History of Medicine, 2025, 11(1): 179-185

DOI: 10.48047/HM.V11.I1.2025.179-185

Authenticating the Study of Leaf Disease Identification using RSA Digital Signature

[1] Soumendu Banerjee, Assistant Professor, Department of Computer Application, Academy of Technology, Adisaptagram, Hooghly

[2] Subhashis Das, Assistant Professor, Department of Computer Science & Engineering, Academy of Technology, Adisaptagram, Hooghly

Abstract**:** *Plant disease is a critical issue for farmers, directly impacting their livelihood. Therefore, collecting data from farmers must be done securely, and delivering the results should be carried out in an authentic and trustworthy manner. Any breach in data security or result authenticity can significantly disrupt a farmer's daily life. Hence, secrecy (confidentiality) and authenticity, the two fundamental pillars of security, are essential in the study and implementation of plant leaf disease identification systems.*

Keywords: Leaf disease identification, DFD, digital signature, image based detection, CNN

Introduction:

Plant diseases are conditions that disrupt a plant's normal physiological functions, typically caused by pathogens such as bacteria, fungi, viruses, and parasites. In severe cases, these diseases can be fatal to the plant. To control their spread, farmers often rely on eradicants and pesticides. While these chemicals can be effective in managing plant diseases, they also carry potential risks. The substances used may contaminate the food supply, posing health hazards to humans. Additionally, if left untreated, plant diseases can spread to other plants or, in some cases, even affect humans, potentially leading to broader ecological and public health concerns. Therefore, it is essential to address plant diseases using methods that not only effectively combat the pathogens but also minimize dependence on potentially hazardous eradicants. Ensuring the safety and effectiveness of these treatments requires careful evaluation and responsible management. Moreover, the collection, handling, and dissemination of information related to plant diseases must be conducted with great care to avoid negative consequences. Mishandling or miscommunication of such data can lead to poor decision-making and further spread of disease. Securely managing this information and restricting access to authorized individuals can significantly improve disease control efforts and enhance overall agricultural practices. Security always play a vital role while we deal with a public network. Non-repudiation and authentication[1] also play a vital role here, which can be achieved through digital signature[2][8].

In this paper, we focus on identifying various types of diseases affecting tomato leaves and visualize the results. We propose a system in which a farmer captures an image of tomato leaves and uploads it to the cloud, where our disease identification model[3] processes the image and returns the diagnosis. To ensure secure communication, we aim to establish an environment where data is transmitted from the farmer’s mobile device to the testing model using end-to-end encryption. The RSA digital signature[4] technique will be employed to ensure authenticity while data is transmitted over a public network. In Section I, we present the Data Flow Diagram (DFD)[5] illustrating the use of the RSA digital signature during the transmission of data from the farmer's mobile device to our model. Given the use of a public network, authentication is a critical component. In Section II, we evaluate the performance of our disease identification model and present the results through pie chart analysis. Finally, in Section III, we will conclude by discussing some potential future enhancements to our system.

Section – I

A Data Flow Diagram (DFD) is a graphical tool used to represent the flow of data within a system, illustrating the input data, the processes applied to it, and the resulting output. Figure1 in Section I presents a DFD outlining the process of sending result of the processed leaf generated by our model admin to the farmer. In this process, the model or lab admin sends the disease identification result and computes its hash value using the hash() function. Both the public key and the admin’s private key are stored in a data repository. The admin uses his/her private key to generate a digital signature, which is then sent to the farmer along with the report and public key. Upon receiving this data, the farmer recalculates the hash value using the admin’s public key and compares it with the received hash value. If the values match, the material is accepted; otherwise, appropriate action is taken.

