Scientific Research Publishing

E-Health Telecommunication Systems and Networks, 2022, 11, 34-46
https://www.scirp.org/journal/etsn
ISSN Online: 2167-9525
ISSN Print: 2167-9517

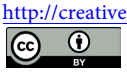
A Secure Model for Preventing the Spread of COVID-19 in Bangladesh

Shaznin Sultana[1], Raisa Tahsin Taspia[1], Md. Farhad Hossain[1], Md. Nahiduzzaman[1], Roksana Akter[2], Rashed Mazumder[3]

[1]ICT, Bangladesh University of Professionals, Dhaka, Bangladesh
[2]CSE, Southeast University, Dhaka, Bangladesh
[3]IIT, Jahangirnagar University, Savar Union, Bangladesh
Email: shaznin1916@gmail.com, raisa.tahsin99@gmail.com, mdfarhad61@gmail.com, xnish28@gmail.com, roksana.akter@seu.edu.bd, rakhu345@gmail.com

How to cite this paper: Sultana, S., Taspia, R.T., Hossain, Md.F., Nahiduzzaman, Md., Akter, R. and Mazumder, R. (2022) A Secure Model for Preventing the Spread of COVID-19 in Bangladesh. *E-Health Telecommunication Systems and Networks*, **11**, 34-46.
https://doi.org/10.4236/etsn.2022.111003

Received: December 17, 2021
Accepted: March 14, 2022
Published: March 17, 2022



Abstract

An alarmingly high mortality and morbidity rate has been observed in COVID-19. As a new disease (similar group of SARS-CoV 2), it has been spread to more than two hundred countries and millions of people. However, COVID-19 infection is increasing in Bangladesh also. Therefore, an effective public health response is needed to control the outbreak of the mentioned new disease. If this high increasing factor turns out of control then it provides potential negative impact on social, economic, and political life of Bangladeshi people. One of the most effective ways to reduce or prevent the growth of COVID-19 is to wear masks. Many variants of COVID-19 are available in the world currently. Latest, there is a variant of omicron. This variant is too infectious. It means the vaccine seems to be not perfect against this deadliest disease COVID-19. However, people are not conscious enough about this matter generally. Nowadays, they are very reluctant to wear a mask. Their main thought is to get vaccinated and it can protect themselves. Definitely, the vaccine can protect at a certain level. However, Omicron proves that vaccine is not the ultimate solution. But, we can protect ourselves to wear a mask and keeping physical distance. This is the borderline of our research work. In this work, we proposed a system that will monitor the people who are outside the home/office via a close circuit camera. It evaluates whether the people are mask-free or not. If one does not wear a mask then an image will be captured and compared with database of national-data center for example NID server. As sensitive data, it needs security and protection. Hence, we adopt a cryptographic solution such as authenticated encryption or tag generation. As a result, receiver will be assured that a valid sender provides data to the valid re-

ceiver. The goal of this system proposal is to ensure wear face masks. As well, people will be punished based on the findings of mask-wearing. Furthermore, message authentication or tag generation secures sensitive information or data, because of accessing NID server. Specially, this model will be suitable for Bangladesh and other overcrowded countries. Because manmade or policing for all-time monitoring system is quite impossible for the populated country. Hence, we should start an automated system in a secure manner that can monitor the people.

Keywords

Face-Mask, COVID-19, Awareness, Public Health, MAC, Hash

1. Introduction

There are many ways to stop the spread of coronavirus worldwide that are not decent for us. Travel restrictions, remote office operations, country lockdown, and social isolation are all examples. As a low-middle income country with one of the world's most dense populations, Bangladesh is difficult to make these rules work in. It would be hard to do mitigation in many parts of the country because of social distance and because the government has limited resources. If things get worse, we can't even imagine going into lockdown for a long time. If you have to go into lockdown, it will have a big effect. Face masks can guard against COVID-19 and protect the public. When the COVID-19 pandemic spreads and people don't want to get sick, people are wearing face masks as a safety measure [1]. Infection rates have dropped, but the COVID virus is attacking people again because they have become careless and thought that only vaccination could protect them, which has been proven wrong by the rise in COVID cases again [2]. It's also very important to make sure that the message you send is true. It is very important to keep messages and personal information true in this world. Data security, identity verification, and authentication of the source of symmetric data can all be accomplished by employing symmetric techniques in association with MACs. Estimating the MAC of the user's files can help you figure out whether they've been changed, for example, by a virus or by an individual user. It is possible to keep track of the results and see whether they have changed, to make people more aware that they can wear masks and still be true to themselves. In this work, we'd like to talk about how to make sure people wear masks and protect the authenticity and other security issues of the NID information they send.

