Dynamic access control and security performance prediction for IoT networking using a novel deep learning technique

Sriramya P. (sriramyaphd2021@gmail.com)
Saveetha School of Engineering
A.K. Reshmy
BS Abdul Rahman Institute of Science and Technology: B S Abdur Rahman Crescent Institute of Science & Technology
R. Subhashini
Sathyabama Institute of Science and Technology
Korakod Tongkachok
Thaksin University
Ajay Prakash Pasupulla
Wachemo University
Yousef Methkal Abd Algani
The Arab Academic College for Education in Israel
S. Balaji
Panimalar Engineering College
B.Kiran Bala
K Ramakrishnan College of Engineering

Research Article

Keywords: Access control, performance prediction, big data, Deep learning, security, IoT

Posted Date: October 7th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-947700/v1

Abstract

Internet of things (IoT) has increased an importance for an area of interest in many devices. Then, the applications such as sensitive home sensors, medical devices, wireless sensors,and other devices are related to IoT network. The transmission of big data is subject to a possible attack that could cause network interruptions and problems with security. The security performance prediction is important for IoT networks to address complicated security issues in real-time which one of the attacks can freely threaten its global performance. Initially,investigate the safety performance of security intelligent prediction techniques is linking with deep learning algorithms into the IoT security risks. This contribution provides a CNN model that improves IoT security risk assessment (SRA) performance. Then, the access control techniques are changed with IoT-like dynamic systems with the number of items spread all over the place. Therefore, dynamic access control models are necessary. Thesedesign not individual use strategies of access but incorporate environmental and real-time data to predict the decision on access. The risk-based access control approach is one of those dynamic models. To decide the access decision, this model assesses the security risk value associated with the access request. This assessment of the model proposed results from the performance and accuracy of IoT networks.

1. Introduction:

The internet of things (IoT) security has generated special issues, because devices are unique in identifying, intelligent for analysis of data, for decision making, and for networking that allows for internet connectivity. Communications can be based on the nature of IoT is done without privacy and authenticity, putting it exposed to assaults (Al Hayajneh, Bhuiyan, and McAndrew 2020). The firewalls and the detection systems in a network edge are traditional ways for network protection to avoid external attacks. However, these defense mechanisms do because of their special characteristics not deal with IoT networks directly. Topics constitute system users requesting access to these resources. Access choice whether to allow or refuse access is based on rules. Access control aims mainly at preventing unwanted users from being able to access a given device and to decrease authorized user's tasks. It also inhibits actions that can lead to a violation of the security (H. F. Atlam et al. 2020).

The risk-based access control model is among the dynamicmethodsare used to make decisions on access with the security risk value related with individually access request. These are various advantages over current approaches in a risky access control paradigm. The ultimate objective of the risk-based access control design is to develop a structure to encourage the distribution of information to improve the benefits of the organization, while also holding users accountable for their operations and stopping any anticipated damages caused by sensitive information releases(H. F. Atlam et al. 2017). However, because every linked item is exposed to security violations, IoT is extremely susceptible. Its fundamental features are virtualization, linkage, diffusion, and heterogeneity expose that to a variety of hazards to physical. Then, the intangible safety concerns are spam, data theft, DoS/DDoS and havens as an attractive target (Xu et al. 2021).

There are SRA methodologies and standards, but mainly a biased procedure is carried out to analyze the security profile of essential equipment. The success of SRA should also be taken into account, in particular, because of the accuracy of risk data(Nurse, Creese, and De Roure 2017). Risk factors were gathered and analyzed for the construction of the risk-based access control design. In addition, risk assessment approaches were identified for assessing safety risks. Our research thereby promotes the improvement of IoT security through the use of deep learning techniques. Deep learning is not a new model. It is an artificial intelligence machine learning subfield. Deep learning helps you to classify texts, imagery, and sound immediately(Al-Garadi et al. 2020). At present, deep learning empowers the IT environment mostly through the resolution of several difficulties and it improves security performance.

The aim of the research to improve the dynamic access control and security performance of IoT network; this study has four sections; the section second examines highlight of the previous effort that can be done by the scholars in this domain with the various experimental tasks; the section third will describe the model proposed; the section four highlights the experimental study of the research; finally, our conclusion isto provide in the final section.