DOI: 10.48047/HM.V11.I1.2025.179-185

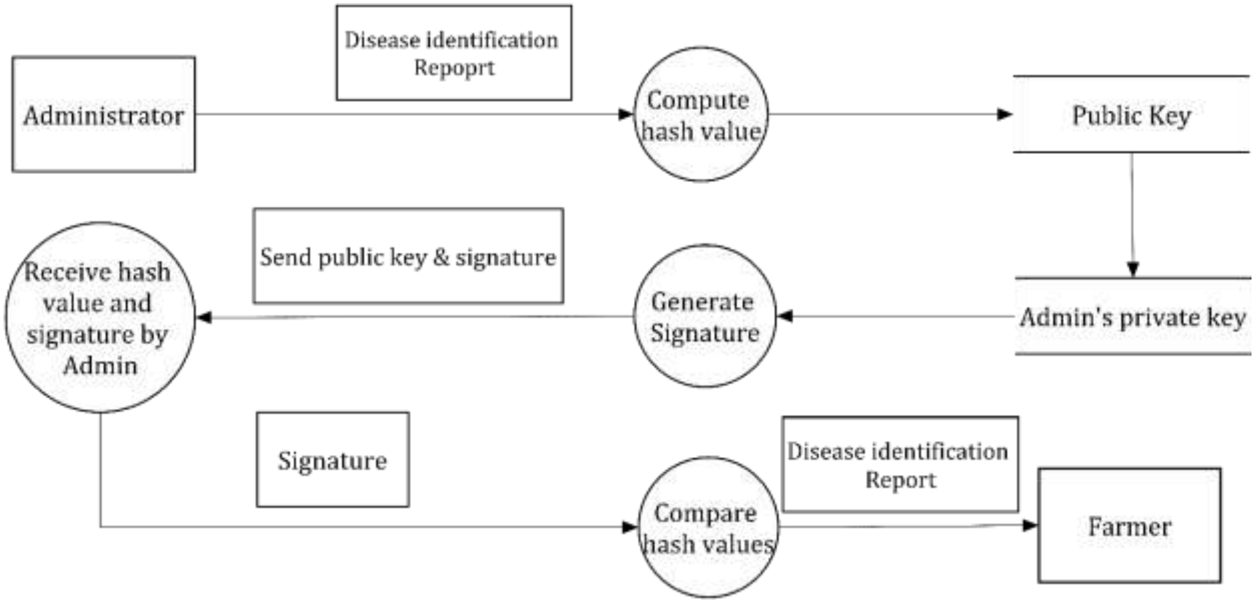
Administrator
Disease identification Repoprt
Compute hash value
Public Key
Receive hash value and signature by Admin
Send public key & signature
Generate Signature
Admin's private key
Signature
Compare hash values
Disease identification Report
Farmer

Figure1: DFD for authenticating report transmission

Section – II

In this paper we have used dataset from M. R. A. Rashid et al. [6] to train the model and evaluate their performance. The Tomato Dataset consists of 2449 images consisting of 4 classes: Bacterial spot, Fresh Leaves, Leaf curl virus and Spotted Wilt[7]. We have applied three approaches MobileNetV2, DenseNet121 and Xception on this dataset and design charts for making comparison among these. Tomato Fresh leaf class achieves perfect scores, underscoring its outstanding performance. Other classes also show excellent metrics, highlighting the model's overall effectiveness. In Figure2 we have shown the Precision comparison among these models. Figure3 displays the Recall comparison among these models. F1-score comparison has been shown in Figure4. Finally, we have shown in Figure5 that classification report for DenseNet121 on the tomato dataset performs exceptionally across all labels.

Below, we have shown all the comparison figures as per the result produced after applying the different deep learning architectures.