1.1. Motivation

Lockdowns, medicines, and public awareness campaigns helped Bangladesh fight coronavirus infections. The country is now facing its biggest crisis due to a fast surge in infection rates regularly rising numbers of diseased and dead.

1) In such circumstances, most sensible governments would choose an extended lockdown at a great financial sacrifice, based on the idea that people should be saved first, and the economic loss to the industry could be delayed. Lockdown is not a choice in Bangladesh, where a large proportion of the population lives on the margin of subsistence. If the government declares a national emergency, this must be resolved [3].

2) In Bangladesh, a vaccine alone cannot address the issue for long. Many people, especially in rural areas and poverty, have shown strong hostility to vaccination efforts, citing a lack of knowledge as a major reason for their objection. The perception of low infection risks, concerns about side effects, and the overall efficacy of immunizations all work against vaccination. Moreover, until recently, the government permitted all public and private institutions, religious institutes, and other similar groups to operate without oversight. Everyone suddenly believed that the country was on the verge of eradicating the coronavirus. But the reality is much different. Also, the immunization takes time to operate correctly in the body. As a result, immunization appears to be ineffective in this circumstance.

3) Masks are helpful in limiting the spread of COVID-19, according to the results of a large randomized investigation involving many people in diverse Bangladeshi areas. Despite the minimal outcome, the findings show how crucial masks are. Face masks significantly reduced serious infections among the elderly [3].

4) Apart from that, the use of MAC secures people's NID information in this system. Many industries use hash functions and symmetric encryption.

1.2. Backgrounds

In order to verify the authenticity of messages, the MAC method utilizes asymmetric key cryptography approach. The sender and receiver share a symmetric key K in order to maintain the MAC process. A MAC is a cryptographic checksum generated on the basic message and delivered with the message in order to assure message validation [4]. Message authentication and integrity are two security services that are supplied in the framework of message transmission. Algorithms providing message authentication do not secure non-repudiation (MACs). Some examples of practical implications of MAC include the Internet of Things, where GSM is used for networking, smart metering, and health parameter tracking.

A journal "Security Concerns with National ID Cards" in the previous work on NID issues introduced three primary parts of NID. The advantages and disadvantages of the National ID card were discussed; in the second, the security properties were discussed; in the third, the possible threats and their results were analyzed. In the security analysis part, the threats are discussed. ID cards, like much new technology, contain a variety of flaws that need to be properly considered. There is greater concern and intention behind identity cards, however, because if the National ID card is compromised, it will harm all citizens and

place the government that issues them in an embarrassing position. Falsification of Information, Man in middle attacks, Skimming attacks, Abuse by authorized personnel. Decrypting the data is the most important thing to think about regarding NID. Hence, NID information should be secured [5].

Previously, A model has been made to figure out how COVID-19 and other lung problems spread. This model came up with a way to measure and interpret behaviors like wearing masks and being alone. This model showed certain things, like how transmission risk and how far away you stay from each other are linked [6].

1.3. Objectives

The basic aim of the thesis study is to raise public awareness of COVID-19 dissemination in attempt to lessen its outbreaks. Thus the system's main objective is to issue warnings and sanctions to persons who don't wear masks or keep sufficient awareness. We discovered that merely vaccination is not enough and must be vigilant. Our main goal is to reduce the worrisome rise of COVID cases. Though it is also possible to utilize this technology to track and act in other areas, NID information is used for individual identification, and it must be kept secure because it contains sensitive data. That is why we employed MAC for authentication, a popular technology for secure communication. The intention is to maintain NID data security and no wrong identification during the system application procedure. The motive is to build a system that specially will be suitable for Bangladesh and other overcrowded countries.

- Reducing COVID spread.
- Tracking people who are not wearing mask and giving penalty to raise awareness.
- Using MAC ensures that no personal information is exploited and that authentication and authorization are maintained.

1.4. Outline

In Section 2, an overview of the proposed system is presented by modules specifications. Section 3 explains the system's implementation design. Section 4 discusses security aspects, and Section 5 provides future work insights. Section 6 concludes the whole model proposal.

