

MobileNet based secured compliance through open web application security projects in cloud system

Rohith Vallabhaneni¹, Srinivas A Vaddadi¹, Sanjaikanth E. Vadakkethil Somanathan Pillai²,
Santosh Reddy Addula¹, Bhuvanesh Ananthan³

¹Department of Information Technology, University of the Cumberland, Williamsburg, United States

²School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, United States

³Department of Electrical and Electronics Engineering, PSN College of Engineering and Technology, Tirunelveli, India

Article Info

Article history:

Received Mar 16, 2024

Revised Apr 20, 2024

Accepted May 7, 2024

Keywords:

Cloud

Cyber attacks

MobileNet

OWASP

Virtual machine

ABSTRACT

The daunting issues that are promptly faced worldwide are the sophisticated cyber-attacks in all kinds of organizations and applications. The development of cloud computing pushed organizations to shift their business towards the virtual machines of the cloud. Nonetheless, the lack of security throughout the programmatic and declarative levels explicitly prone to cyber-attacks in the cloud platform. The exploitation of web pages and the cloud is due to the uncrated open web application security projects (OWASP) fragilities and fragilities in the cloud containers and network resources. With the utilization of advanced hacking vectors, the attackers attack data integrity, confidentiality, and availability. Hence, it's ineluctable to frame the application security-based technique for the reduction of attacks. In concern to this, we propose a novel Deep learning-based secured advanced web application firewall to overcome the lack of missing programmatic and declarative level securities in the application. For this, we adopted the MobileNet-based technique to ensure the assurance of security. Simulations are effectuated and analyzed the robustness with the statistical parameters such as accuracy, precision, sensitivity, and specificity and made the comparative study with the existing works. Our proposed technique surpasses all the other techniques and provides better security in the cloud.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Rohith Vallabhaneni

Department of Information Technology, University of the Cumberland

College Station Drive, Williamsburg, KY 40769, USA

Email: rohit.vallabhaneni.2222@gmail.com

1. INTRODUCTION

The standard method for delivering knowledge and amenities over the world's biggest network has been web applications [1]. Many companies in a variety of industries are still shifting their activities digitally. The majority of the public and private sectors use web apps that perform necessary administrative duties and store private information. Examples of such apps include social media sites, electronic mail, banking, and additional ones. Since mobile devices are so widely used in contemporary life, criminals have also become interested in them. Their goal is to exploit any weaknesses in these programs to carry out destructive acts, which will make company operations less efficient and effective.

Because websites [2] are so common and important in modern times, businesses need to know that the program is designed with reliability as well as safety in mind, taking responsibility for the proper safety precautions and reducing threats to the resources. While the phrase web page has been in use for many years, the terminology online program is relatively new. But gradually, both of these phrases seem to have lost any

meaning and are now frequently used identically. Everyone can control money, obtain knowledge rapidly, contact worldwide, purchase from residence, view films, attend to tunes, and do a lot, a lot more things with the help of the global web. Because personal information about customers as well as business details may be compromised, breaches of privacy [3] on such types of software are very concerning. Any web-based app must consider preserving these resources, and the creation strategy needs to cover a few crucial functions. This covers the procedures for information, monitoring and inspection, resource management, consent, and verification.

Ensuring app safety from the start can prove to be cheaper, with fewer problems over time. Companies must communicate with one another and provide goods distantly. Organizations quietly and efficiently communicate with clients through web-based apps. A number of the primary disadvantages of online applications are safety concerns [4], restricted traditional effectiveness, slowdowns, internet link reliance, connectivity problems, restricted utilization of gadget capabilities, and an absence of platform-specific customer service, troubles in revenue, and patches and preservation. For the secured programmatic and declarative level, we propose the novel MobileNet based advanced web application firewall which ensures the security in open web application security projects (OWASP).

The rest of the work is organized as, the review of the state-of-art works are enclosed in section 2. The proposed methodology to ensure the security in the programmatic level is stated in section 3. The experimental investigation is displayed in section 4. The work is concluded in section 5.

2. LITERATURE SURVEY

Kagita *et al.* [5], the authors have presented an internet of things (IoT) technique for applying dynamic and static examinations to connected vehicle software connectivity layouts and connectivity offerings to perform compliance assessments and risk assessments. Within a constrained amount of duration, the suggested structure provided a wide spectrum of detection of weaknesses. The framework can be seen as an initial move into a customizable autonomous risk evaluation and inspection platform for the safety and reliability of IoT components, notwithstanding its constraints. However, there is a lack of such an assessment.