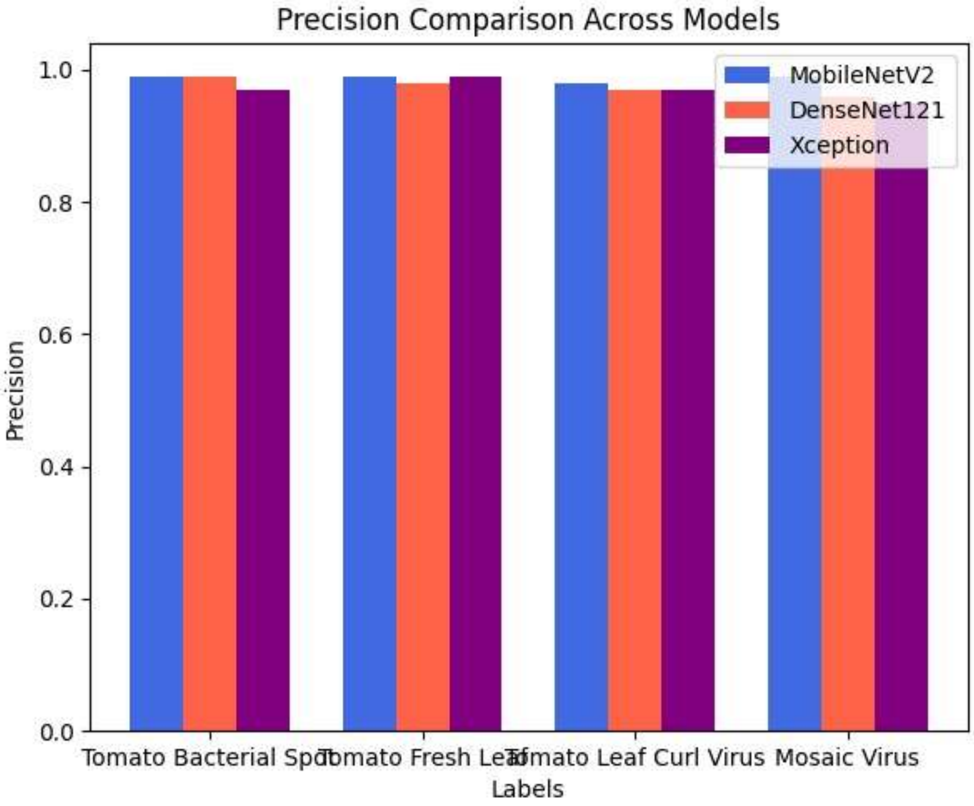

Figure2: Precision comparison across models

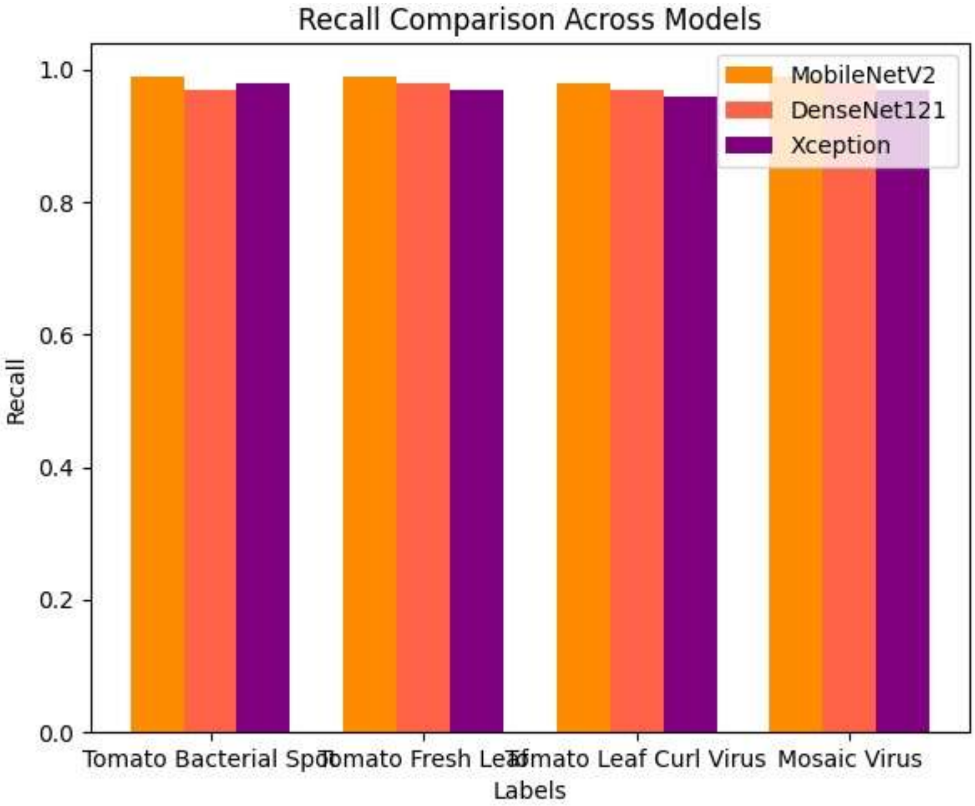

Figure3: Recall comparison across models

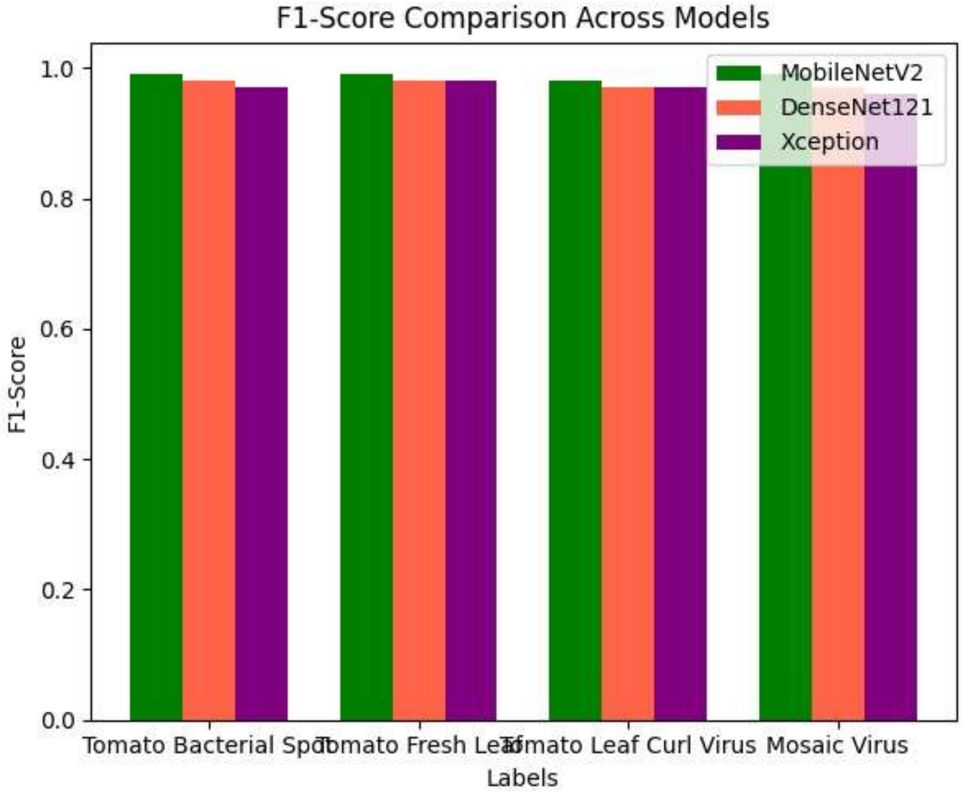

Figure4: F1-Score comparison across models

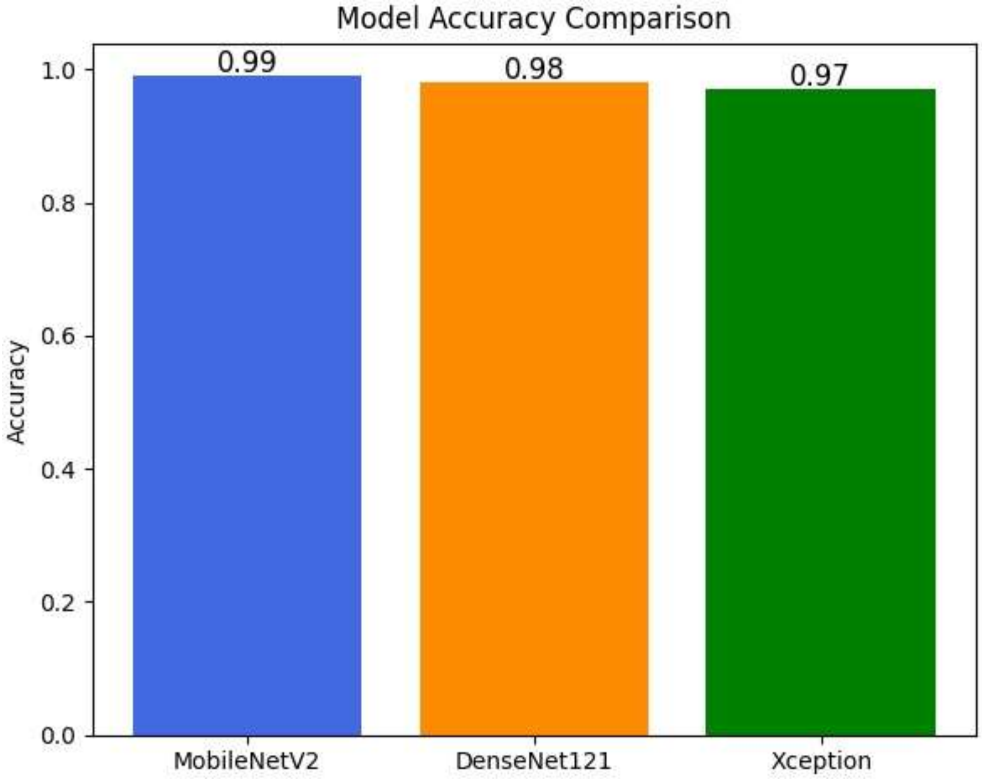

Figure5: Model accuracy comparison

Unit – III:

In conclusion, we can improve the model as per the requirements. We can design a custom algorithm to send the data in multiple chinks from multiple servers to improve throughput. Additionally, those servers will be replicated to maintain data consistency. In order for more security we can use various Blockchain techniques to secure the data. However, we also need to maintain cost since this will be applicable in a large area and maintaining 24 x 7 uptime will incur a high amount of cost. Therefore, we will try to provide the best security possible in a reasonable amount of cost.