2. Proposed System

2.1. System Overview

The first part of the work detects persons not wearing a mask. It will capture an image of that person's face only. The live camera will be checking everyone on the road. The camera is set up on an important road junction. With the help of image processing, people who are not wearing a mask will be detected and captured. After this, the image is matched with our local server database images to find the person's personal information. Suppose the image does not match with

anyone in the database. In that situation, it is forwarded to the national identity card server, which stores sensitive personal information of all NID cardholders. That captured image is matched with the pictures in this server. The person's name and NID number are sent to our local server immediately identified. For secure communication, the asymmetric algorithm is chosen. This system uses a whirlpool algorithm that will ensure personal information like NID number, name, address, email, etc has not been tampered with. Then, it will generate a message authentication code. Later, this code will be concatenated with the personal information and then sent to the receiver side, our local server. The MAC is verified on the receiver side for data authenticity and authorization. Simply with the help of the encryption algorithm, a tag will be generated automatically on the feeding of the information. The tag is only be verified by the one who has the secret key. This shared secret key is populated by Diffie-Hellman Key Exchange protocol. If the tag is valid, personal data will be saved in the local server for further action; otherwise, the message is discarded. Hence if some adversary tries a forgery attack on the personal information, it won't be possible and will be detected. After the tag validation, the email address will receive a warning message with a penalty alert. This is how people are charged. As a result, this fine makes them more conscious about wearing a mask which is the dedicated purpose of this system. In addition, **Figure 1** shows the general model view of the system. Moreover, **Figure 2** describes the activity diagram of the proposed system. Furthermore, the sequence diagram is represented in **Figure 3**.

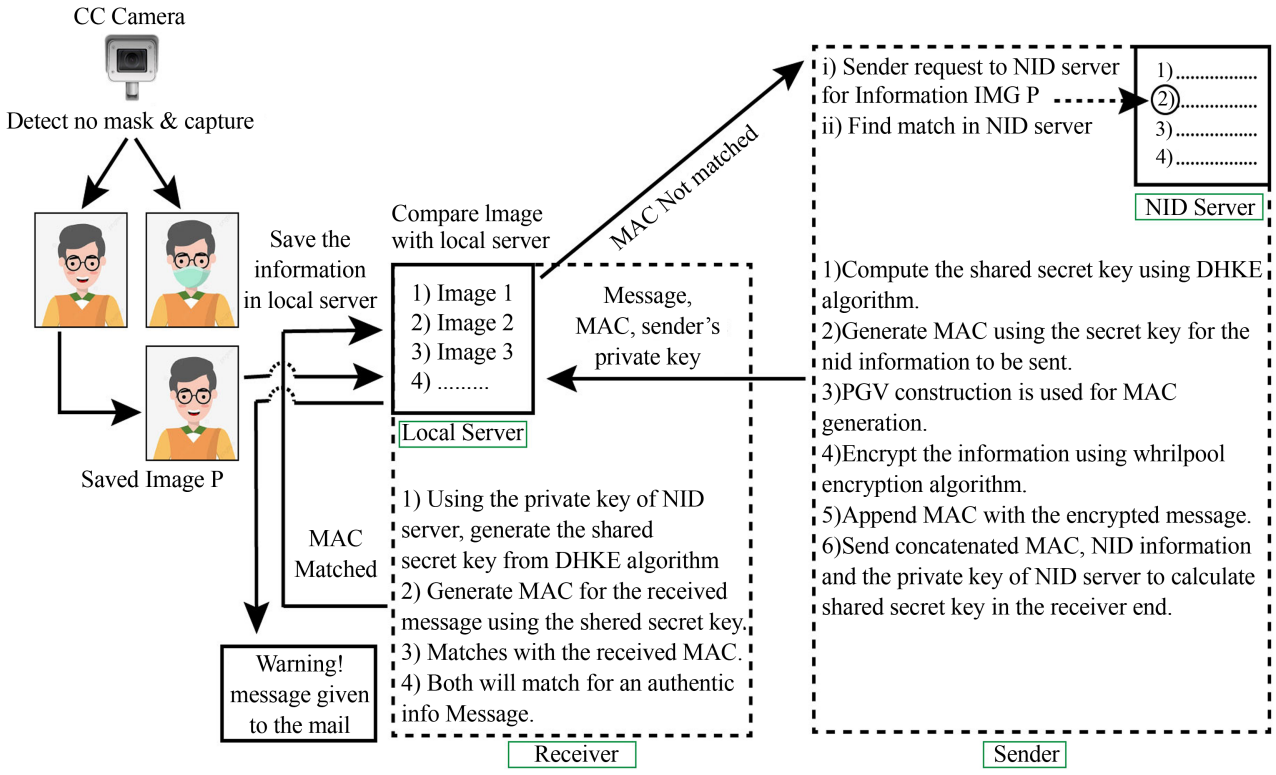


Figure 1. General structure of the system.

