Global Journal of Medical Research: K Interdisciplinary
Volume 22 Issue 2 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4618 & Print ISSN: 0975-5888

A Practical Approach of Central Monitoring Management System that Ensure Mask Wear to Prevent the Spread of COVID-19 in Bangladesh

By Shaznin Sultana, Raisa Tahsin Taspia, Sadia Afreen, Nafiz Al Asad & Rashed Mazumder

Bangladesh University of Professionals

Abstract- The infectious spread of corona-virus disease (COVID-19) has been prevailing in more than two hundred countries and causing millions of deaths worldwide. The pandemic has wreaked havoc in all sectors of life. Since COVID-19, the most common and effective preventive measure to control the transmission has been to wear face masks. With the decline of infectious virus cases in most countries due to vehement vaccination programs, people are now reluctant to wear masks. However, the recent variants of the virus, such as Delta, Omicron, etc., have proven to be resistant to a degree against vaccines. So, there is no alternative to wearing masks to protect ourselves and those around us. The proposed work in this paper implements a full-proof automated system to detect whether a person has worn a mask and warns the person if he has not.

Keywords: facemask, COVID-19, consciousness, public health, MAC, hash.

GJMR-K Classification: DDC Code: 616.2 LCC Code: RC776.S27

Strictly as per the compliance and regulations of:

A Practical Approach of Central Monitoring Management System that Ensure Mask Wear to Prevent the Spread of COVID-19 in Bangladesh

Shaznin Sultana [α], Raisa Tahsin Taspia [σ], Sadia Afreen [ρ], Nafiz Al Asad [ω] & Rashed Mazumder [¥]

Abstract- The infectious spread of corona-virus disease (COVID-19) has been prevailing in more than two hundred countries and causing millions of deaths worldwide. The pandemic has wreaked havoc in all sectors of life. Since COVID-19, the most common and effective preventive measure to control the transmission has been to wear face masks. With the decline of infectious virus cases in most countries due to vehement vaccination programs, people are now reluctant to wear masks. However, the recent variants of the virus, such as Delta, Omicron, etc., have proven to be resistant to a degree against vaccines. So, there is no alternative to wearing masks to protect ourselves and those around us. The proposed work in this paper implements a full-proof automated system to detect whether a person has worn a mask and warns the person if he has not. The proposed method works in several parts: monitoring to detect persons without masks using a close circuit camera, evaluating whether they are wearing a mask using a machine learning algorithm, capturing their pictures, then comparing with the NID database in a secure way. Finally, the persons without masks are notified via email. As the data fetched from the NID database is a piece of private and sensitive information, we have proposed a cryptographic solution of authenticating message or tag generation to assure the validity of the data sent by a valid sender. Therefore, a fully automated and secured system is proposed that is suitable for densely populated countries like Bangladesh where real-time monitoring is unachievable. The mentioned system is an efficient working implementation of a paradigm proposal published very recently. [1]

Keywords: facemask, COVID-19, consciousness, public health, MAC, hash.

I. Introduction

COVID-19 is a highly infectious disease with an extreme morbidity rate. The key reasons behind the recent drop in infection rates is public health awareness by wearing masks, social distancing, country lockdown, travel bans, etc. However, it is impossible for a country with limited resources such as Bangladesh to carry on with extreme preventive measures. Hence, it is strongly recommended to wear masks as it is the easiest and the most effective safety measure for stopping the spread of the virus. Face masks could be effectively used as a preventive measure in a COVID-19 pandemic [1]. Vaccination percentages have risen; however various strains of the COVID virus continue to spread the disease since people became careless and believed that vaccination might be the only means of protecting themselves [2]. Simultaneously, we must take action to reduce transmission while expanding vaccination coverage. It is accomplished with simple instructions, such as using a well-fitted mask. Right now, the most critical issue is to make sure you do not even get vulnerable to infection. In the proposed system, the person detected without a mask must be notified, which is done securely. The captured photo of the person is sent to the NID database to compare, and the personal information of the said person must be sent back to the system in an authentic way. Consequently, the proposed method generates message authentication codes to encrypt the user's data and verify the data altercation by a virus or a third party. After proper verification, the system notifies the person via email and warns about the further actions to take if they continue to be unwilling to wear masks. Thus, the study proves to be a protected system that ensures the wearing of masks by the public as a safety measure against the COVID-19 pandemic.

a) Problem Statement

With the frequent detection of more infectious COVID-19 variants, it is vital to wear masks for minimizing COVID-19 expansion effectively. However, citizens are not sufficiently conscious of the risks, and are reluctant to wear masks. Therefore, this research implements a system that ascertains citizens wearing masks by detecting mask-free individuals. It also warns them, followed by penalization if necessary. The system uses authenticated encryption or tag creation approach, thus making the system exceptionally secured.

b) Rationale of the study

Like the entire world, Bangladesh was able to control corona-virus outbreaks with maintaining lockdowns, medications, and public awareness campaigns. The arrival of the Covid-19 epidemic has inflicted a massive blow on Bangladesh's economy. But lockdown, vaccine activities are not a permanent solution to prevent covid-19.

Author α σ ρ ω: ICT, Bangladesh University of Professionals, Dhaka, Bangladesh. e-mail: shaznin1916@gmail.com
Author ¥: Jahangirnagar University, Savar, Dhaka, Bangladesh.