Shameli-Sendi [6], the researchers have described an efficient security data-driven approach for putting danger evaluation into practice. It can be carried out at numerous levels, such as for resources or company policies. It sets a specific company apart from another is its safety of knowledge; these are the things that matter, and it is these that both of us must prioritize. The locations of the creation, editing, processing, transmission, visible, and ultimate storage of information are all included in the knowledge existence phase. Consequently, it falls short of providing all the protection solutions needed to build reliable web pages.

Casola *et al.* [7], the authors have developed a secure software development methodology designed to assist professionals with safety planning and evaluation and appropriate for incorporation into contemporary operations processes. The suggested technique makes use of a model-based technique that facilitates the identification of current risks, the choice of corrective measures to implement, and the verification of the success of such suppression using focused safety assessments as well as periodic evaluation processes. Risk estimation and assurance sections are part of a widely recognized exposed internet program that is often employed for safety awareness functions. The primary cause of this is the tremendous expense of safety measures.

Chadwick *et al.* [8], the authors suggested a five-level trust model for developing a framework for the transfer of information using the digital periphery. To change the database before releasing it for assessment, the information possessor can select a suitable level of security and database disinfection method, which can range from simply typing to authentication. The examination that occurred currently involves four experimental endeavors that are confirming the functionality of the system. Unfortunately, there aren't enough institutions to examine the pooled information.

Wen and Katt [9], the authors highlighted a quantitative security evaluation and analysis model that seeks to effectively assess the protection features of online tools while offering insightful information. To guarantee enough trust when purchasing online communication programs, companies need to establish an innovative and fast technique for reviewing and evaluating its safety. To describe the protection measures that an infrastructure achieves, statistical safety assessment uses numerical and theoretical methodologies. Therefore, it is constantly vulnerable to emerging security flaws that could result in lost data.

Neshenko *et al.* [10], discussed how to classify state-of-the-art surveys using a comprehensive strategy and addressed IoT vulnerabilities that are always changing. Furthermore, although [11] detailed the popular IoT communication protocols and how they implemented certain security procedures to make a comparison of the taken into consideration IoT technologies, the works in [12], [13] concentrated primarily on discovering vulnerabilities in IoT firmware. On the other hand, a publication evaluated the most recent research and discussed IoT vulnerabilities, but it didn't delve further into the ML and DL methods that are employed to increase IoT security [14]. By concentrating on certain algorithms, the most recent survey to be published offered a state-of-the-art approach to leveraging AI to improve IoT security [15]. Weak password

vulnerabilities were typically used to launch attacks against IoT device authorization, granting the attacker access to and control over the ecosystem [16]–[20]. The system's availability, secrecy, and integrity are all hampered by insecure network services [21]–[23].

3. PROPOSED METHOD FOR SECURITY

The proposed technique utilizes code-level security for the application layer of TCP/IP with the association of MobileNet incorporated with the web application firewalls. The code level security ensures the security from the initial stage of the code while developing the software. Meanwhile, the code must follow the guidelines of the OWASP community and also attain declarative security based on the VM container and network of cloud containers. The main purpose of considering the cases is to reduce the exploitation of OWASP at the code level.

3.1. Scenarios of attack

The scenarios taken in the attack are i) the monitoring phase, ii) the injection phase, iii) the attack phase, and iv) the exploitation phase:

- Monitoring phase: this phase identifies the attackers in the web application that are targeted.
- Injection phase: this phase is the injection of malicious payloads in the web pages by transferring the attack URLs for processing the web server.
- Attack phase: when the malicious code is used to run on the web page it might have provided valuable data such as database names, versions, tables, and columns as a response to the hacker. This might have mitigated the integrity, confidentiality, and availability of the server of the web page by accessing the sensitive content.
- Exploitation phase: after getting access to the sensitive information by the unauthorized user, the information is analyzed and targeted by the attackers. This is followed by exposing the data to social media or any other online sites thus establishing the information loss.

3.2. Security at the application layer

The security at the application layer is not considered by most of the researchers for cloud-based web applications. This is because the security parameters of OWASP are difficult to handle by the coders and the less time taken for developing the code is also one of the issues. This might have led to the unpatched vulnerabilities [24]. To reduce the OWASP exploitation we have adopted the MobileNet-based web application firewall which can be applied in the application layer. This defends the web server from the attacks and replaces the intrusion detection system. The details of MobileNet are elucidated in the following section.