2. Related Work:

(Ullah et al. 2019) evaluates the combined deep learning method to distinguish the malware-infected files and pirated software through the IoT network. The tensor flow deep neural network is designed to recognize lifted software via source code piracy. To filter noisy data to emphasize the value of individually token as to the plagiarism of the source code, the tokenization and weighing approaches are applied. Google code jam (GCJ) collects the dataset for software piracy investigating. In addition, the deep coevolutionary network serves as the basis of visualization of colour images to discover malicious infections in the IoT network. The results obtained indicate that the significant capability of the system presented to detect IoT cyber safety concerns is greater than the state-of-the-art approach.

(Chen et al. 2018) evaluates the fuzzy deep-learning method known as FDCN is evaluated for detecting the citywide circulation flow. This methodology is based on the theory and profound model of the remaining network. Our main idea is to include fluid image in the DL design to reduce the data effect insecurity. A mode is built for improving traffic flow predictions while examining the longitudinal and sequential connection of traffic flow. As far asknow, that's the first moment that a fluid DL technique is utilized to provide traffic characteristics for predictions of traffic flow. The results showed greater efficiency compared with state-of-the-art methodologies in the proposed methodology to traffic flow prediction.

(Wu et al. 2015) estimates the multi-channel harmonic sinusoidal signals estimation (CSI) combined multi-pitch and the direction-of-arrival (DOA) problem is taken into account. The ESPRIT approach is used to estimate the multi-pitch multiple harmonic frequencies signals are based on subspace approaches, which leverage the invariance property in the time domain. Also, estimates employing the shifting invariance structure in the spatial domain are reported in the DOA based on the ESPRIT approach.

Computationally more efficient is the approach propose based on ESPRIT without 2-D search but performs equally. Also included are an asymptotic DOA performance study and a pitch estimate of the suggested approach. Finally, on synthetic signal and real-life data, the usefulness of the suggested strategy is demonstrated.

Now IoT has more issues than ever before with regards to security is evaluates (Tahsien, Karimipour, and Spachos 2020). Security measures can be added to secure IoT already in place. However, the advancing booms and diverse sorts of attack. Then, their severity are not as efficient in conventional approaches. For the next generation IoT system a strong and updated, the security system is necessary. In machine learning (ML), numerous possible research opportunities have been created to deal with ongoing and future difficulties for IoT, and this is significant technological progress. ML is used as a powerful technique to detect assaults and identify aberrant behavior on intelligent devices and networks. IoT's architecture is explored and the necessity of IoT security in terms of many forms of probable threats is examined following an exhaustive literature analysis of ML. In addition, prospective IoT security solutions based on ML have been introduced and future problems explored.

(Weng et al. 2019)It presents SDN controllers to manage network and SDN applications via arbitrary access utilizing a northbound interface (NBI) programmed configuration. Most of the previous jobs have used resource access restriction authorization systems. On NBI for BENBI-named SDN-based VANET, present a dynamic and scalable access control method. In the suggested approach, regulate network resources dynamically and flexibly by using broadcast encryption (BE) instead of modifying controller sources or updating granularity lists. Using a BENBI prototype. The test results show that the rate of secret key assignmentsis independent of the amount of SDN units designated, which shows that this technique is scalable.

3. Proposed Methodology:

IoT security performance is a vital component of preventative and reactive safety measures is applied over access control for physical, platform, and software layer management. In this research, suggest solving security problems with the CNN algorithm of deep learning(Amanullah et al. 2020). In fact, in various fields of research, CNN has produced incredible findings and dynamic access control models are introduced. Its principal advantage is the capacity to learn hierarchical characteristics from the number of data sets which is attractive to IoT's Security.

3.1 Iot Security Using Deep Learning Method:

The main artifacts of deep learning consist of several parallel layers. These layers mainly include a layer of input, several hidden layers, and a layer of output. They are interconnected with respectively layer by the output of the preceding layer. Deep learning is important to the hidden layers. All of these layer's attention on a specific function to boost the efficiency of some other layer on their deduction. There were different algorithms for deep learning. The most important developments include recurrent neural

networks (RNNs) (Zaremba, Sutskever, and Vinyals 2014), convolutional neural networks (CNN). The main ones are deep networks of stacking (DSNs); restricted Boltzmann machines (RBMs)(Fischer and Igel 2012).

RNNs to verify their use in the detection of objects. It just improved process correctness and did not improve performance so much. Semi-supervised method RBMs for network object detection. However, the precise technique has been minimized, not including previous knowledge. DSN-based intrusion model(Sun et al. 2018). The learning period, has an impact on the performance.