[1] The preliminary version of this work has been published into ETSN, SCRIP [17]

While vaccination can be a viable solution, in this scenario, public perception makes it insufficient. The public's dissatisfaction stems mostly from vaccination side effects, limited efficacy, and unavailability. On the other hand, a prolonged lockdown would be the prudent choice for most governments in these increasingly dire conditions. Because of the lengthy country-wide lockdown, the global economic crisis, and the resulting disruption of demand and supply chains, the economy is likely to experience a prolonged slowdown in recent months. Moreover, people of Bangladesh are not conscious enough about wearing facemasks. Results from unbiased research involving a large number of participants in various Bangladeshi locations show that wearing masks can prevent the spread of Covid-19. Despite the dismal outcome, the studies demonstrate how important face masks are. Face masks have been shown to drastically prevent severe infections in the older population [3]. Other than that, MAC is used to authenticate NID data in this system. The usage of hash functions and symmetric encryption is widespread.

c) Research objectives

The study's main goal is to raise public awareness of COVID-19 outbreaks in order to reduce outbreaks. As a result, the system's primary goal is to send warnings and fines to the non-mask bearing persons or maintain enough awareness. As vaccination can not provide entire protection. Our primary objective is to slow the alarming progression of COVID cases. However, this technologies might also be used to track and act in other areas. NID data is used to identify individuals and must be kept safe since it contains sensitive information. For authentication, we used MAC, an established way for secure communication. The objective is to maintain NID data security and no erroneous identification during the system application procedure. The motive is to design a system that will be suitable for Bangladesh and other overcrowded countries.

- Limiting the COVID dispersion
- Those who do not use masks are being tracked down and penalized to increase awareness.
- The use of MAC ensures that no personally identifiable information is accessed or manipulated, and that authentication and consent are maintained.

II. Background

This section provides a detailed discussion of related works on COVID-19 dissemination, mask ensuring works were previously done, NID security and MAC in security.

This paper presents an analysis of the current COVID-19 condition in Bangladesh, as well as some recommendations on how the government could address the crisis. Considering its economic position, Bangladesh is fighting the disease's spread. Almost all country has embraced nontherapeutic methods, but there is a continuous discussion about whether they have been adequately understood and applied. Bangladesh being a low-middle-income country, is subjected to several regulations aiming at minimizing the virus's spreading. This research focused solely on the medical situation in Bangladesh and the constraints in preventing the development of COVID [17]. It depicted the entire COVID condition in Bangladesh, as well as the irresponsibility of people who were not wearing masks. While maintaining the lockdown at all costs with increasingly stringent maintenance, the country is confronted with severe problems. As a result, a new viable approach may be able to reduce the rising COVID problem. Considering the circumstances in Bangladesh, no other model was presented [3].

COVID-19 and other respiratory problems have been studied in the past using a model. In this approach, behaviors like wearing masks and being alone may be measured and interpreted. This model demonstrated a number of things, including how transmission risk and the distance between two linked up people [6].

Their research indicates that broad public usage of face masks could be highly beneficial in reducing communal dissemination and crisis impact. Face masks are estimated to have the most community-wide advantages if used in association with non-pharmaceutical techniques and when adoption is almost uniform, and concordance is strong [7].

In the previous study on NID concerns, the publication "Security Concerns with National ID Cards" introduced three major components of NID. The pros and limitations of a National ID card were covered in the first section, followed by a discussion of its security features and finally a look at prospective threats and their impacts. The threats are detailed in the security analysis section. Many modern technologies, such as ID cards, have faults that need to be considered. Man-in-the-middle attacks, skimming assaults, and authorized personnel have abused the system are all examples of data falsification. Most of the confidential information is disclosed unintentionally - and occasionally intentionally - by the general populace which demonstrates the importance of NID data protection. The purpose of this study is to examine the defining characteristics of national ID cards, the security characteristics of resident ID cards, potential risks, and access controls [5].

Entities from across the world are attempting to grow the maximum cyber security mechanism. The information they convey is usually highly secretive which can be misused. Today, information security is becoming highly significant. To verify the validity of messages, the MAC technique uses a symmetric key cryptography strategy. The MAC approach uses a symmetric key cryptography strategy to check message

correctness. To keep the MAC process running, the sender and receiver exchange a symmetric key K. A message authentication code (MAC) is a cryptographic checksum created on the core message and sent with it to ensure message legitimacy. [4]. Message authentication and integrity are included in the security characteristics of message transmission. Examples of practical MAC applications include the Internet of Things, where GSM is used for networking, smart meters, and health parameter tracking.

III. Theoretical Framework

The implementation of this work is intended for major road crossings [17]. The system's data is arranged into two tables. These are referred to as the Local Server and the NID Server. Even though the system is based on real-time data, the data on the servers is drawn from practical scenarios. The initial function of this system to identify those who are not wearing a mask. The live camera will be looking over everyone's face while they travel along the road. The camera is deliberately placed at a major junction. Individuals without masks will be identified and captured using image processing algorithms. Following that, the image is compared to pictures stored on our local server database to determine personal information of the person. This storage is for the purpose of not accessing the NID server more than once for the same person. So, for instance, suppose that the image does not correspond to anyone in the database. The info is sent to the national identity card server, which keeps track of sensitive personal data for all NID users. Obtained image is compared to the images stored on this server. Name, NID number, and some details of that person are transmitted to the local server which is promptly identified.