3.3. MobileNet

The lightweight CNN is named MobileNet, which is well effective architecture. The running process with its computational power becomes less and it has various merits of MobileNet. The TensorFlow library with data detection and categorization is performed by train the model using MobileNet [25]. The machine learning applications specialized with Google that generates TensorFlow that provided short training time with high accuracy also to train less number of data. Due to great performance, higher accessibility and flexibility, the TensorFlow developed abundant attention in the machine learning field. Figure 1 illustrates the structure of MobileNet.

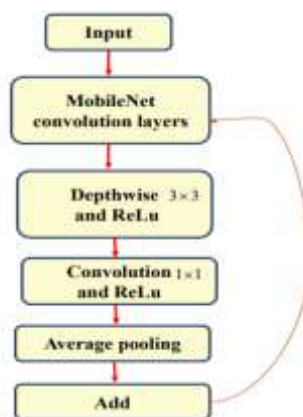


Figure 1. The structure of mobilenet

The depth oriented separable convolutions utilizes MobileNet instead of standard convolutions. Compared to standard convolution, lower depth based separable convolutions requires number of multiplications, which has reduced computational power. The point and depth wise convolution involved in the depth oriented separable convolution [26]. At the same time, apply convolution to each channels. The depth based convolution output is merged by applying in point wise convolution. Below formula computes the standard convolution with its computational cost:

$$E_k \cdot E_k \cdot A \cdot B \cdot E_D \cdot E_D \quad (1)$$

the following expression is for depth based separable convolution with its computational cost:

$$E_k \cdot E_k \cdot A \cdot E_D + A \cdot B \cdot E_D \cdot E_D \quad (2)$$

the point and depth based layers with 2 strides and convolution layers present in the MobileNet structure.

3.4. Proposed advanced web application firewall based on MobileNet

The advanced application firewalls is achieved with the proposed MobileNet technique and with its training model the online attacks are mitigated dynamically. The advantage of using the proposed technique over the traditional one is that in the traditional one, the attacks are detected using the predetermined rules, whereas, the proposed technique detects the attacks by performing training and testing approaches. For the coding, the Python libraries used are Numpy, seaborn, Pandas, Matplotlib, and scikit learn library. The proposed data flow for providing the advanced web firewall is depicted in Figure 2.



Figure 2. Proposed workflow for providing web advanced firewall in cloud system

The proposed work begins with the collection of datasets. Data Collection is made with the top malicious attack vectors of OWASP with various 10 classes. The collected data are pre-processed to ignore the null and repeated values to validate the dataset and allow it to fit for designing the model. Henceforth, the features are extracted using the Python libraries and enable the human-understandable data to the machine-understandable codes. This ensures the smoothness of the proposed work in identifying the cyber-attacks to provide firewall protection. Subsequently, the dataset is split into training, testing, and validation datasets. The training for the proposed MobileNet model is provided for the training dataset and the validation is effectuated in the testing and validation dataset. The proposed technique is used to classify the various 10 classes from the dataset that are collected as per the training program. The training is done until it reaches the saturation accuracy to attain the bias factor. The proposed model is used to predict the attacks and then ensure the security of the cloud-based virtual machine. This protects the web pages that use cloud computing [27].

3.5. MobileNet-based OWASP vulnerabilities scanner tool

The overall workflow of the proposed work by injecting the attacks and detecting them using the advanced web application firewall is illustrated in Figure 3. The proposed MobileNet-based scanner tool is utilized to provide security at the programmatic level. The detection of vulnerabilities and earlier patching are the most needed to avoid the setbacks of the security in the application layer. Some of the commercially available scanner tools execute over the source code to detect the vulnerabilities from each line by scanning it properly but it is time-consuming and needs to be patched manually. Hence the proposed MobileNet-based

web application firewall checks the source code often provides solutions and reduces time consumption. This also ensures the security of the web application pages.