CNN carries two important steps of many layers as classification and extraction. The initial stage extraction uses raw data to automatically study and drain characteristics. It has two fundamental layers are the convolutional layer consists of neurons gathering input layer data; the max-pooling layer that automatically classifies the collected data into sub-sample following a convolution layer. It mostly involves reducing the data collected by the number decrease in convolution layer of features.

The knowledge is carried out via back propagation referring to numerous repetitions of the convolution layers and Max-pooling. The next stage as arrangement which transmits the information to classificatory consists of a single layer is the fully connected layer, which primarily conducts thinking by linking the neurons to one final output. Therefore, the IoT paradigm is related to shown in Fig. 1 allows us to provide an intelligent design to categorizes risks. It contains;

- A new model for the deep learning smart risk assessment
- Organization of the IoT security risk features
- Performance, Assessment, accuracy of the developed method

Our major objective is to build a network of neurons that anticipates IoT safety problems. To achieve this, established a neural network.which models features over time. indeed, the outcome is retained as an input for additional calculation with each training, which results in an intelligent method. This boots the security pattern considerably.Furthermore, existing examine papers don’t support present an advanced SRA design or neither a particular strategy aimed at improving the performance and accuracy. There have been very few efforts to employ deep learning processes to improve SRA performance and accuracy (Kassani et al. 2019). Therefore, provide an innovative CNN based security framework from deep learning method. Security performance and accuracy should be optimized using the proposed model.

3.2 Security Risk-based Access Control In Iot:

The mai features of dynamic access control architectures would be that they analyse just not access to the network but also contextual and dynamic variables gathered also at peroid of an order made when making access choices. This gives you greater flexibility it allows you to respond to different scenarios and conditions when making an access decision. The prospect of damage or harm is sometimes referred to as a risk. It is about an occasionthat could happen in the end and result in losses. The risk is well-

defined as the potential harm that may result from the current action or approximately prospective occasion (H. F. Atlam and Wills 2019). From the standpoint of the security risk associated with data computing is identified as the destruction that adversely affects action and its relevant material, whereas managing risk was its process of gathering and minimizing problems that could outcome in a violation of privacy, honesty, or accessibility of a data scheme(H. Atlam et al. 2017).

In the domain of access control, the SRA is depend on the probability of security breaches as well as the importance of this information which may increase the risk of exposing network resources. The risk-based access control paradigm used security risks as a factor to regulate access for respectively access application(Dubois et al. 2010). This design is based on dynamically assessing the security risk direct relationship for each access request, then deciding whether to allow or refuse access depending on the calculated risk value. The possibility of an occurrence is increased by the significance of that incidence is the most popular mathematical formula for representing risk in a quantitative form.

A security risk-based access control model can be built in several ways. These techniques share certain characteristics with other models. The following are the key components of a Fig. 2 depicts a risk-based access control mechanism. The three major components form the risk-based access control mechanism(Babu and Bhanu 2015). Hazardestimate module received access requests from users, analyses them, gathers the necessary risk factor data, assesses the any identify learning has a risk assessment direct relationship with it. To define against security settings, the determined risk signal is significantly to security policies whether access should be granted or denied. These methodsare used to improve security performance on IoT networks.

4. Result And Discussion:

The cloud infrastructure is used in the selected IoT experimental research. This latter is made up of two-node sensors, one of which serves as a client and the other as a server. A raw log heading file was used to start the extraction process. Indeed, created a model of a typical cloud client-server interaction. The raw data contains 14 attacks such as unauthorized network access, virus incursion, probing assaults, data indignation, stability loss, DoS, and direct attack. To be able to discern the appropriate network limitations, initially it is defined as the CNN structure assmall in size having an input data, neural network layer, and a convolutional layer. As a result, the convolutional layer has divided the input into three categories are content, fundamental and mobility. The max-pooling layer then performed downsampling by dividing the convolutional layer’s output into two sub-samples as normal and abnormal. As a result of the back-propagation was used to update the parameters to learn and optimize its inference. On each layer, five iteration trails have been completed.