A symmetric approach is selected to provide secure communication. The whirlpool method is used in this system to ensure that personal details such as NID numbers, names, contacts, and mailing addresses is not altered with. After that, it will engender an authentication code for the message. When this MAC identifier is combined with the personal information to be communicated, it is delivered to the sender's side, which is our own local server. On the receiving end, the MAC is evaluated to ensure that the data is genuine and allowed. A tag is computed when the information is sent into the tag generation algorithm. Those who possess the secret key are the only ones who can authenticate the tag. The Diffie-Hellman Key Exchange protocol is required for generating this shared secret key. The information received is removed if the tag is not valid; if the tag is legitimate, Personal information is stored on a local server for onward purpose. If an attacker attempts to fake personal information, it will be impossible and will be identified because of the security measures in place. Following the tag validation, the email address associated with the tag will receive a warning message. For getting caught more than twice, he will receive an email containing a penalty alert. People are charged in this manner. Because of this, they are more conscientious about wearing masks, which is precisely what this approach is designed to do. In addition, the flow diagram of the suggested system is depicted in Figure 2.1: [17]

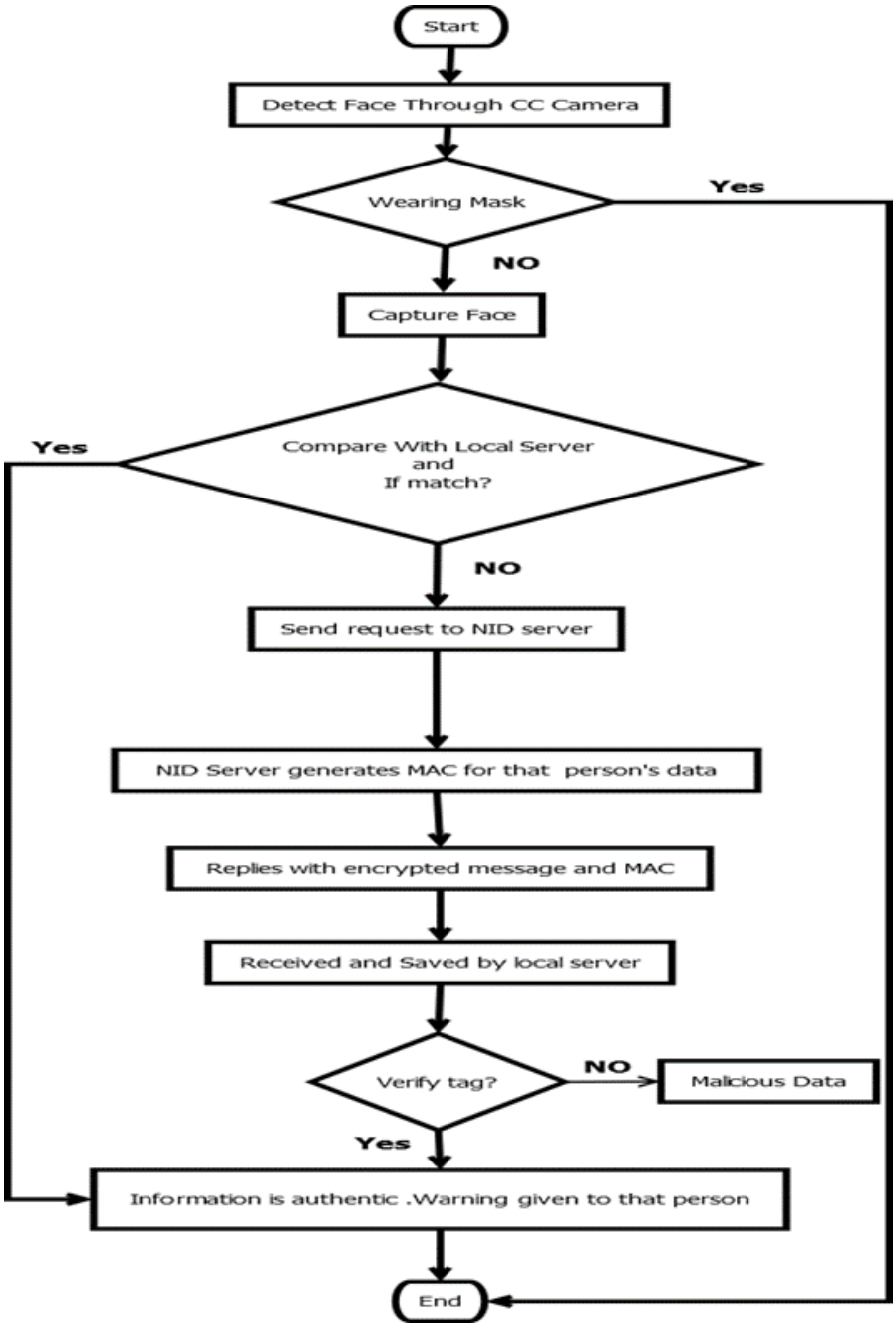

Fig. 2.1: A flow diagram depicting the proposed system's workflow [17]

IV. Research Methodology

This chapter covers the several approaches utilized in the procedure, data collection, and analysis pertinent to the work. It will incorporate the work sequence, research design, frameworks, data gathering, and security management.

The system implementation has been conducted in a series of steps. A general model diagram depicts the system implementation design (figure 2.2) [17].