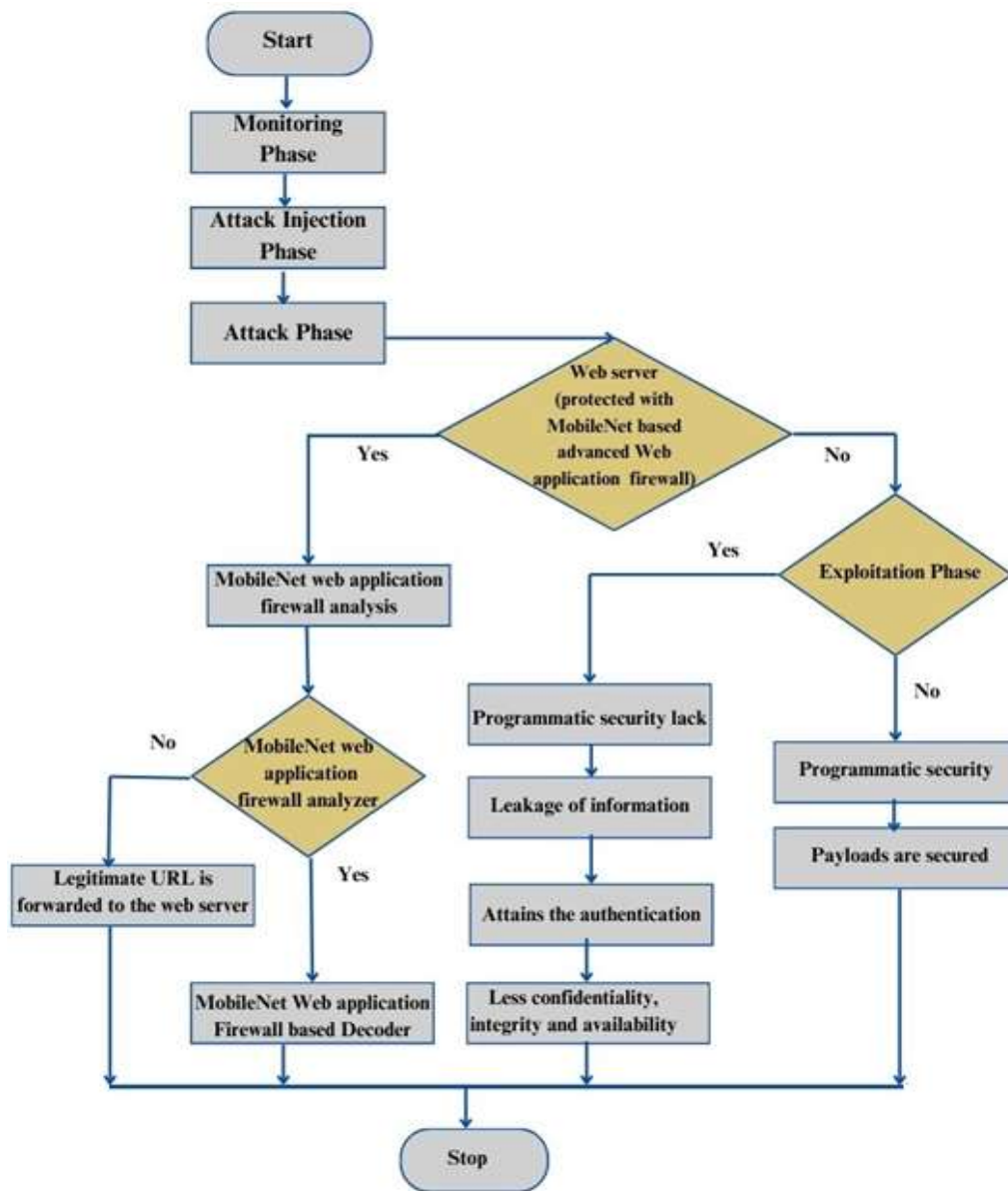


Figure 3. Overall systematic diagram of proposed work from injecting the attack to detecting the attack using the advanced web application firewall

4. EXPERIMENTAL RESULTS

This section outlines the experimental study of proposed work. Demonstrates with previous techniques and it comparison results by using different evaluation measures. The MATLAB 2019a simulator carried out simulation.

4.1. Evaluation measures

The real positives proportions are recognized accurately with the prediction true positive rate is named as precision (Pr):

$$Pr = \frac{T^{+ve}}{T^{+ve} + F^{+ve}} \tag{3}$$

Recall (Re) measures the correctly expected positive value proportion:

$$Re = \frac{T^{+ve}}{T^{+ve} + F^{-ve}} \quad (4)$$

the precision and recall harmonic mean defines the F-score value:

$$F_{score} = 2 \times \frac{Re \times Pr}{Pr + Re} \quad (5)$$

an accurate prediction percentages are determined with the indicator of accuracy:

$$Accuracy = \frac{T^{+ve} + T^{-ve}}{T^{+ve} + T^{-ve} + F^{+ve} + F^{-ve}} \quad (6)$$

by these equations, the truly positive and negative values are T^{+ve} and T^{-ve} with the false positive and negative values are F^{+ve} and F^{-ve} .