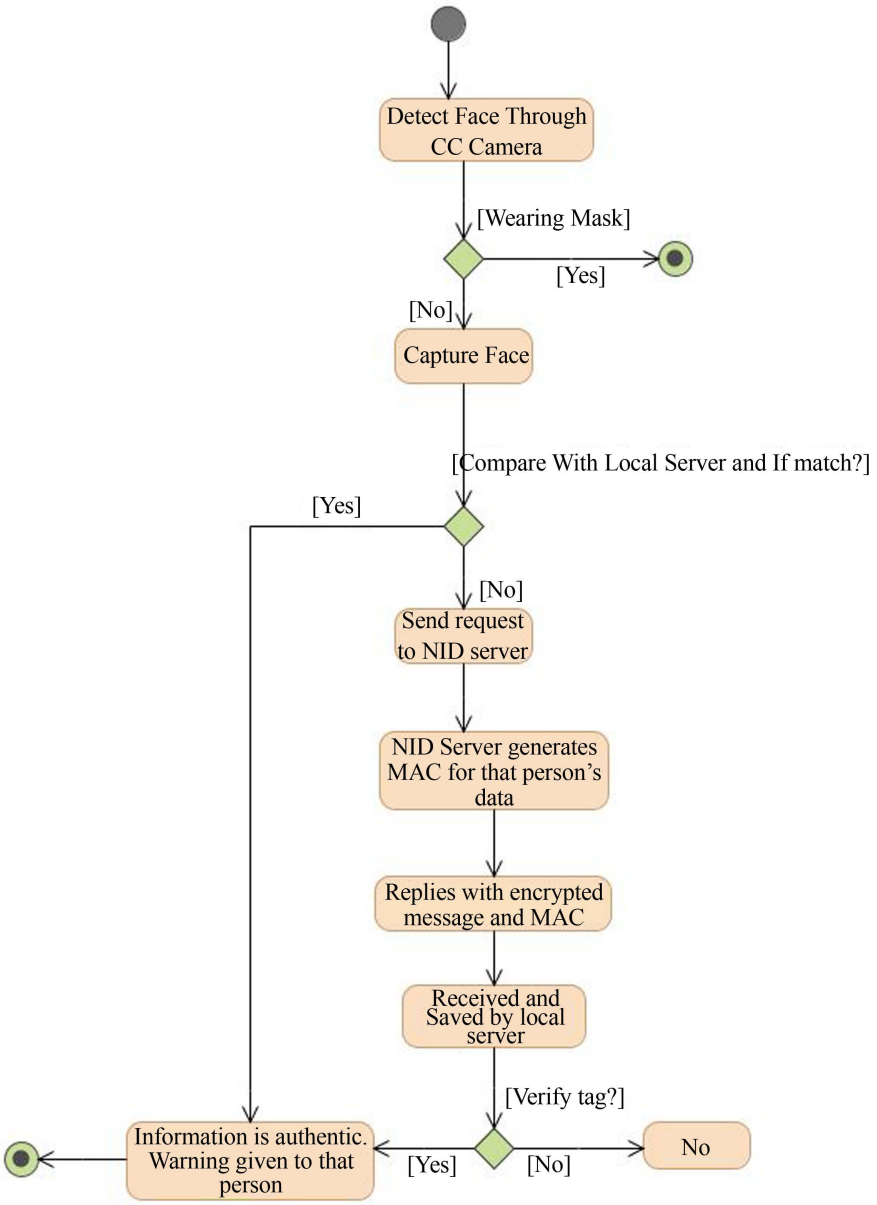


Figure 2. Work flow of the proposed system using activity diagram.

2.2. System Module

Each of the modules in this system falls into one of three types:

1) Live Camera

- Detect people who are not wearing the mask.
- Capture a picture of the face.

2) Local Server

- Name, National Identity Card number, NID image, E-mail id of people who have previously been caught guilty for not wearing a mask are stored in the database.
- Can match the captured image with people in the database.
- A warning message is sent to the e-mail address of that person.

