# Web Attack Detection Based on ResNet and RNN

Xin Chen
Hanyang University
Ansan-si, Korea 15588
xxtx0122@hanyang.ac.kr

Zhiqiang Wu
Hanyang University
Ansan-si, Korea 15588
wzq0515@hanyang.ac.kr

Scott Uk-Jin Lee
Hanyang University
Ansan-si, Korea 15588
scottlee@hanyang.ac.kr

## ABSTRACT
Web attack detection is an important part of web security. As our society already depends heavily on web technologies, web attacks can actually cause serious problems such as economic losses, data leakage, business interruption and even attacks on Internet of Thing devices that affect personal and social security. In order to prevent such disasters, we propose a web attack detection approach based on ResNet and Gate Recurrent Unit (GRU). In this approach, Word2vec is used to extract features of HTTP request URL with which detection model is trained using ResNet and GRU. As a result, our approach can greatly improve model training speed and web attack detection accuracy and recall.

## CCS Concepts
**• Security and privacy→Web protocol security • Computing methodologies→Neural networks.**

## Keywords
Web security; Web attack detection; convolutional neural network; ResNet; recurrent neural network; gated recurrent unit.

## 1. INTRODUCTION
With the rapid developments of Internet and web technologies, web applications became an essential part of our daily lives. In particular, web-based cloud storages became very popular nowadays, resulting a large amount of personal information to be stored on the cloud. Such personal data on the cloud can be very venerable as a simple web attack, such as injecting malicious code into the web, can be used to steal the data.

Hence, detecting a possible web attack is very important to prevent such an unintended personal data access. Currently, there are two popular methods, signature-based and anomaly-based, to detect web attacks [1]. Signature-based method detects web attacks by looking for known attack strategies whereas anomaly-based method sets up a normal request library to compare and filter out anomaly request. However, there are drawbacks to these methods where improvement can be made to better detect web attacks. Although evaluation from various research indicates the signature-based method to be efficient in detecting web attacks with higher accuracy and lower false alarm rate, it cannot detect unknown type of web attack. In other words, signature-based method cannot provide effective protection for the web server and personal data when the new type of web attack approaches comes [2]. Anomaly-based method has high false positive rate in filtering anomalous requests from normal ones and it also consumes more time detecting web attacks [3].

In recently years, deep learning technology especially in feature representation and classification has developed rapidly. Among them, Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) are extended from traditional neural network (NN) to have better support for system overheads. As a result, CNN and RNN have wider adaptability where they are applied to more research fields including web attack detection.

In this paper, we propose an approach to detect web attacks using ResNet [4] and Gate Recurrent Unit (GRU) [5]. ResNet is a classical model in CNN where gradation vanish will not occur with the deepening of the neural network when compared with other CNN models. GRU is a neural network used to process sequential data. In the proposed approach, the features of URLs are retrieved by regular expressions with tokens and converted into URL vectors using Word2vec technique. Then request URLs with normal behavior are fed to the ResNet and GRU models to train and obtain normal URL features strategy. The combination of ResNet and GRU models are used to prevent decreasing of detection accuracy caused by the increased layers of neural network. In addition, the proposed approach no longer limits the detection to the known types but enables variants of web attacks to be detected.

The remainder of the paper is organized as follows. Section 2 describes the related works. Section 3 outlines the overall architecture of our approach and provides detailed explanation of each stage involved in this approach. In section 4, we conclude our work and discuss possible further works.

## 2. RELATED WORK
Kruegel et al. [6] proposed a first attempt in using anomaly detection method to detect web attacks with HTTP queries containing parameters as input. The proposed system learns parameter characteristics (such as length and structure) from input data. But this detection method has limitations on the HTTP request type and string length.

Valeur et al. [7] also proposed an anomaly-based detection system that use many different models to learn profiles for normal database access performed by web application. These models train and learn normal SQL query profiles to distinguish whether a SQL query is normal or not. This detection system can detect unknown attack and has less overhead. In addition, these models reduce the chances of simulation attack based on SQL.