4.2. Evaluation investigation

The overall comparison for accuracy is depicted in Figure 4. The existing authors of Kagita *et al.* [5], Shameli-Sendi *et al.* [6], Casola *et al.* [7], Chadwick *et al.* [8] and proposed work for computing the accuracy comparative investigation. The accuracy percentages of [5]-[8] and proposed becomes 45%, 50%, 67%, 80% and 94.89% at the level of 20th epochs. Based on 20th to 100th epochs, an accuracy level of proposed becomes 94.89%, 95.76%, 95.90%, 96.11% and 96.40%. This plot reveals the recommend work accuracy is higher comparing with the existing works of [5]-[8]. Figure 5 plots the overall comparison for recall outputs. The previous works of [5]-[8] and proposed work for computing the recall comparison plot. The recall percentages of [5]-[8] and proposed becomes 66%, 70%, 79%, 87% and 93.89% at the level of 20th epochs. Based on 20th to 100th epochs, a recall stage of proposed becomes 93.89%, 94.70%, 95.13%, 96.03% and 96.43%. This plot reveals the recommend work recall is higher comparing with the existing works of [5]-[8]. The recall result of proposed with all epochs is accomplished highest values apart from the previous [5]-[8].

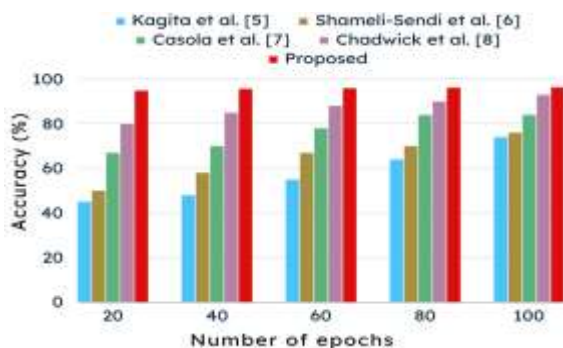


Figure 4. Overall comparison for accuracy

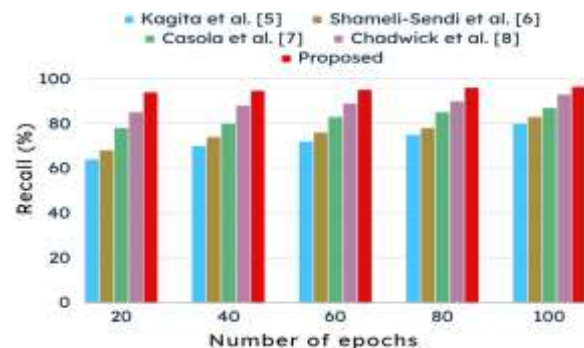


Figure 5. Overall comparison for recall

Figure 6 designs the overall comparison for precision representation. The previous works of [5]-[8] and proposed work for computing the precision comparison plot. The precision percentages of [5]-[8] and proposed becomes 64%, 68%, 78%, 85% and 93.12% at the level of 20th epochs. Based on 20th to 100th epochs, the level of precision for proposed becomes 93.12%, 94.24%, 95.16%, 95.14% and 96.21%. This plot reveals the recommend work precision is higher contrasted by the existing works of [5]-[8]. The result of proposed precision by all epochs realized highest values apart from the previous [5]-[8].

The F-score results with its graphical plot is outlined in Figure 7. The state-of-art studies of [5]-[8] and proposed work for computing the F-score comparison graph. The F-score percentages of [5]-[8] and proposed becomes 69%, 78%, 80%, 83% and 94.30% with a level of 20th epochs. Based on 20th to 100th epochs, the level of F-score for proposed becomes 94.30%, 94.80%, 95.20%, 95.80% and 96.10%. The recommend work F-score plot reveals higher contrasted by the existing works of [5]-[8]. The result of proposed F-score by all epochs comprehended highest values apart from the previous [5]-[8].