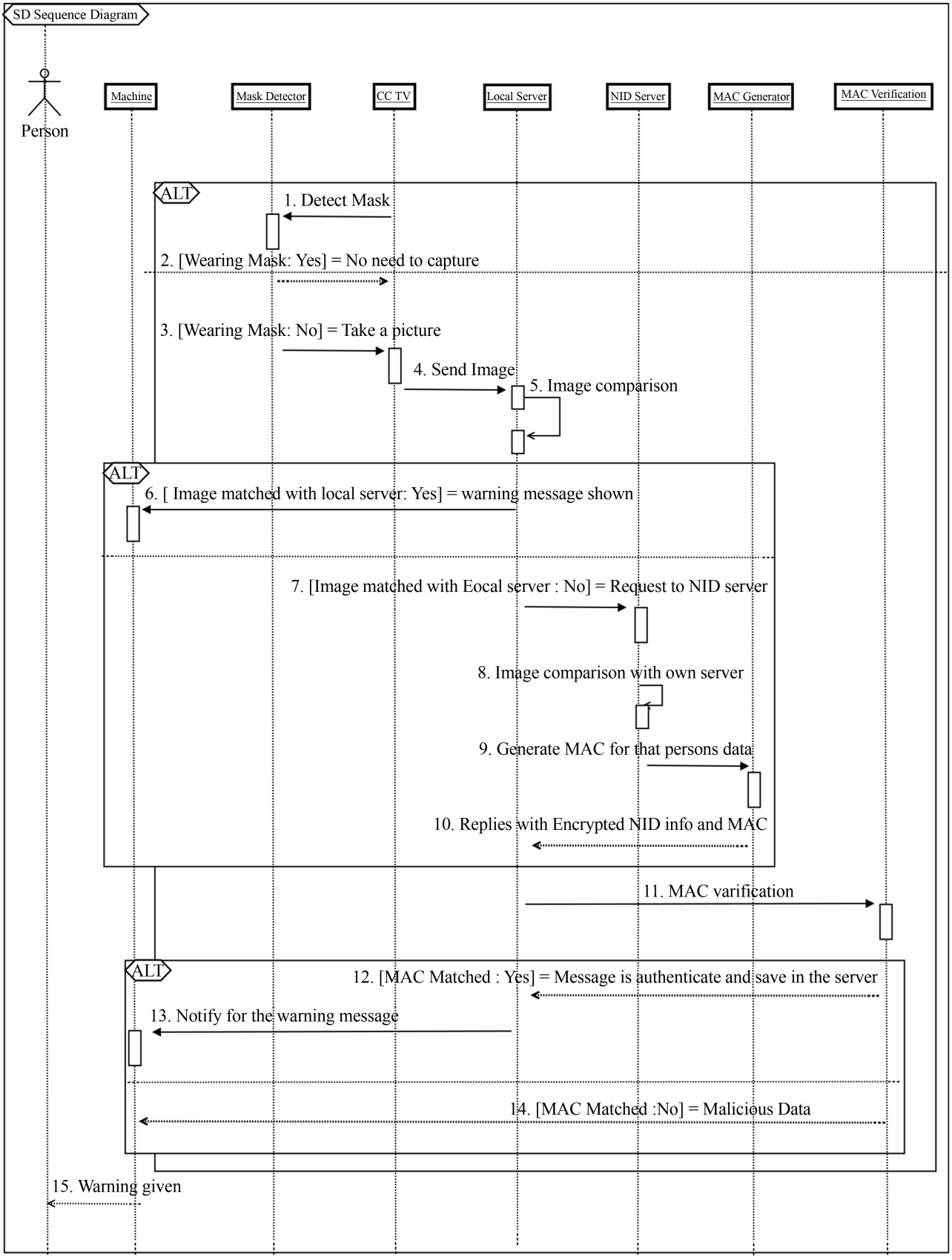


Figure 3. Work flow of the proposed system using sequence diagram.

- If not found in this database, requests to the national id server of the country for information.
- Generate shared key for decryption.
- Verify the message authentication code.

3) NID Server

- A database with all the personal details of national id holders living in the country.
- In reply to the request from a local server, asked information is transmitted securely.
- Generate shared key for encryption.
- Generate message authentication code and append it to the transmitted message.

2.3. Procedure

A framework is the functional assemblage of elements, materials, or components, as well as the corresponding communication and power flow that allows a mechanism, operation, or platform to produce the desired outcome.

1) Face mask detection: This Real-Time Face Mask Detection OpenCV Python program is developed using Python Detection OpenCV. In this project, a program is developed for face mask detection using Python, Keras, and OpenCV.