References:

[1] A. Kahate, “Cryptography and Network Security”, McGraw Hill Education (India) Private Limited, New Delhi, 2013.

[2] S. Karforma & S. Banerjee, “Object-Oriented Modeling of RSA Digital Signature for security in E-Learning”, International Journal of Advanced Technology in Engineering and Science, Vol-02(01), September 2014, pp: 283-290.

[3] S. Das, S. Banerjee, P. Banerjee and N. Das, "Securing Comparative Study of Leaf Disease Identification with Different Deep Learning Models Using Hyperledger Fabric," 2024 4th

DOI: 10.48047/HM.V11.I1.2025.179-185

International Conference on Computer, Communication, Control & Information Technology (C3IT), Hooghly, India, 2024, pp. 1-6.

[4] S. Banerjee & S. Karforma, “Object Oriented Metric based analysis of RSA Digital Signature to authenticate mark sheet in e-learning”, International Journal of Control Theory and Application, Vol – 9(42), 2016, pp: 429-436

[5] Rajib Mall, Fundamentals of Software Engineering, Prentice Hall of India, New Delhi, June 2006

[6] M.R.A.Rashid, T.K.Tarin, R.Kamara, M.Y.Mou, S.F.Rabbi, and M.Hasan, “Plant leaf freshness and disease detection dataset from Bangladesh,” https://doi.org/ 10.17632/n67gctmjyj.3, 2024.

[7] K. Babu, “Plant disease identification and classification using image processing,” International Journal of Engineering and Advanced Technology (IJEAT), vol. 8, pp.442–446, February 2019.

[8] S. Karforma & S. Banerjee, “Object-oriented modeling of rsa digital signature for security in e-learning”, International Journal of Advanced Technology in Engineering and Science, vol. 2(1), pp.283–290, September 2014.