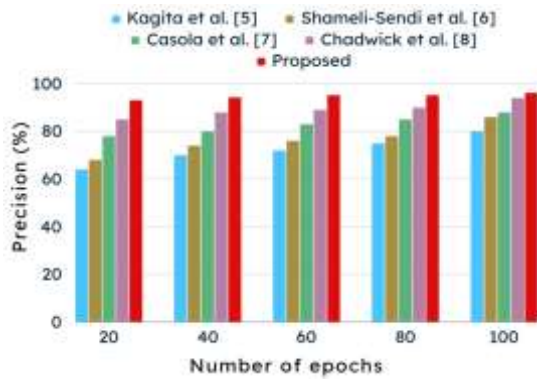


Figure 6. Overall comparison for precision

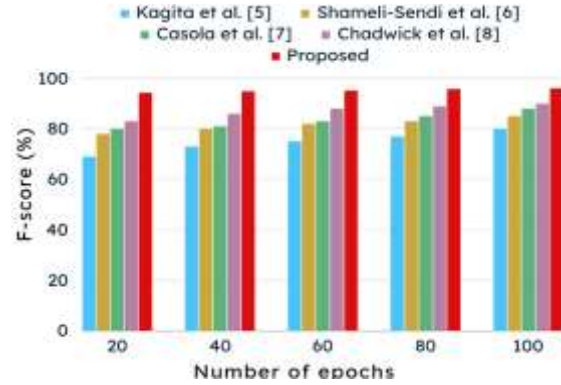


Figure 7. Overall comparison for F-score

Figure 8 reveals the F-score graphical plot. The state-of-art studies of [5]-[8] and proposed work for computing the comparison graph of computational time. The percentages of computational time of previous works [5]-[8] and proposed becomes 291s, 250s, 242s, 220s and 132s with a level of 20th epochs. According to 20th to 100th epochs, the computational time in seconds for proposed becomes 182s, 189s, 174s, 161s and 132s. The recommend work computational time plot reveals higher distinguished by the existing works of [5]-[8]. The result of proposed computational time to each epochs comprehended highest values apart from the existing studies [5]-[8].

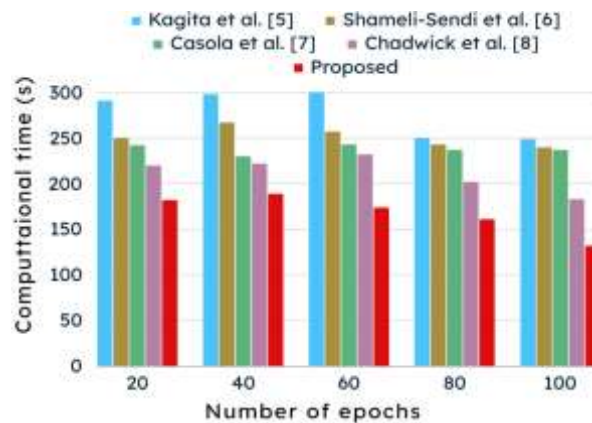


Figure 8. Overall comparison for computational time

The significance of MobileNet-based secured compliance through OWASP in a cloud system lies in its ability to provide efficient, real-time threat detection, comprehensive security coverage, scalability, cost-effectiveness, user trust, and compliance assurance for mobile applications. By integrating MobileNet-based intrusion detection systems with OWASP guidelines, organizations can enhance the security posture of their mobile applications and mitigate the risk of security breaches and compliance violations. Overall, MobileNet-based secured compliance through OWASP in a cloud system offers efficient resource utilization, real-time threat detection, comprehensive security coverage, scalability, cost-effectiveness, user trust, and compliance assurance for mobile applications. By integrating MobileNet-based intrusion detection systems with OWASP guidelines, organizations can enhance the security posture of their mobile applications and mitigate the risk of security breaches and compliance violations.

5. CONCLUSION

The work in this article is to provide an advanced web application firewall to safeguard the web pages of the cloud. Cloud vulnerabilities are presented at the programmatic and declarative level and most of the works ignore those security and lead to loss of information. To provide protection we proposed an innovative technical approach known as MobileNet-based Web application firewall which ensures security at

the programmatic level. The different scenarios used for the attack detection are explained in this work. The work also started from the attack injection level to the detection level by the proposed work. To achieve this, the data collected from OWASP are pre-processed to ignore the repeated and null words and followed by the feature extraction. The proposed MobileNet provides better security on the web page. Simulations were made to ensure the security of the proposed work and a comparative study was also made. The detection accuracy of the proposed work is 96.40%. In future, the authors will extend this research in MobileNet-based secured compliance through OWASP in cloud systems, contributing to more efficient, robust, and trustworthy cybersecurity solutions for mobile applications.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.