We can accomplish pretty much anything with OpenCV [7]. We need to know which modules and functions to employ. Face recognition isn't the same as face detection, which locates a face in an image. If our system marks any person without a mask, it first runs a face detector to locate the face, and then a face recognizer to identify the person. Face recognition is covered in one module. Then it will report those individuals to the NID server. A shape recognition algorithm analyzes visual data. For our project, this module recognizes the face, mask, and other ratios. Keras is a high-level deep learning API for neural networks. It's written in Python and helps implement neural networks., TensorFlow has incorporated Keras as its official high-level API. It's part of TensorFlow, which has built-in modules for all neural network computations [8]. The face mask detector program detects whether or not someone is wearing a mask. The model is trained using Keras with network architecture. Training the model is the first part and testing using a webcam using OpenCV is the second part. Whether there are any faces in a picture or clip, the intention of face detection is to identify those. There are bounded rectangles around all of the faces when there is more than one, so we understand exactly where each one is.

2) Message Authentication Code: A MAC is a hash function that accepts a secret key as an input, and the basic security requirement is that it should be computationally impossible to guess the tag value of a message without the key [9]. Rather than the actual text itself remaining secret, key privacy becomes something even more significant and essential. Diffie-Hellman Key Exchange is used to accomplish the purpose of exchanging a shared secret key that generates

a shared secret utilizing the private keys of the sender and the receiver. MAC computations provide the wrong output if the content of the message is being altered during transmission. Message authentication and integrity are both offered as security services in terms of message transmission [10]. The algorithm in this system is adopted from the PGV compression function [11]. The block cipher algorithm used for this structure is whirlpool which uses 512-bit blocks of data and a 512-bit key.

3) Socket Connection: Following the capture, the image is checked against the database. If not, transmit the image to the NID server for more details. The connection between the NID server and the local server is made via socket programming. Both ends of the link are connected [12].

Socket programming is a way to connect two network nodes. This means that one socket (node) listens on a specific port at an IP address, while the other socket establishes a connection. The server creates the listener socket while the client connects to the server. A listener socket is created while the client connects to the server. These are the core web services. Simply put, there is a server and a client. Socket programming begins with importing the socket library and constructing a simple socket. Both ends of the link are connected. Socket programming is also used to send warning messages [13].

3. Implementation Design of Proposed System

The system implementation is planned to perform in a few consecutive steps. A block diagram is used to show the planning of the system implementation (**Figure 4**). The waterfall model is being used to build an entire system (**Figure 5**).

The main features are depicted in **Figure 4** in a progressive manner. The first step is to capture a photograph of the person without a mask on their face. Then, in order to send a warning email, this image is compared to its own local server for personal information. If the image does not match, a socket connection is created with the NID server to allow for further communication with it. The details of the person are requested by the local server. As soon as they locate the requested information, they are securely transmitted to the local server with the

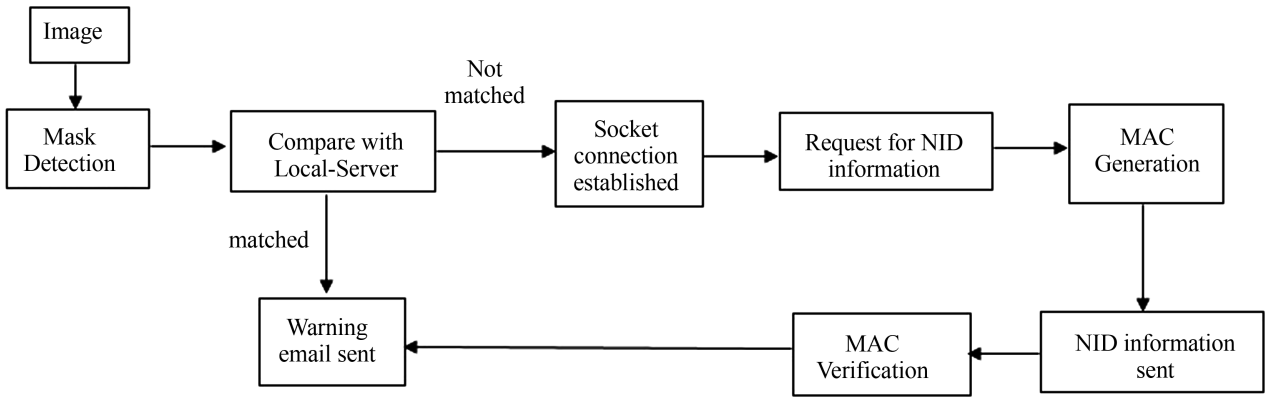


Figure 4. Proposed system data flow.

