	Харилцах хэсэг[a]	28 (9%)	272 (91%)
4.	Санал асуулга өгөх[b]	2 (1%)	298 (99%)

a. *Мэдээлэл үлдээх, харилцах цонх байна*

b. *Санал асуулгын цонх байна*

Зур. 2. Монголын веб сайтын капча хэрэглээ. *(чартаар)*

Үүнээс дүгнэхэд өнөөдрийн байдлаар Монгол улсын хэмжээнд веб сайтууд ботын халдлагаас хангалттай хамгаалагдаж чадаагүй байна.

Тус сайтуудын олонх нь гадаад улс орны Капча сервис үйлчилгээг ашиглаж байгаа нь цаг хугацаа, зардлыг нэмэгдүүлж байна. Мөн веб сайтуудад хэрэглэгдэж байгаа Капчаг оптик тэмдэг таних арга (OCR) болон бусад аргуудыг ашиглан тайлж, зүй бусаар халдах боломжтой байна [12, 13, 14]. Иймээс дотооддоо байрласан сервертэй, үйлчилгээний урсгал хурдан, хэрэгцээг бүрэн хангах MonCaptcha сервисийг хөгжүүлэх хэрэгцээ байна.

B. Captcha service үйлчилгээ

Фото зургаар сканердаж авсан мэдээллийг оптик тэмдэгт танигч OCR - ийн тусламжтайгаар тоон бичвэрт хийн хөрвүүлдэг. Үүнд зарим фото текст танигдахгүй байх нь элбэг байдаг. Энэ асуудлыг шийдэх дээ OCR програмаар танихгүй зургыг авч Капча - д байршуулан, хүний тусламжтайгаар хялбар, өртөг багатайгаар шийдэж болох юм [11]. Үүнийг анх reCAPTCHA нэвтрүүлсэн бөгөөд давхар ботоос хамгаалдаг, дэлхийд өргөн хэрэглээтэй сервис систем тул уг судалгаандаа загвар болгож сонгон авлаа.

reCAPTCHA сервисийг веб сайтдаа ашиглахдаа дараах үйл ажиллагааг дэс дараалан гүйцэтгэнэ.

1) Хэрэглэгч сервис үйлчилгээг авахын тулд Google - д бүртгүүлнэ, хэрвээ бүртгүүлсэн бол хэрэглэгчийн эрхээрээ reCAPTCHA авах гэсэн дээр дарж орно. [https://www.google.com/recaptcha/admin]

2) Шинэ сайт бүртгүүлэх хэсэгт тайлбар, домейн нэр, электрон шуудангийн хаягийг оруулан бүртгүүлнэ. Үүний дараа site key ба secret key-ийг үүсгэн харуулна.

   site key - нь хэрэглэгчид зориулсан, ил түлхүүр юм.

   Secret key - нь хэрэглэгч сайт болон reCaptcha сервисийн хооронд холбоо тогтооход хэрэглэх бөгөөд аюулгүй байдлын үүднээс нууцлах ёстой түлхүүр юм.

3) Хэрэглэгч веб сайтын клиент ба серверийн талбаруудад reCaptcha сервис үйлчилгээний зааврын дагуу тохиргоо хийнэ.

4) Клиент талын тохиргоонд Капчаг дүрслэх скрифт код ба тагууд хийгдэнэ.

5) Веб сайтын капчаг суурилуулсан формыг ажиллуулахад reCAPTCHA сервертэй холболт хийгдэж хүсэлт илгээн хариуд нь Капча дэлгэц дээр дүрслэгдэнэ.