REFERENCES

- [1] T. Shi, H. Ma, G. Chen, and S. Hartmann, "Cost-effective web application replication and deployment in multi-cloud environment," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 8, pp. 1982-1995, 2021, doi: 10.1109/TPDS.2021.3133884.
- [2] M. Saad, A. Zia, M. Raza, M. Kundi, and M. Haleem, "A comprehensive analysis of healthcare websites usability features, testing techniques and issues," *IEEE Access*, vol. 10, pp. 97701-97718, 2022, doi: 10.1109/ACCESS.2022.3193378.
- [3] P. Zhang, Y. Wang, N. Kumar, C. Jiang, and G. Shi, "A security-and privacy-preserving approach based on data disturbance for collaborative edge computing in social IoT systems," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 97-108, 2021, doi: 10.1109/TCSS.2021.3092746.
- [4] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriya, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545-2554, 2021, doi: 10.1109/JIOT.2021.3077803.
- [5] M. K. Kagita, G. R. Bojja, and M. Kaosar, "A framework for intelligent IoT firmware compliance testing," *Internet of Things and Cyber-Physical Systems*, vol. 1, pp. 1-7, 2021, doi: 10.1016/j.iotcps.2021.07.001.
- [6] Shameli-Sendi, "An efficient security data-driven approach for implementing risk assessment," *Journal of Information Security and Applications*, vol. 54, pp. 102593, 2020, doi: 10.1016/j.jisa.2020.102593.
- [7] V. Casola, A. D. Benedictis, C. Mazzocca, and V. Orbinato, "Secure software development and testing: A model-based methodology," *Computers and Security*, vol. 137, pp. 103639, 2024, doi: 10.1016/j.cose.2023.103639.
- [8] D. W. Chadwick *et al.*, "A cloud-edge based data security architecture for sharing and analysing cyber threat information," *Future Generation Computer Systems*, vol. 102, pp. 710-722, 2020, doi: 10.1016/j.future.2019.06.026.
- [9] S. F. Wen, and B. Katt, "A quantitative security evaluation and analysis model for web applications based on OWASP application security verification standard," *Computers and Security*, vol. 135, pp. 103532, 2023, doi: 10.1016/j.cose.2023.103532.
- [10] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Communications Surveys and Tutorials*, vol. 21, pp. 2702-2733, 2019, doi: 10.1109/comst.2019.2910750.
- [11] W. Xie, Y. Jiang, Y. Tang, N. Ding, Y. Gao, "Vulnerability detection in IoT firmware: A survey," *In Proceedings of the 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, Shenzhen, China, 15-17 December 2017, New York, NY, USA, pp. 769-772, 2017, doi: 10.1109/icpads.2017.00104.
- [12] X. Feng, X. Zhu, Q.L. Han, W. Zhou, S. Wen, and Y. Xiang, "Detecting vulnerability on IoT device firmware: A survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 10, pp. 25-41, 2022, doi: 10.1109/jas.2022.105860.
- [13] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things Journal*, vol. 6, pp. 8182-8201, 2019, doi: 10.1109/jiot.2019.2935189.
- [14] M. Yu, J. Zhuge, M. Cao, Z. Shi, and L. Jiang, "A survey of security vulnerability analysis, discovery, detection, and mitigation IoT devices," *Future Internet*, vol. 12, no. 27, 2022, doi: 10.3390/fi12020027.
- [15] T. A. Ahanger, A. Aljumah, and M. Atiqzaman, "State-of-the-art survey of artificial intelligent techniques for IoT security," *Computer network*, vol. 206, pp. 108771, 2022, doi: 10.1016/j.comnet.2022.108771.
- [16] OWASP "Internet of things," *OWASP Foundation*: Bel Air, MA, USA, 2022, doi: 10.1504/ijitca.2020.10033810.
- [17] J. Qu, "Research on password detection technology of IoT equipment based on wide area network," *ICT Express*, vol. 8, pp. 213-219, 2021, doi: 10.1016/j.icte.2021.09.013.
- [18] R. S. Verma, B. R. Chandavarkar, and P. Nazareth, "Mitigation of hard-coded credentials related attacks using QR code and secure web service for IoT," *In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, pp. 1-5, 2019, doi: 10.1109/icccnt45670.2019.8944592.
- [19] H. M. Sun, Y. H. Chen, and Y. H. Lin, "oPass: a user authentication protocol resistant to password stealing and password reuse attacks," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 651-663, 2012, doi: 10.1109/tifs.2011.2169958.
- [20] D. Mouris, and N.G. Tsoutsos, "Zilch: A framework for deploying transparent zero-knowledge proofs," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3269-3284, 2021, doi: 10.1109/tifs.2021.3074869.
- [21] M. E. Erendor, and M. Yildirim, "Cybersecurity awareness in online education: a case study analysis," *IEEE Access*, vol. 10, pp. 52319-52335, 2022, doi: 10.1109/access.2022.3171829.
- [22] T. Alladi, V. Chamola, B. Sikdar, and K. K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, pp. 17-25, 2020, doi: 10.1109/mce.2019.2953740.
- [23] D. Chatterjee, H. Boyapally, S. Patranabis, U. Chatterjee, and A. Hazra, Mukhopadhyay, D, "Physically related functions: exploiting related inputs of PUFs for authenticated-key exchange," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3847-3862, 2022, doi: 10.1109/tifs.2022.3214089.