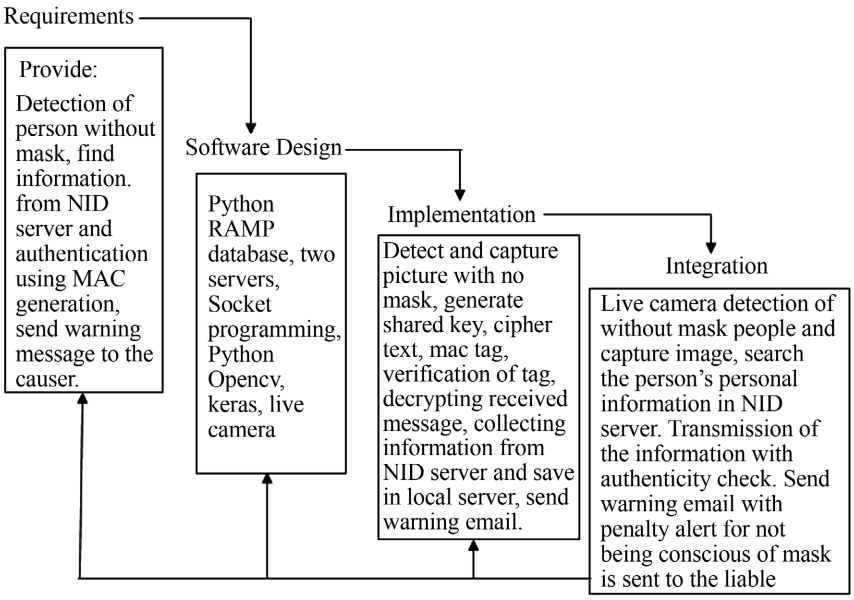


Figure 5. Development process is shown using waterfall model [14].

use of a MAC (Message Authentication Code) that is sent together with the NID information. The MAC is validated at the receiving end, which is the local server of the system. As a consequence, the local server sends a warning email. These tasks are carried out by the three modules that are detailed more below.

1) Live Camera Module:

Part one involves training the model, while part two involves testing it with a camera and OpenCV. The purpose of face detection is to assess whether or not there are any faces visible in a picture or video clip. In this project, a program for face mask detection is created using Python, Keras, and OpenCV. The face mask detector program is being developed to determine whether or not a person is wearing a mask. **Figure 4** describes the data flow of the proposed system.

2) Local Server:

For testing purposes, the database is created using XAMP.

After capturing a person's picture, it will be matched with the database whether it is already there. If not, then send the picture to the NID server for requesting details. The connection between NID server and the local server is established using socket programming and also used to send warning messages.

When the data is received, the tag is verified. It will implement the verification algorithm on the received message and compare it with the received tag. Matching of the tags assures that the message is authenticated. Otherwise, the message will be discarded.

3) NID Server:

This server is created with all the national ID card holders' details. This system creates a dummy database using XAMP with 50 data entries for testing.

Socket programming establishes a connection with the local server, which requests the details of the corresponding image. Thus it compares that image and searches for the details.

Only the nid number, name, and email address are sent from the database using whirlpool encryption and MAC generation.

4. Proposed System Security Discussion

The inspection and evaluation of many elements that can impact the security of a system are known as security analysis. An intruder or an unauthorized individual will not access any of the system's components or data unless the task has been completed. In other words, the system will be fully safeguarded against any potentially hazardous actions. The tag provides the main security. The tag is generated by whirlpool algorithm where the size of the key is 512 bits which outputs a 512-bit-sized tag [15].

Any forging of the message, whether malicious or unintentional due to transmission faults, will be discovered by the recipient due to failed tag verification. All bits of the message are crucially significant to the MAC. The concern is for the shared secret key, which is also exchanged using a secure protocol Diffe-Hellman. To offer strong security, a random large prime number used in the protocol has a value of 1024 bits or above. In addition, the whirlpool method has a robust overall structure that has demonstrated to be resilient to the conventional threats on block-cipher-based hashes. Whirlpool is significantly more scalable than most recent hashing methods encourage large parallel execution of the component mappings. Also, it does not require a great amount of storage space. It may therefore be implemented efficiently in various situations with limited resources. Still, it can benefit from the bigger cache memory available on newer CPUs to gain higher speed. The hash length is also extremely high, which not only gives improved security against birthday attacks but also allows for a larger internal state for entropy confinement, which is necessary for certain kinds of pseudo-random number generators [16].