Shon et al. [8] presented an anomaly intrusion method to detect zero-day attack based on Support Vector Machine (SVM). Due to the high false positive rate of SVM, they propose a new SVM approach with soft-margin SVM and one-class SVM combined. The proposed approach provides unsupervised learning and low false alarm capability.


DOI: http://dx.doi.org/10.1145/12345.67890

Mac et al. [9] used autoencoder to detect malicious pattern in the HTTP/HTTPs request. They have used unsupervised learning without label but the performance, in terms of precision, recall and F1-score, is lower than RNN. Liang et al. [1] proposed an anomaly detection approach for detecting web attacks where RNN model is used for learning patterns of normal requests to distinguish normal request from anomalous.

Wang et al. [10] explored various deep learning methods for web attack detection and evaluated CNN, long-short term memory and their combined method. Their method resulted in decreasing precision of CNN with an increase of neural network layers.

Although the current research has already achieved high accuracy on web attack detection based on HTTP requests, existing methodologies cannot provide flexibility in raw input length and excellent performance. Therefore, we propose an improved approach to detect potential web attacks from HTTP requests URLs.

# 3. PROPOSED APPROACH

In this section, we first introduce the overall process of our approach as shown in Figure 1. For test and evaluation of our approach, CSIC 2010 dataset [11] are used as a benchmark for our experiment. The CSIC 2010 involve various web attacks such as SQL injection, Cross-site scripting, CRLF injection, and parameter tampering.

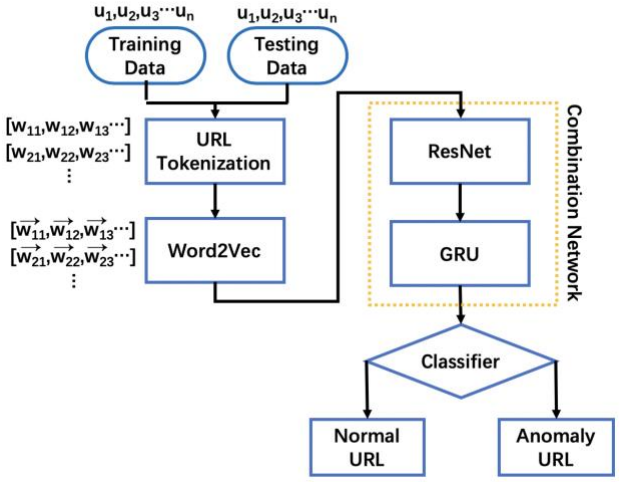


**Figure 1. The overall Process of Web attack detection**

We divided the CSIC 2010 dataset into two parts where 90% of dataset is used for training and rest 10% is used for testing. Initially, all query parameter inputted from end-users are replaced by a series of specific tokens. Word2Vec is applied next to convert each tokenized vector of query parameters into a numerical vector for deep learning network. Then, RestNet generates refined query parameters where GRU will predict the data type of query parameter to verify the consistency against the actual inputted data type from users. If the predicted and actual data type does not match, the corresponding URL are considered as an anomalous URL with potential attacks.

## 3.1 URL Tokenization

In order to extract the features of query parameters from URLs, all URLs collected from dataset are tokenized where query parameters of suffix URL are replaced by tokens. The tokenized set of URLs is formally represented as $U = \{u_1, u_2 \cdots u_n\}$, where $U$ is URL and $u_i$ is the $i_{th}$ URL. After the tokenization procedure, the below representation is obtained.

$W := [\ [w_{11},w_{12},w_{13}\cdots], [w_{21},w_{22},w_{23}\cdots],\cdots]$

The $W$ denotes the structure information of the query parameters within which each row represents one query parameter [12].

According to features of HTTP request URL, we designed a series of customizing regular expression. The regular expressions are used in the input data tokenization as shown in Table 1 below.