This section assesses the findings of our experimental research. The security risks classification is indicated in Fig. 3

The observed performance findings show that when more iterations are completed, more inference is gained, resulting in performance improvement. As a result, noticed that if additional iteration will be

necessary to generate an accurate result when more training data becomes available. Conducting multiple rounds saves CNN time in terms of training and development. Furthermore, show that when back-propagation occurs CNNs perform better. The planned approach appears to be promising and its optimized performance is shown in Fig. 4.

risk classification to measure accuracy. Our given structure has correctly divided IoT's security vulnerabilities to its network layer as demonstrated in the above Fig. 4. standardized the log heading is used as the data set before paper did the training and classification to boost our model speed. Our CNN algorithm has proven to be capable of identifying DoS sufficiently. But mainly because of the huge variation, the proposed model precision is biased. To distinguish the optimal settings, CNNs require several experiments. Indeed, it is highly important to collect a proper dataset to prevent obtaining biased results. The results of this experimental investigation can be used in addition to risk treatment. Indeed, given that deep learning algorithms enable quicker risk classification, the fundamental importance of securing the network layer is evident. A successful risk management approach is an efficient risk assessment.

5. Conclusion:

The use of the CNN deep learning algorithm to the IoT network layers security field has been described in this study. The implementation of CNN is a time-consuming and hard operation. Current access control models give a static approach for different apps to make access decisions. However, contextual and real-time data should rely on a model for access control for a dynamic distributed system. This model can dynamically provide the access decision by estimating the security the risk factor associated with the access request. CNN is applied on SRA has advantageously with the rise of IoT uncertainty diverse structure and undertaken the data large scale. It is used to recognize the DoS outbreaks. This future model provided a better performance accuracy result. The performance of IoT SRA has improved accordingly. However, precision needs to be improved. Overall, findings confirm the more effective evaluation of profound learning of IoT risks.

Declarations

Funding

There is no funding.

Conflict of Interest

This paper has not communicated anywhere till this moment, now only it is communicated to your esteemed journal for the publication with the knowledge of all co-authors.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent

All authors have seen the manuscript and approved to submit it to the journal.

Author contributions

All authors have seen the manuscript and approved to submit it to the journal.

References

1. Al Hayajneh, Abdullah MdZAlam, Bhuiyan, McAndrew I (2020) Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). Computers 9(1):8. https://doi.org/10.3390/computers9010008
2. Al-Garadi M, Ali A, Mohamed AK, Al-Ali X, Du I, Ali, Guizani M (2020) A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Communications Surveys Tutorials* 22(3):1646–1685
3. Amanullah M, Ahzam RAhamedA, Habeeb FH, Nasaruddin A, Gani E, Ahmed, Abdul Salam Mohamed Nainar, Nazihah Md Akim, and Muhammad Imran. 2020. “Deep Learning and Big Data Technologies for IoT Security.” *Computer Communications* 151: 495–517
4. Atlam H, Alenezi A, Walters R, Wills G, and others (2017) “An Overview of Risk Estimation Techniques in Risk-Based Access Control for the Internet of Things.&#8221
5. Atlam HF, Ahmed Alenezi RJ, Walters GB, Wills, Daniel J (2017) “Developing an Adaptive Risk-Based Access Control Model for the Internet of Things.” In *2017 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and Ieee Smart Data (SmartData)*, 655–61. IEEE
6. Atlam HF, Ajmal M, Azad, Madini O, Alassafi AA, Alshdadi, and Ahmed Alenezi (2020) Risk-Based Access Control Model: A Systematic Literature Review. Future Internet 12(6):103. https://doi.org/10.3390/fi12060103
7. Atlam HF, Gary BW (2019) An Efficient Security Risk Estimation Technique for Risk-Based Access Control Model for IoT. Internet of Things 6:100052
8. Babu B, Mahesh, and Mary Saira Bhanu (2015) Prevention of Insider Attacks by Integrating Behavior Analysis with Risk Based Access Control Model to Protect Cloud. Procedia Computer Science 54:157–166
9. Chen W, An J, Li R, Fu L, Xie G, Md Zakirul Alam Bhuiyan, and Li K (2018) “A Novel Fuzzy Deep-Learning Approach to Traffic Flow Prediction with Uncertain Spatial–Temporal Data Features.” *Future Generation Computer Systems* 89 (December): 78–88. https://doi.org/10.1016/j.future.2018.06.021