5. Future Work

Message authentication is a critical aspect when it comes to real-world applications of cryptography. As a result, it's interesting to see if existing structures can withstand the IoT environment and big data platform while still being secure and efficient. We will continue our activity with a formal and strict security margin. In addition, we'll run simulations of the innovative and more applicable ideas and compare them to tested ones. We will be progressing in the security proofs to be more concrete. This work is just a proposed model. So the main future work is to implement it and see how it results. Based on that, the efficiency can be improved in terms of the requirements. Our work is theoretically grounded; thus the efficiency is not quantified mathematically. If it runs quite appropriately, we would be focusing on implementing it in bigger projects in real life. This work has much more scope in the future.

6. Conclusion

In this study, we explored how with currently available technology, we can de-

sign a new mechanism that will be beneficial to reduce the COVID-19 rising issue. This concept is developed in the context of Bangladesh based on the goal to enhance public knowledge of COVID dissemination in an attempt to reduce breakouts while also ensuring the security of personal information. Several technologies already provide authentication. Researchers are continually developing new ways to incorporate the MAC Algorithm into data solutions to improve transparency, security, and immutability. It is now possible to acquire significant reliability over a solution with the help of MAC. As a result, we've decided to use MAC for our case, which is the purpose for safeguarding the management of smart national identity cards in the main architecture. Our proposed architecture is capable of protecting data against unauthorized changes. We expect that by using this architecture, the government will safeguard other systems that require high levels of security. Implementation of this application can ensure mask-wearing awareness as well as preserve and protect the authenticity of sensitive data. Bangladesh will benefit from this application that monitors mask use and protects the authenticity and other security threats of NID information used for citizen identification.

Acknowledgements

We would like to express our gratitude to a number of individuals who assisted us in the creation of this project report. Our teammates and teachers were always willing to help by providing knowledge and expressing their own thoughts. This is our opportunity to express our appreciation to everyone on our team for their hard work and dedication to this work. We gathered information from a group of organization, each of which provided various instructions for preparing this document. We would also like to thank the programmers who worked hard to help develop this paper.

We hope that our report will be of assistance to you.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Venkatesan, P. (2021) NICE Guideline on Long COVID. *The Lancet Respiratory Medicine*, **9**, 129. https://doi.org/10.1016/S2213-2600(21)00031-X

[2] Green, J., *et al.* (2021) The Implications of Face Masks for Babies and Families during the COVID-19 Pandemic: A Discussion Paper. *Journal of Neonatal Nursing*, **27**, 21-25. https://doi.org/10.1016/j.jnn.2020.10.005

[3] Anwar, S., *et al.* (2020) COVID-19 and Bangladesh: Challenges and How to Address Them. *Frontiers in Public Health*, **8**, Article No. 154. https://doi.org/10.3389/fpubh.2020.00154

[4] Message Authentication. https://www.tutorialspoint.com/cryptography/message_authentication.htm

[5] Alkhurayyif, Y. (2013) National ID Cards. *International Journal of Computing Science and Information Technology*, **1**, 44-48.

[6] Mittal, R., *et al.* (2020) A Mathematical Framework for Estimating Risk of Airborne Transmission of COVID-19 with Application to Face Mask Use and Social Distancing. *Physics of Fluids*, **32**, Article ID: 101903. https://doi.org/10.1063/5.0025476

[7] https://docs.opencv.org

[8] Keras API Reference. https://keras.io/api

[9] Preneel, B. (1997) Hash Functions and MAC Algorithms Based on Block Ciphers. *IMA International Conference on Cryptography and Coding*, Vol. 1355, 270-282. https://doi.org/10.1007/BFb0024473

[10] Paar, C. and Pelzl, J. (2009) Understanding Cryptography: A Textbook for Students and Practitioners. Springer Science & Business Media, Berlin. https://doi.org/10.1007/978-3-642-04101-3

[11] Black, J., Rogaway, P. and Shrimpton, T. (2002) Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. In: *Annual International Cryptology Conference*, Springer, Berlin, 320-335. https://doi.org/10.1007/3-540-45708-9_21

[12] Socket Programming in Python. Geeks for Geeks. https://www.geeksforgeeks.org/socket-programming-python

[13] How to Transfer Files in the Network Using Sockets in Python. https://www.thepythoncode.com/article/send-receive-files-using-sockets-python

[14] SDLC Waterfall Model. https://www.tutorialspoint.com/tutorial_view.htm?cid=sdlc&pid=sdlc_waterfall_model.htm

[15] Stallings, W. (2006) Cryptography and Network Security. Pearson Education, Delhi.

[16] Barreto, P.S.L.M. and Rijmen, V. (2000) The Whirlpool Hashing Function. In First Open NESSIE.