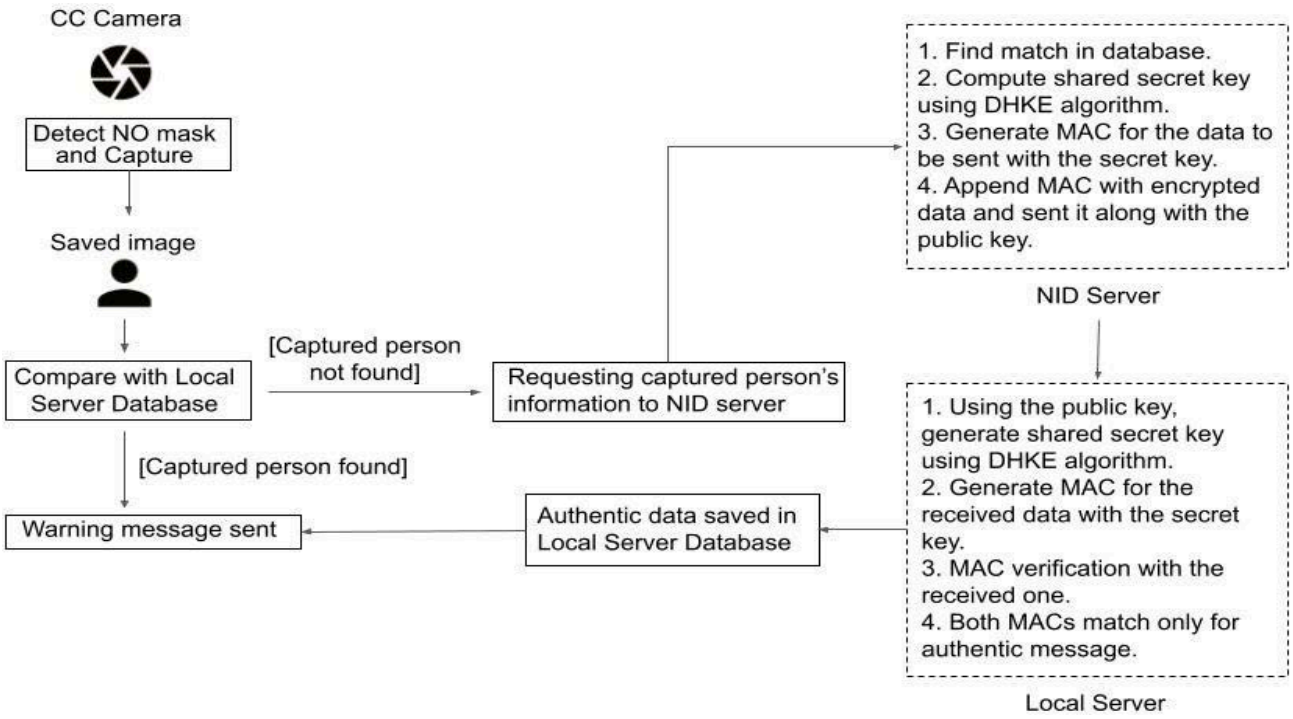

Fig. 2.2: General structure of the system [17]

This section depicts the critical components of a progressive approach. The tasks are conducted via three modules which are described below in detail.

The first step is to capture the individuals without a mask on their faces. To send a notice statement, the photo is matched to its local server for personal details. For subsequent interaction with NID server, a socket connection is made if the image could not be resembled. The person's data is collected by the local server. When they find the necessary details, these are securely sent to the local server using the MAC (Message Authentication Code) and NID details. The MAC is checked at the system's local server on the receiver section. As an outcome, the local server sends an email notification to the guilty.

1) Face Mask Detection

The main functionalities of this module are:

- To recognize individuals who might not be wearing a mask.
- Take a photo of the individual's face.

Using Python, Keras, and OpenCV, a code for face mask identification is constructed within this module. The mask scanner algorithm is being designed to assess whether or not someone is putting a mask. Face detection is intended to evaluate whether any faces are viewable in a photograph or film footage. Face detection finds a face in an image. A face detector locates any uncovered individual recognized by the system, subsequently detected by a facemask recognizer. A face, mask, and other ratios are recognized by this module. Keras is a deep learning framework with a high-level interface [9]. When there are multiple faces, a bounded rectangle surrounds each oneso we know where they are. Captured face image is sent to the server to find out the person's identity.

2) Local Server

The main functionalities of the local server are:

- Comparing the image collected with those in the directory.
- If information isn't available in this database, contact the national id server.
- That person receives a warning notice.
- To validate the message authentication code, construct a shared private key.

Local server is a database containing names, national identity card (NID) numbers, NID images, E-mail addresses of those who have been found guilty of not using masks in the past. The dataset is prepared with XAMP for trial objectives. As soon as the person with no mask is detected and captured through the CC camera, it is matched with the database whether it is already there which is finding out if the person has been caught before. If not, the image is transmitted to the NID server for more information. Socket programming is used to make a link here between NID server and the local server and to convey warning mails. The tag is confirmed after the NID feedback is gathered. The verification algorithm will be applied to the received message to get its corresponding tag and compared to the received tag. The authenticity of the communication is ensured by matching the tags. If not, the data will be erased.

3) NID Server

The main functionalities of the NID server are:

- The requested records are securely delivered in response to a request from the local server.
- Compute shared secret key for tag generation.
- Addition to creating a message authentication code and concatenate it to the message to be delivered.

The NID server in this case is a dummy dataset built with XAMP and fifty data records for demonstration reasons, which holds all of the personally identifiable information of national ID holders in the country. A connection is established with the local server for requesting the details of the person in the captured image. It then analyzes the two images and looks for information. As soon as the person is found, their NID number, name, and email address are sent to the local server. A message authentication code (MAC) is generated and appended to the encrypted message to be sent.

V. Result Discussion

The purpose of this chapter is to present an observation of the experimental data obtained using the constructed model. This portion also discusses the outcome of each phase and the method that we employed in our model.