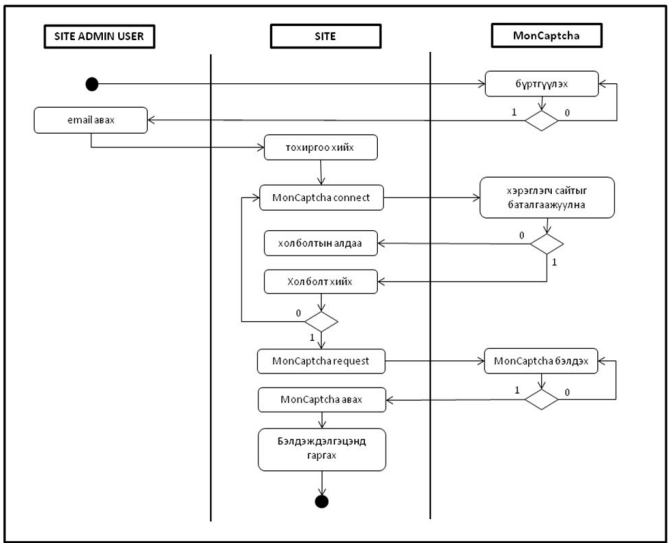
6) Сервер талын тохиргоонд веб сайт, reCAPTCHA хоёрын хоорондын авах, өгөх урсгалын өгөгдлийн боловсруулалтын тохиргоо хийгдэнэ.

III. СИСТЕМИЙН ХЭРЭГЖҮҮЛЭЛТ БА ТЕХНОЛОГИ

Энэ хэсэгт загвар системийг хэрэгжүүлэх ерөнхий архитектур болон технологийн талаар дурдав.

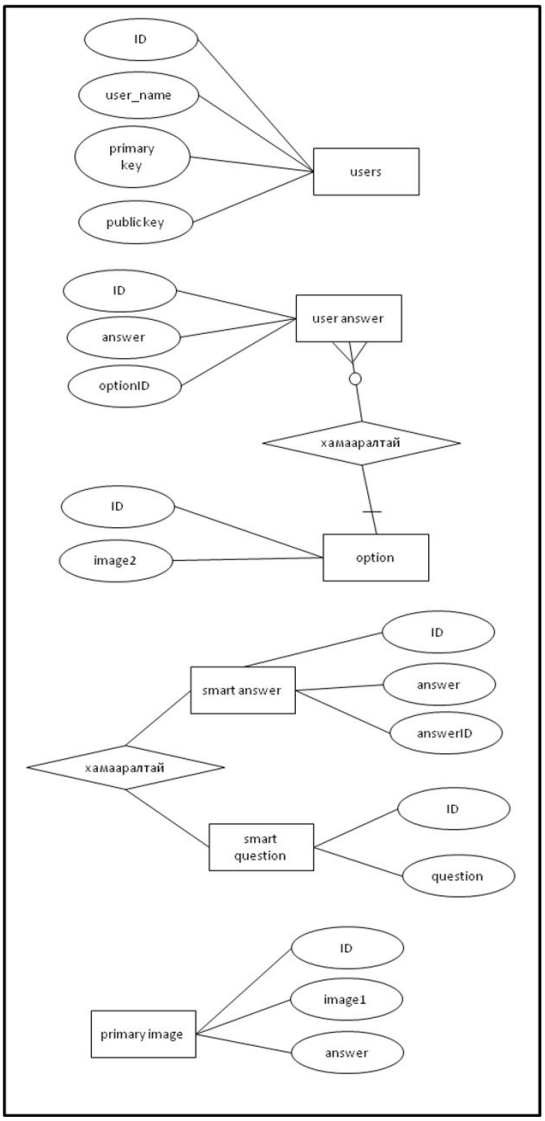
A. MonCaptcha системийн ерөнхий архитектур

Зур 3-д reCAPTCHA системийн үйл ажиллагаанд суурилан загварчилсан MonCaptcha системийн үйл ажиллагааны диаграмыг дүрслэв.



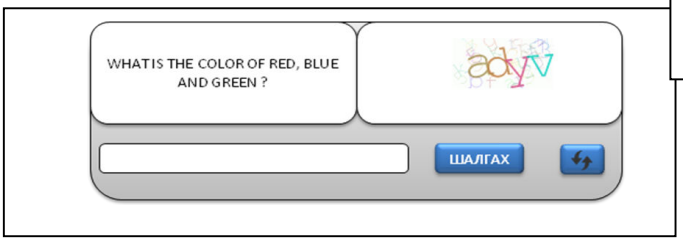
Зур. 3. Үйл ажиллагааны диаграм.