- [24] Q. Meng, X. Nian, Y. Chen, and Z. Chen, "Attack-resilient distributed nash equilibrium seeking of uncertain multiagent system over unreliable communication networks," *In IEEE Transactions on Neural Networks and Learning Systems*; New York, NY, USA, pp. 1–15, 2022, doi: 10.1109/tnnls.2022.3209313.
- [25] I. M. Abbadi, "Middleware services at cloud application layer," *In International Conference on Advances in Computing and Communications, Berlin, Heidelberg: Springer Berlin Heidelberg*, 2021, doi: 10.1007/978-3-642-22726-4_58.
- [26] Y. C. Chiu, C. Y. Tsai, M. D. Ruan, G. Y. Shen, and T. T. Lee, "Mobilenet-SSDv2: An improved object detection model for embedded systems," *In 2020 International Conference on System Science and Engineering (ICSSE)*, IEEE, 2020, doi: 10.1109/icsse50014.2020.9219319.
- [27] M. Bach-Nutman, "Understanding the top 10 owasp vulnerabilities," *arXiv preprint arXiv:2012.09960*, 2020, doi: 10.1063/pt.5.028530.

BIOGRAPHIES OF AUTHORS







Dr. Rohith Vallabhaneni     received his Ph.D. degree in Information Technology from the University of the Cumberland in the United States. As a Senior IEEE member, he has contributed significantly to various research journals, both as an author and co-author. His professional journey is marked by a strong work ethic and a profound ability to lead teams in addressing organizational challenges. His exemplary team leadership skills and dedication to his work underscore his contributions to the field of Information Technology. He can be contacted at email: rohit.vallabhaneni.2222@gmail.com.







Srinivas A. Vaddadi     is a dynamic and forward-thinking professional in the field of Cloud and DevSecOps. With a solid educational foundation in computer science, Srinivas embarked on a journey of continuous learning and professional growth. Their relentless pursuit of knowledge and commitment to staying at the forefront of industry advancements has earned them recognition as a thought leader in the Cloud and DevSecOps space. He can be contacted at email: vsad93@gmail.com.



Sanjaikanth E. Vadakkethil Somanathan Pillai     (Senior Member, IEEE) holds an MS in Software Engineering from The University of Texas at Austin, Texas, USA, and a BE from the University of Calicut, Kerala, India. Currently pursuing a PhD in Computer Science at the University of North Dakota, Grand Forks, North Dakota, USA, his research spans diverse areas such as mobile networks, network security, privacy, location-based services, and misinformation detection. He is a proud member of Sigma Xi, The Scientific Research Honor Society, underlining his commitment to advancing scientific knowledge and research excellence. He can be contacted at email: s.evadakkethil@und.edu.



Santosh Reddy Addula     holds a master's degree in Information Technology from the University of the Cumberland in Kentucky, United States of America. He has over five years of experience working in the IT industry, and he has showcased expertise across various domains in IT. He has 3+ patents, has contributed as an author and co-author of research articles, and has a role as a reviewer for esteemed journals such as IEEE, Springer, and Elsevier. He can be contacted at email: santoshaddulait@gmail.com.



Dr. Bhuvanesh Ananthan     received the B.E. degree in Electrical and Electronics Engineering from Anna University in 2012, M.Tech. in Power System Engineering from Kalasalingam University in 2014 and Ph.D. degree from Faculty of Electrical Engineering of Anna University in 2019. He has published more than 65 papers in reputed international journals, 25 papers in international conferences and 10 books. He is a life time member of International Society for Research and Development, International Association of Engineers. He can be contacted at email: bhuvanesh.ananthan@gmail.com.