The shared secret key is calculated at first using the Diffie Hellman Key Exchange protocol. This system utilizes Diffie-Hellman Key Exchange to distribute a shared secret key producing the private keys of both the source and the destination. The Whirlpool algorithm is used to encrypt the message and construct the tag. Whirlpool is a block cipher that encrypts data with 512-bit blocks and a 512-bit key. Tags are generated using this shared secret key. The message is attached with the Message Authentication Code (MAC) and sent to the local server from the NID server. We used a socket connection between the NID server and the local server for requesting and transmission of data. Socket programming is used to establish a connection between two network nodes. The link is connected on both ends [13]. The first steps in socket programming are to import the socket library and create a simple socket. Both endpoints of the link are connected. Warning messages at the last step are also sent via socket programming [14]. The receiver side, which indicates the local server, follows the same approach. The same implementation is used to generate the MAC compared to the MAC obtained from the sender-NID server. As soon as the authentication is completed, the local server verifies the message's authenticity and saves it in the database for later alerting notifications.

The purpose of using MAC is validation of data transmission. A MAC is a hash function that utilizes a secret key as well as the data as input, and the security protection constraint is that estimating the tag value of the data without the key should be operationally challenging [10]. The MAC estimations yield an error in the data if the original message is altered throughout transmission. Message authentication and message integrity are offered as security facilities for communication processes [11]. The tag formation mechanism employed in this system is derived from the PGV compression function [12].

a) No mask detection

When someone approaches the machine without wearing a mask, the machine identifies this and snaps a photo of them.

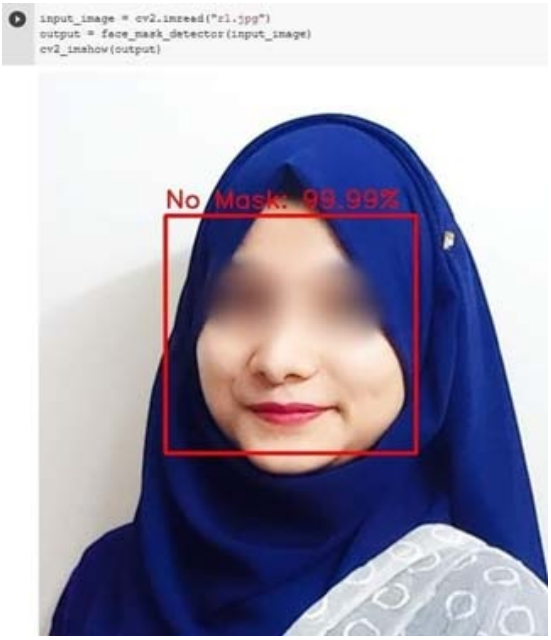

Fig. 3.1: No mask detected

b) Local Server

A picture that is taken at the start will be compared to the one that is already on its own server. If the picture is found in the database, it email to the person's email address warning them about the picture and what to do. If the image cannot be found on the local server, then the image will be sent to the NID Server for more information about what it is.

No	Image	Name	NID	MailID	ConcatenateMessage	MacValue
1	[BLOB - 7.3 KiB]	ARSHIA HABIB	7184456708	arshia@gmail.com	ArshiaHabib7184456708arshia@gmail.comb' E\x17\\x0...	b' E\x17\\x0bXq\x00[^UU\x01\x01R\x02\x06\x01U\x03...
2	[BLOB - 13.3 KiB]	MD. MUMINUL BARI	6184456708	mumin@gmail.com	MDMuminulBari6184456708mumin@gmail.comb'z[z\x10[P\...	b'z[z\x10[P\nDX!SDQU\x06\r\x04R\x05\x0eQQ\n\X\x14X\...
3	[BLOB - 5.6 KiB]	FOYSAL AL GABID	5151856708	foysal@gmail.com	FoysalAlGabid55151856708foysal@gmail.comb'=_M\x16\...	b'=_M\x16\x07[%Xf\x04Q\x08Q\x07\x00\x03\x03\x04\n\...
4	[BLOB - 3.6 KiB]	Md. Sujaur Rahman	6454310268	suja@gmail.com	MdSujaurRahman6454310268suja@gmail.comb'{\x02fD^SB...	b'{\x02fD^SBGdPZXWX\x06\x0cV\x01U\x08\x03SUZ\x15AX...
5	[BLOB - 105.8 KiB]	Shaznin Sultana	6490576885	shaznin22@gmail.com	ShazninSultana6490576885shaznin22@gmail.comb'0vRL...	b'0vRL^\i^dB^\x12\x04\r\x00W\x04XT\x03TU^tT\x17^...
6	[BLOB - 178.5 KiB]	Sadia Afreen	5090306855	sadia13@gmail.com	SadiaAfreen5090306855sadia13@gmail.comb'a\x03Q]SvP...	b'a\x03Q]SvP\x11\x01\x06\x0fVV\\V\nSUZTP\x16\x05\x...
7	[BLOB - 6.2 KiB]	MD. SAJJAD HOSSAIN SAWRAN	5183456902	sawran@gmail.com	MD.SajadHossainSawran5184456708sawran@gmail.comb'...	b'.`L `\x00\x0e^PWy\x0cGFP\x0b\rgX\x15K\x03]\x03P\x...
8	[BLOB - 12.2 KiB]	MEHEDI RIDOY	7403275517	ridoy06@gmail.com	MehediRidoy7403275517ridoy06@gmail.comb'/RQVS\x08a...	b'/RQVS\x08a\\Wt\K\x0f\r\x07\x04\x0bR\x07\x00\x06\x...