Тус систем нь бүртгүүлэх, баталгаажуулах, Капча бэлдэх гэсэн элементүүдээс бүтэж байна. Зур 4-д системийн өгөгдлийн сангийн ER моделийг харуулав.



Зур. 4. ER-модель.

MonCaptcha системийн хэрэглэгчийн интерфейсийг дараах байдлаар хийв.



Зур. 5. MonCaptcha системийн хэрэглэгчийн интерфейс.

B. Технологи

PHP бол веб хөгжүүлэлтэд зориулагдан хийгдсэн, динамик өгөгдлийн төрөлтэй, сервер талын иж-бүрэн, туршлага сайтай програмчлалын хэл юм [15]. Facebook, Twitter болон бусад сайтууд уг хэлийг сонгон хэрэглэдэг [15] тул PHP хэлийг сонгов.

MySQL нь нээлттэй эх кодтой, өгөгдлийн сангийн менежмент систем бөгөөд кросплатформ програм хангамж юм. Мөн PHP хэл MySQL хэлтэй хослон ажиллах боломжтой [16] ба веб програмчлалд өргөн хэрэглэдэг учир MySQL - ийг сонгов.

WAMP нь өөртөө SSL, SQLite, phpMyAdmin зэргийг нэгтгэсэн бөгөөд серверийн програм хангамжийн шаардлагад Apache веб сервер, MySQL өгөгдлийн сан, PHP сангууд хэрэгтэй учраас Windows үйлдлийн системд зориулсан WAMP програм хангамжийг сонгон хэрэглэв [17].

Модель-Харагдац-Удиртгал (MVC) нь програм хангамжийн архитектур бөгөөд програм хангамжийн инженерчлэлд ашиглагддаг загвар юм [12]. Иймээс MonCaptcha системийн програмчлалд MVC архитектурыг сонгов.

IV. Үр дүн

Системийн хэрэгжээд байгаа хэсгүүдээс дурдав.

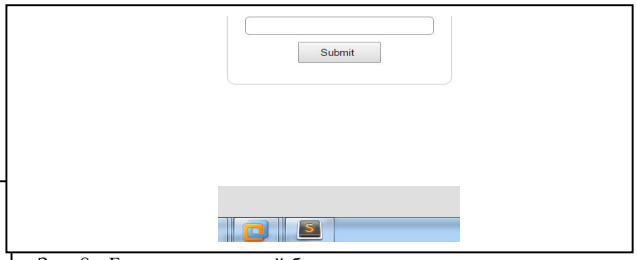
1. Зур 6-д хэрэглэгч бүртгүүлэх хэсгийн интерфейсийг тавив.

Зур. 6. Хэрэглэгч бүртгүүлэх цонх.

2. Зур 7-д Хэрэглэгч амжилттай бүртгэгдсэнийг харуулах мессеж.

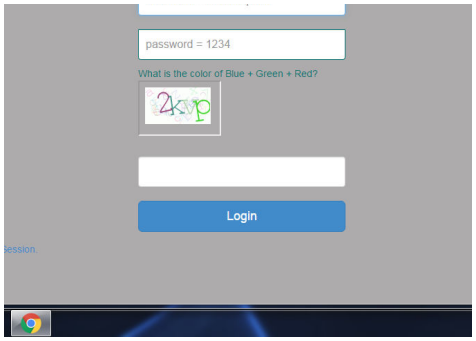
Зур. 7. Амжилттай бүртгэгдсэн мессеж.

3. Зур 8-д хэрэглэгч амжилтгүй бүртгүүлсэн үед гарах мессеж.



Зур. 8. Бүртгэл амжилтгүй болсон мессеж.

4. Зур 9-д хэрэглэгчийн веб сайт дээр Капча гарч ирж байгаа нь.



Зур. 9. Хэрэглэгч сайтын капча хэрэглэсэн форм.