**Table 1. The URL request tokenization method**

| Tokenization | example |
|---|---|
| Change all letters into lower case | http://aa.com |
| Replace numerical query parameter with <NV> | http://aa.com/query.php?id=<NV> |
| Replace string query parameter with <SV> | http://aa.com/query.php?id=<NV> &email=<SV> |
| Insert <START> token at the beginning of the URL | <START>http://aa.com/query.php ?id=<NV>&email=<SV> |
| Insert <END> token at the end of the URL | <START>http://aa.com/query.php ?id=<NV>&email=<SV><END> |

## 3.2 Word2Vec

In this step, Word2Vec technique [13] is applied to convert URL tokens into URL vectors to be used as an input for deep learning model where natural language is transformed into one-hot vector. Through such step, URL tokens are transferred into URL feature vectors. Then, these URL vectors are fed into ResNet and GRU models for training the classifier of anomaly URLs.

Word2Vec provides two models to train word vectors, Continuous Bag of Word (CBOW) and Skip-Gram models, which can carry out the single-layer neural network of lexical association prediction. In this paper, we applied CBOW to predict possible words based on the context of the target word. The training flow chart of CBOW is shown in Figure 2.

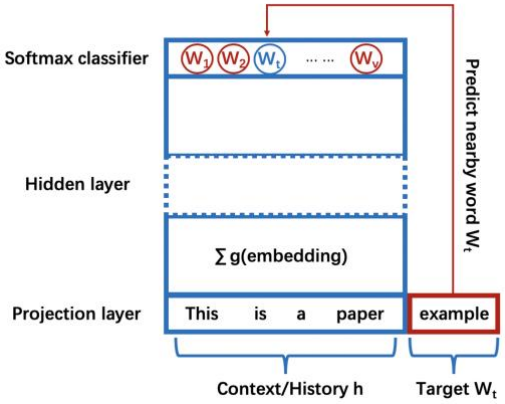


**Figure 2. The training flow chart of CBOW**

## 3.3 ResNet

ResNet (Residual Neural Network) was proposed by He et al. from Microsoft research institute [4] to support more layer of neural network without gradient vanish. ResNet also accelerates the training of neural network quickly, and recently the accuracy of the model has been greatly improved [14].

The aim of ResNet is to set a connection between $x$th layer and the $(x+i)$th layer network. The conventional neural network structure

such as CNN is to perform a nonlinear transformation. Meanwhile, ResNet allows the raw input information to be directly transmitted to the next layer of neural network. The structure of ResNet is as shown in Figure 3.

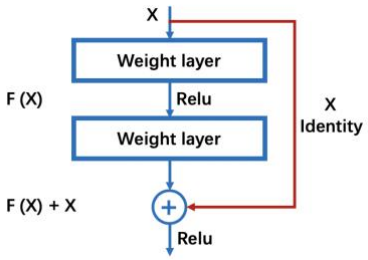


**Figure 3. The ResNet network structure**

In this approach, we apply ResNet to refine features of URL vector. Even in deep layers of neural network, the model can still provide good accuracy for refining features of URL.

## 3.4 Gated Recurrent Unit

Gated Recurrent Unit (GRU) is a kind of RNN without gradient descent issue [15]. This issue leads to lower memorization ability of RNN. In order for information of RNN to be memorized over more stacked layers, the structure of RNN is changed to GRU. GRU enables information to flow directly from the last layer to the current layer without continuous matrix action. The GRU model structure is shown in Figure 4.

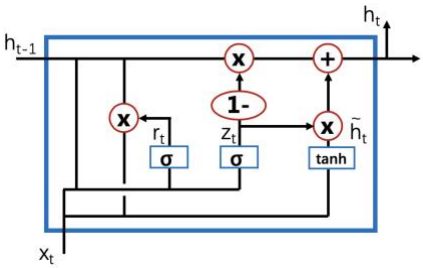


**Figure 4. The structure of GRU model**

In this paper, the GRU is used to predict the final result for each query parameter. If the predicted token is same as the raw input, we consider current query parameter as a normal behavior. Otherwise, it is considered as an anomalous query parameter. The current URL may contain multiple query parameters. Thus, the URL will be determined as normal when all tokens of query parameters in URL are same as the predicted result.