Fig. 3.2: Local server

Using socket programming, the NID server connects to the local server.

c) Socket Successfully Establish

```
c, addr = s.accept()
print ('Got connection from', addr )

# send a thank you message to the client. encoding to send byte type.
c.send(bytes('Thank you for connecting'),"utf-8")
```

Fig. 3.3: Connection setup

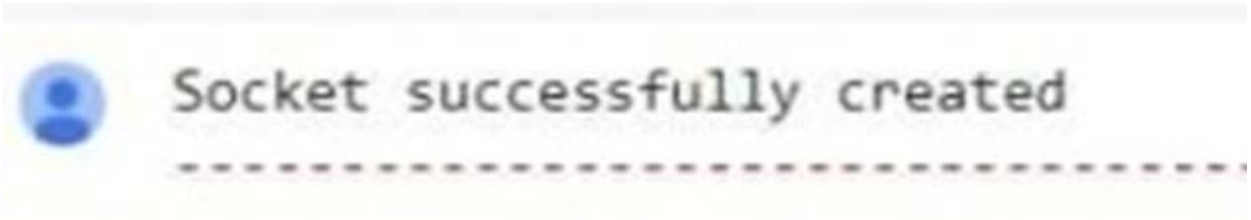

Fig. 3.4: Socket establishment

d) NID Server to Compare Detected Image

Image captures are forwarded to NID if they cannot be found local server. After comparing the NID image to the captured image, the next step is to proceed to the next step.

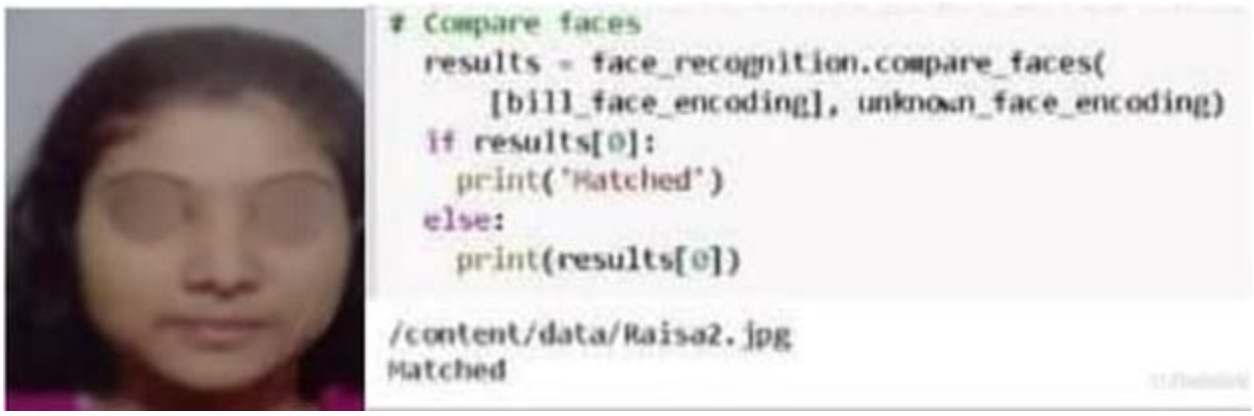

Fig. 3.5: Matched with NID server

The NID server's data is extremely private and crucial. During the system application process, the purpose is to keep NID data secure. A MAC is produced to send the NID data securely to the local server. It is important to have a common shared key when creating a MAC. Using the Diffie-Hellman key exchange method, a shared key is created.

```
The Value of P is :999999999989
The Value of G is :999999937
The Private Key a for Alice is :999999936
The Private Key b for Bob is :999999935
661161930946
661161930946
```

Fig. 3.6: Key generated using Diffie-Hellman algorithm

The NID server will send this concatenated information to the local server using the key and whirlpool encrypted message.