V. ДҮГНЭЛТ БА ХӨГЖҮҮЛЭХ АЖИЛ

MonCaptcha системийн хөгжүүлэх шалтгаан, холбоотой ажлууд болон системийн ерөнхий архитектуруудыг тайлбарлав. Програмчлалын мөр код нь 3300 болоод байна. Загвар хувилбарын хувьд хэрэглэгч бүртгэх хэсэг нь хэвийн ажиллагаатай болсон, бүртгүүлэх мэдээллийг шалгах хэсэг хийгдсэн ба бүртгэл амжилттай хийгдэж байна. Харин одоогоор хэрэглэгчид очих түлхүүрийг гараар оноохдоо тусгай санг ашиглаж үүсгэж байна.

Ойрын ирээдүйд дараах ажлыг хийхээр төлөвлөж байна.

- Програмчлалын кодыг MVC архитектураар хөгжүүлэх
- Загвар системийн хэрэглэгчийн түлхүүрийн модулийг бүрэн ажилд оруулах
- Капча үйлчилгээний модулийг хөгжүүлэх
- Хэрэглэгчид мэйл илгээх модулийг хөгжүүлэх
- Шаардлагын дагуу хэрэглэгчид зориулсан тусламжийн хэсгийг хөгжүүлэх
- Загвар хувилбарыг сайжруулах

Уг системийн талаарх санал хүсэлтийг нээлттэй хүлээн авах болно.

Ном зүй

[1] Харилцаа Холбооны Зохицуулах Хороо. Салбарын 2015 оны эхний хагас жилийн үндсэн үзүүлэлтүүдэд. х21-22

[2] Кибер аюулгүй байдлын газар. 2016 оны 2-р сар. http://www.ncsc.gov.mn/index.php?id=132

[3] Ved Prakash Singh, Preet Pal "Survey of Different Types of CAPTCHA", in International Journal of Computer Science and Information Technologies, Vol. 5, 2014.

[4] Report. Kaspersky security bulletin 2015. Kaspersky Labortory. pp65-66

[5] Статистик DDOS-атак с использованием ботнетов в первом квартале 2015 года. Лаборатория Касперского. июнь 1, 2015

[6] Symantec. ISTR Appendices, VOLUME 21, APRIL 2016

[7] Xiao Ling-Zi and ZHANG Yi-Chun "A Case Study of Text-Based CAPTCHA Attacks," in International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 2012.

[8] Wei-Bin Lee, Che-Wei Fan ,Kevin Ho, Chyi-Ren Dow , and "A CAPTCHA with Tips Related to Alphabets Upper or Lower Case," in Seventh International Conference on Broadband, Communication, Wireless Computing and Applications, 2012.

[9] Baljit Singh Saini and Anju Bala "A Review of Bot Protection using CAPTCHA for Web Security," IOSR Journal of Computer Engineering, 2013, pp. 36-42, 2013.

[10] Kumary R Soumya, Rose Mary Abraham and Swathi K V "A Survey on Different CAPTCHA Techniques", International Journal of Advances in Computer Science and Technology, Vol. 3, February 2014.

[11] Luis von Ahn, Benjamin Maurer, Colin McMillen, "reCAPTCHA: Human-Based Character Recognition via Web Security Measures", in Computer Science Department, Vol. 321., 2008.

[12] Bartosz Porebcki, Karol Przystalski, Leszek Nowak., "Building PHP Applications", 2011.

[13] Gursev Singh Kalra, "Attacking CAPTCHAs for Fun and Profit", in McAfee An Intel Company, 2012.

[14] Jayshree Ghorpade, Shamika Mukane, Devika Patil., "Novel Method for Graphical Passwords using CAPTCHA", in International Journal of Soft Computing and Engineering, Vol. 4, November 2014.

[15] Wikipedia The Free Encyclopedia, https://en.wikipedia.org/wiki/PHP

[16] Wikipedia The Free Encyclopedia, https://en.wikipedia.org/wiki/MySQL

[17] Wang Nina, "Building the WAMP Platform", in Mikkeli University of Applied Sciences, 2011.