10. Dubois Éric, Heymans P, Mayer N, Matulevičius R (2010) “A Systematic Approach to Define the Domain of Information System Security Risk Management.” In *Intentional Perspectives on Information Systems Engineering*, 289–306. Springer
11. Fischer A, and Christian Igel (2012) “An Introduction to Restricted Boltzmann Machines”. In: Iberoamerican Congress on Pattern Recognition. Springer, pp 14–36
12. Kassani S, Hosseinzadeh PH, Kassani, Michal J, Wesolowski, Kevin A, Schneider, and Ralph Deters (2019) “Classification of Histopathological Biopsy Images Using Ensemble of Deep Learning Networks.” *ArXiv Preprint ArXiv:1909.11870*
13. Nurse, Jason RC, Creese S, and David De Roure (2017) Security Risk Assessment in Internet of Things Systems. IT Professional 19(5):20–26
14. Sun C, Ma M, Zhao Z, Chen X (2018) Sparse Deep Stacking Network for Fault Diagnosis of Motor. IEEE Trans Industr Inf 14(7):3261–3270
15. Tahsien S, Manjia H, Karimipour, and Petros Spachos (2020) Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey. Journal of Network Computer Applications 161 (July):102630. https://doi.org/10.1016/j.jnca.2020.102630
16. Ullah F, Naeem H, Jabbar S, Khalid S, Latif MA, Al-turjman F, and Leonardo Mostarda (2019) Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach. IEEE Access 7:124379–124389. https://doi.org/10.1109/ACCESS.2019.2937347
17. Weng J-S, Weng J, Zhang Y, Luo W, Lan W (2019) BENBI: Scalable and Dynamic Access Control on the Northbound Interface of SDN-Based VANET. IEEE Trans Veh Technol 68(1):822–831. https://doi.org/10.1109/TVT.2018.2880238
18. Wu Y, Amir L, Jensen JR, and Guisheng Liao (2015) Joint Pitch and DOA Estimation Using the ESPRIT Method. IEEE/ACM Transactions on Audio Speech Language Processing 23(1):32–45. https://doi.org/10.1109/TASLP.2014.2367817
19. Xu L, Zhou X, Tao Y, Liu L, Xu Yu, and Neeraj Kumar (2021) “Intelligent Security Performance Prediction for IoT-Enabled Healthcare Networks Using Improved CNN.” *IEEE Transactions on Industrial Informatics*
20. Zaremba W, Sutskever I, and Oriol Vinyals (2014) “Recurrent Neural Network Regularization.” *ArXiv Preprint ArXiv:1409.2329*