No	Image	Name	NID	FathersName	MothersName	DateOfBirth	MailID	MacValue
1	[BLOB - 6.2 KiB]	MD. SAJJAD HOSSAIN SAWRAN	5183456902	ABDUL MALEK	SOKINA KHATUN	31-12-1998	sawran@gmail.com	b".L`\x00\x0e*PWy\x0cGFP\x0b\rg;X\x15K\x03[\x03P\x...
2	[BLOB - 13.3 KiB]	MD. MUMINUL BARI	6184456708	MANIK MIA	ASIA KHTUN	13-09-1999	mumin@gmail.com	b'z[z\x10[PlnDX!SDQU\x06\r\x04R\x05\x0eQQ\nX\x14X\...
3	[BLOB - 66.8 KiB]	RAISA TAHSIN TASPIA	5276209108	MD. NURUL AFSAR	GULSHAN ARA KHANOM	22-01-1999	raisa@gmail.com	b'cX\r\x10YfPQAI|aU\x15\x11XU\x03\x01\x05S\x03T_\...
4	[BLOB - 9.5 KiB]	TARANNUM TORI	8184456708	TAWHIDUL ISLAM	AFROZA KHAN	21-03-1998	Tori123@gmail.com	b'bTEWW\\x17\lg\'\x17Y\x0b\x01\x01\x03\r\x01R\x02\...
5	[BLOB - 6.7 KiB]	EMRUL MINHAZ	1844567087	EMDADUL HAQUE	MONI AKTER	19-10-1997	emrul@gmail.com	b'tU\x17\x11Y\x7f\r\n!tU\x1e\x00Y\r\x06\x03\x01\x0...
6	[BLOB - 9.5 KiB]	MAYESHA BINTE MIZAN	5184785670	MD. MOHIUDDIN	MUKTA KHANAM	30-01-1998	mayesha@gmail.com	b',WA]\x10P\x07z\x08\r\x16T/*R\x0b\x04S\x00\x05\x...
7	[BLOB - 25.8 KiB]	SHADMAN SHAKIB	5184356808	SOFIUDDIN CHAWDHURY	MOMENA KHANAM	31-12-1998	Shakib123@gmail.com	b'7]\x00P\r\x03\x0b]\x0ePZ\x0bQVS]R\x05\x06\x07\x0...
8	[BLOB - 5.6 KiB]	FOYSAL AL GABID	5151856708	FORID HOSSAIN	ARUFA AKTER	29-08-1998	foysal@gmail.com	b'#_M\x16\x07[%X\r\x04Q\x08Q\x07\x00\x03\x03\x04\nl...
9	[BLOB - 12.1 KiB]	JULIA AFROSE	5190516708	MD. RAHIM	SONIA AKTER	02-12-1999	juliafrose@gmail.com	b'zGZZP\r\x03K\lDTST\x0e\x05\x0c\x05\x03UQ\x08Z\x10...
10	[BLOB - 13.7 KiB]	JAKIR KHAN	5187036708	KAMAL KHAN	NAZIA BEGUM	29-09-1998	jakirkhan@gmail.com	b'[\x07\r\x0b\x10r[T]\r\x02\x08Q\x05UT\x07SZXR^QA\...
11	[BLOB - 71.1 KiB]	MIR IMTIAZ TAREK	6220768382	RIDWAN HASAN	NAFISA ISLAM	02-04-1997	imtiazmir@gmail.com	b'.\r\x17*\x0e\x15\x0c\x07!gR\x14PRS\x02QUVT\x0eP\...
12	[BLOB - 10.5 KiB]	JUBIN KHAN	4037285826	MOHAMMAD ALAMIN	SHAHIN PARVIN	16-11-1998	jubin16@gmail.com	b'xL\x00Z]yYT*U\x07\x03\x02W\x0e\x01]\x00P_\x13\x0...
13	[BLOB - 12.2 KiB]	MEHEDI RIDOY	7403275517	NAHIYAN HOSSAIN	ANTORA ISLAM	16-06-1998	ridoy06@gmail.com	b'RQVS\x08a\lWd\x0f\r\x07\x04\x0bR\x07\x00\x06\x...
14	[BLOB - 7.3 KiB]	ARSHIA HABIB	7184456708	ASADUZZAMAN KHAN	SAHIDA AKHTER	16-12-1998	arshia@gmail.com	b' E\x17\l\x0b\Xq\x00[*UU\x01\x01R\x02\x06\x01U\x03...
15	[BLOB - 21.5 KiB]	MOHAIMINUL ISLAM	6305284017	RIDWAN SIDDIKI	ROWZA HOSSAIN	05-04-1996	mohaiminul@gmail.com	b'xZrQZ\x08\x0f\r\x11\]D_\x00T\x04V\x02\r\x05Z\x...
16	[BLOB - 14.9 KiB]	MD. SAKIB	2835028173	AZMAIN IKTIDAR	TANZILA ALAM	20-09-1998	sakib20@gmail.com	b',\x05S\x02S\x0b\x03\x05\r\x07VQ\x07\x0eT\x0e\x01...
17	[BLOB - 12.3 KiB]	MEHEDI HASAN MISHU	4036492501	TOWSIF HASAN	FARIHA ANIKA	08-07-1999	mishu08@gmail.com	b'[WX\x04V\x0b\x7fYC\x03_fx0b@XC\x04\x02\r\x02\x0...
18	[BLOB - 132.5 KiB]	MD. NURUL AFSAR	9381503792	MD. ABU SAYED	ZAKIA KHATUN	31-12-1965	afsar@gmail.com	b'}P~AK\x11}yPBSDlrU*\x01QU\x03T\r\x05ST\x15WK"S\\...
19	[BLOB - 118.8 KiB]	GULSHAN ARA	7401395628	A.B.M ISHAQ	ROKSAN ARA	06-10-1974	gulshanara@gmail.com	b'%\x17U\x10[QV#\x14\x07\x01\x0c\x05\x07\x01\x0c\x...
20	[BLOB - 8.6 KiB]	APPEL MAHMUD PRANTO	7401395637	MD. ILIAS MIA	PARUL AKTER	29-12-1999	pranto@gmail.com	b'rF\x12]XzP\x0b\x0bC\x004A\x03\x0cA[\x00P\x01RR\\...
21	[BLOB - 33.1 KiB]	PRANTA BISWAS	9382504792	SHOILENDRA BISWAS	RINA BISWAS	13-01-1999	pranta13@gmail.com	b'1D\x04\x0cMQ\x11$X\x11\x16\x02\x12\x0eQ[PWU\x0...
22	[BLOB - 9.5 KiB]	K.A.Y Nuruddin Jahangir	1969504792	MD. NURUL HASAN	NILA BEGUM	4-06-1990	nuruddin05@gmail.com	b'(sav@Jx16Q\x06ZY[\x07^UZ\x02\x08F\x03\r\x05\x0b...
23	[BLOB - 10.1 KiB]	Mariam Akter	1976504792	MD. MOKBUL HASAN	MIM CHOWDHURY	5-07-1994	konica@gmail.com	b'}X\x10\r\x03\\ld\x06B\x04\x0bT\x02\x05\x05\x06...
24	[BLOB - 229.7 KiB]	Md. Asaduzzaman	1962504792	ABDUL KALAM	AMENA BEGUM	2-02-1993	asaduzzaman@gmail.com	b"uTBS\lMx18lR^\x00X\x03\x0bR\r\x0b\x04\x06\x0cT[S...
25	[BLOB - 312.2 KiB]	Sabeeha Khatun	1970506892	RAHIM KHAN	SALMA AKTER	8-12-1998	sabeeha@gmail.com	b'}\x07TPQ_W]^U\x17\x10\x0f\x04X\x02\x00\rQ\x06YXQ...
26	[BLOB - 274.0 KiB]	Sakib Zaman	6970506892	KARIM HASAN	JANNATUL FERDOUS	6-05-1988	sakib01@gmail.com	b'cW\lPU;Q_XZW]\x00\x00\x01R\x03\x0f\x0cV\x12\x05_...
27	[BLOB - 178.5 KiB]	Sadia Afreen	5090306855	MD NUR UDDHIN	MASHIYAT TASNIM	12-12-1995	sadia13@gmail.com	b'a\x03Q]SvP\x11\x01\x06\x0f\rV\l\rnSUZTP\x16\x05\x...
28	[BLOB - 105.8 KiB]	Shaznin Sultana	6490576885	RAHMAN CHOWDHURY	DALIA NOUSHIN	23-04-1990	shaznin22@gmail.com	b'0\rRL^\l^dB^\x12\x04\r\x00W\x04XT\x03TU^tT\x17^...
29	[BLOB - 199.5 KiB]	Ishrar Mannan	6546776085	ABDUL MANNAN	SINTHIA KABIR	16-10-1994	ishrar@gmail.com	b'zAQOWA]W\r\x08\x03][\x04\r\x00\x03\x05\x06W\x06]P...
30	[BLOB - 3.6 KiB]	Md. Sujaur Rahman	6454310268	LUTFUR RAHMAN	AYESHA AYNAZ	25-01-1996	suja@gmail.com	b'[\x02fD^SBGdPZKWX\x06\x0cV\x01U\x08\x03SUZ\x15AX...
31	[BLOB - 194.0 KiB]	MD. Abdul Goni	1962310568	ROHAN KHAN	NAMIRA RAHMAN	27-06-1987	goni@gmail.com	b'y\'#\x00!L\x0e*WY'Q\x03X\x00W\x05P\x01S\x0e\x00^...
32	[BLOB - 260.0 KiB]	Zannatul Ferdous Tunny	6456231446	NAZMUL ISLAM	TANHA ISLAM	20-11-1992	tunny11@gmail.com	b'>Q\x0c\x0f\x05MM\l~PGQ\x0cE\x16`LVXOS\x01\x04\x0...