# 4. CONCLUSION

In this paper, we proposed an improved approach to detect web attacks using ResNet and GRU. We used the URLs to detect whether the HTTP requests are anomalies. ResNet and GRU are applied to predict the current result of URL query. If the result of prediction is different from the current query parameter, the query will be determined as anomalous request. Moreover, an URL may consist of multiple query parameters in the suffix of absolute path. If any query parameter is detected as anomaly, the URL will be determined as anomaly and considered as potential attacks. Meanwhile, our approach can convert arbitrary length of HTTP requests without any limitation by using two neural network models. With the use of ResNet, the accuracy will not be decreased as the layer of neural network increases. This approach can effectively improve Web attack detection accuracy and recall.

As a future work, we will create an actual implementation of this model and conduct further optimization. The CSIC HTTP dataset will be used to train the model and test the web attack detection efficiency and accuracy.

# 5. ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP) (No. NRF-2016R1C1B2008624).

# 6. REFERENCES

[1] Liang, J., Zhao, W. and Ye, W. 2017. Anomaly-Based Web Attack Detection: A Deep Learning Approach. In *Proceedings of the 2017 VI International Conference on Network*, Communication and Computing, 80-85. ACM.

[2] Tekerek, A., Gemci, C., & Bay, O. F. 2014. Development of a hybrid web application firewall to prevent web based attacks. In *2014 IEEE 8th International Conference Application of Information and Communication Technologies* (AICT), 1-4. IEEE.

[3] Gao, Y., Ma, Y., & Li, D. 2017. Anomaly detection of malicious users' behaviors for web applications based on web logs. In *2017 IEEE 17th International Conference on Communication Technology* (ICCT), 1352-1355. IEEE.

[4] He, K., Zhang, X., Ren, S. and Sun, J. 2016. Deep residual learning for image recognition. In Proceedings of the *IEEE conference on computer vision and pattern recognition*, 770-778. IEEE

[5] Nallapati R, Zhai F, Zhou B. 2017. Summarunner: A recurrent neural network based sequence model for extractive summarization of documents. In *Thirty-First AAAI Conference on Artificial Intelligence*.

[6] Kruegel C. and Vigna G. 2003. Anomaly detection of web-based attacks. In *Proceedings of the 10th ACM conference on Computer and communications security*, 251-61. ACM.

[7] Valeur F., Mutz D. and Vigna G. 2005. A learning-based approach to the detection of SQL attacks. In *International Conference on Detection of Intrusions and Malware*, and Vulnerability Assessment, 123-40. Springer.

[8] Shon, T., and Moon, J. 2007. A hybrid machine learning approach to network anomaly detection, *Information Sciences*, 177(18): 3799-821.

[9] Mac, H., Truong, D., Nguyen, L. and Nguyen, H. 2018. Detecting Attacks on Web Applications using Autoencoder. *In Proceedings of the Ninth International Symposium on Information and Communication Technology*, 416-21. ACM.

[10] Wang, J., Zhou, Z. and Chen, J. 2018. Evaluating CNN and LSTM for Web Attack Detection. In *Proceedings of the 2018 10th International Conference on Machine Learning and Computing*, 283-87. ACM.

[11] Giménez, C.T., Villegas, A.P. and Marañón, G.Á. 2010. HTTP data set CSIC 2010. *Information Security Institute of CSIC (Spanish Research National Council)*.

[12] Yong, B., Liu, X., Liu, Y., Yin, H., Huang, L. and Zhou, Q. 2018. Web Behavior Detection Based on Deep Neural Network. In *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*

(SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 1911-16. IEEE.

[13] Mikolov, T., Chen, K., Corrado, G. and Dean, J. 2013. Efficient estimation of word representations in vector space. *arXiv preprint arXiv:1301.3781*.

[14] Fang, Y., Li, Y., Liu, L. and Huang, C. 2018. DeepXSS: Cross Site Scripting Detection Based on Deep Learning. In *Proceedings of the 2018 International Conference on Computing and Artificial Intelligence*, 47-51. ACM.

[15] Fu Y., Lou F., Meng F., Tian Z., Zhang H. and Jiang F. 2018. An intelligent network attack detection method based on rnn. In *2018 IEEE Third International Conference on Data Science in Cyberspace* (DSC), 483-89. IEEE.