Figures

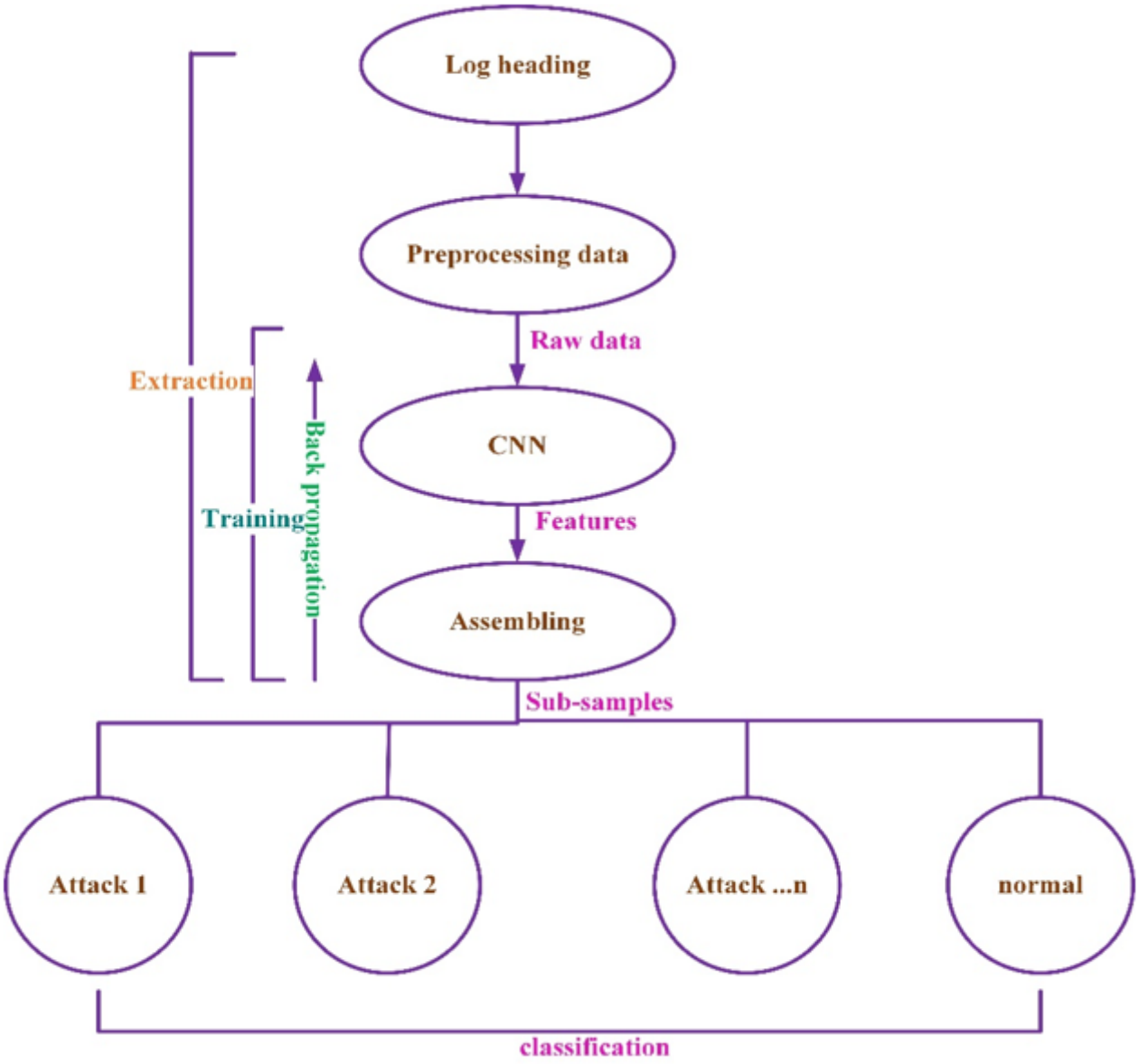

Figure 1

overview of the model using a deep learning approach

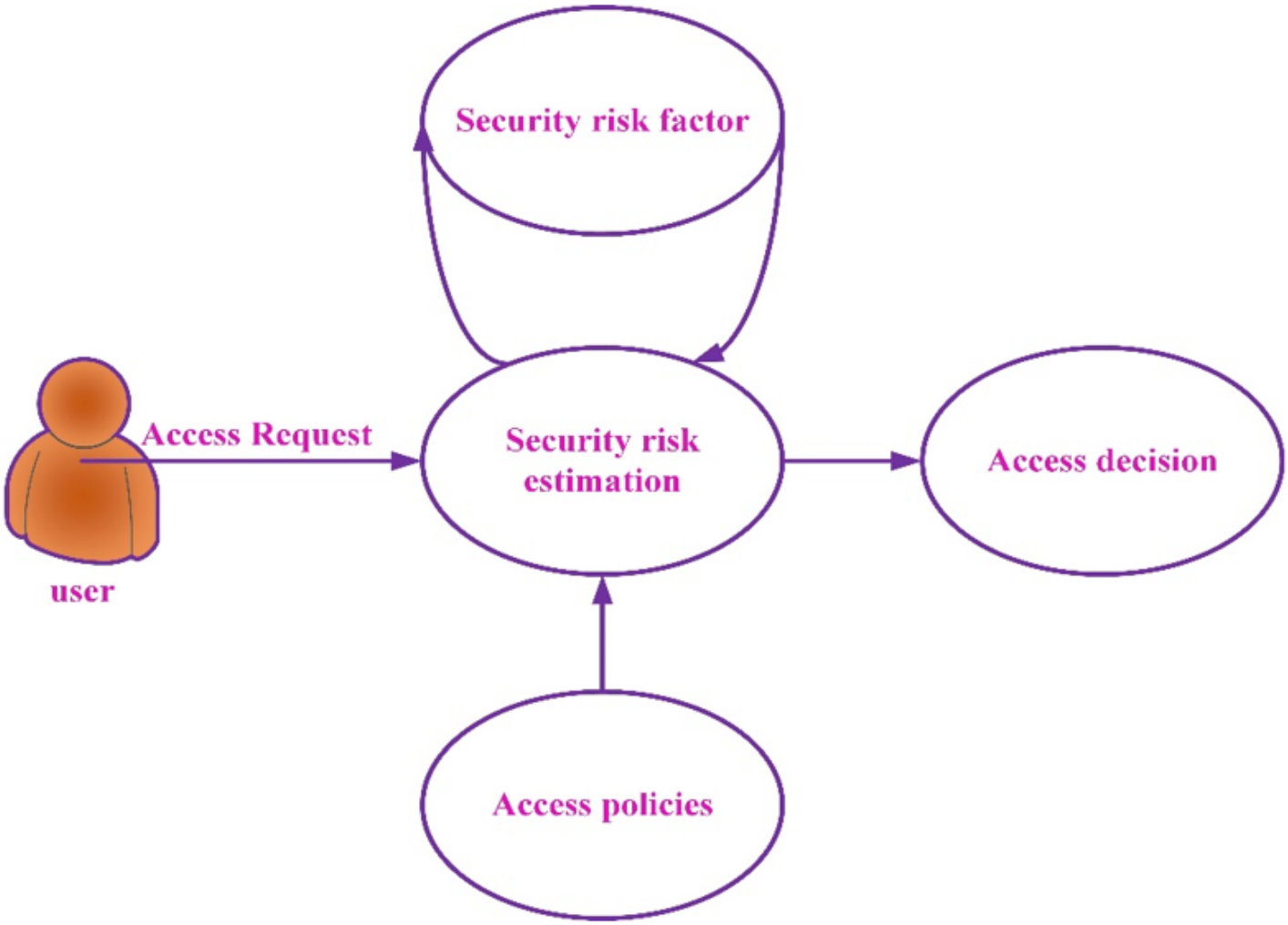

Figure 2

Security risk-based access control

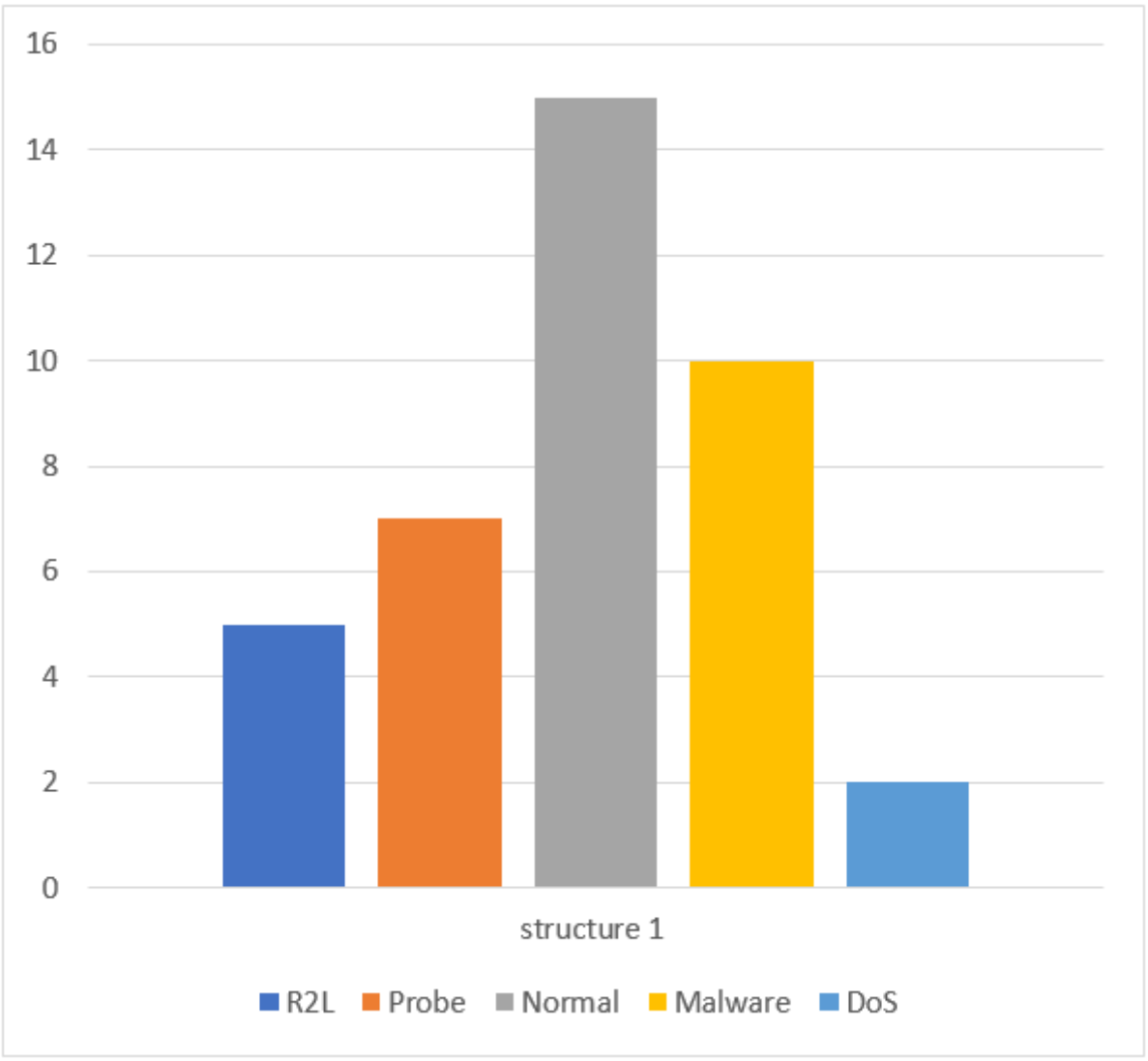

Figure 3

security risks

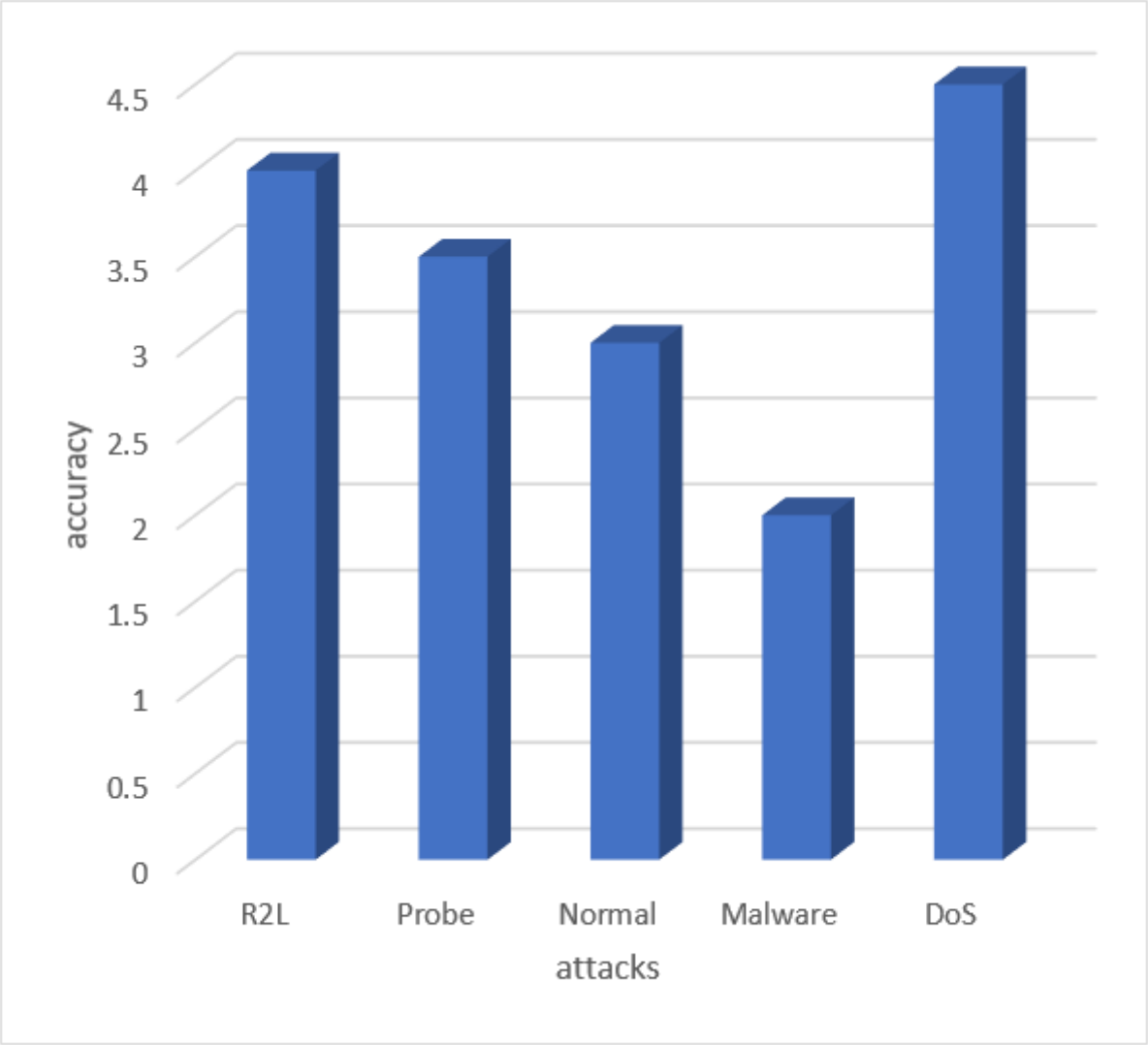

Figure 4

Accuracy results