Fig. 3.7: Demo NID server

```
print("The hashed value is")
print(hashed_output)

The hashed value is
19dc821925354fa14632e1df9b5ab14f385d08fc2b450e793519f663fe2bf99c6f75ae31801d06383d36352f162615914de2900080da5eb5d570aaa0deadf984

[9] final_output = sxor(ms,hashed_output).encode('utf-8')
    print(final_output)

    b'cX\r\x10YfPQA\\]aU\x15\x11XU\x03\x01\x05S\x03T_\x08R\r\x13\x03XG\x07s_X\x05YTH\x00]\x0f'

[10] final_output=str(final_output)
     y=str(y)
     concat=ms+final_output+y
     print(concat)

     RaisaTahsinTaspia5276209108raisa@gmail.comb'cX\r\x10YfPQA\\]aU\x15\x11XU\x03\x01\x05S\x03T_\x08R\r\x13\x03XG\x07s_X\x05YTH\x00]\x0f'349949173096
```

Fig. 3.8: Sender will send this concatenate message

After accepting this concatenated message, the receiver will first distinguish between the message and its mac value.

```
RaisaTahsinTaspia5276209108raisa@gmail.com
b'cX\r\x10YfPQA\\]aU\x15\x11XU\x03\x01\x05S\x03T_\x08R\r\x13\x03XG\x07s_X\x05YTH\x00]\x0f'
349949173096
```

Fig. 3.9: Differentiate message & MAC value

Additionally, when a message is received, the receiver generates a MAC value. The message of information is validated if the generated MAC and the received MAC are the same.

```
final_output = sxor(ms,hashed_output).encode('utf-8')
print(final_output)
final_output=str(final_output)
if mac == final_output:
  print("Message is correct!")

b'dWXBWeX[CPZb'
The hashed value is
19dc821925354fa14632e1df9b5ab14f385d08fc2b450e793519f663fe2bf99c6f75ae31801d06383d36352f162615914de2900080da5eb5d570aaa0deadf984
b'cX\r\x10YfPQA\\]aU\x15\x11XU\x03\x01\x05S\x03T_\x08R\r\x13\x03XG\x07s_X\x05YTH\x00]\x0f'
Message is correct!
```

Fig. 3.10: Message is authenticated

Following the transmission of authenticated information from the NID server, a warning message will be sent to the individual's email account. It will initially display a prudence notice. If the person makes the same mistake a second time, a penalty will be sent to that person's registered mail.

e) A Warning Message has been sent

```
import smtplib, ssl
#raisa.tahsin99@gmail.com
#tahsin18511109@gmail.com
port = 465  # For SSL
smtp_server = "smtp.gmail.com"
sender_email = input('enter sender mail address:')  # Enter your address
receiver_email = input('enter receiver mail address:')  # Enter receiver address
password = input("Type your password and press enter: ")
message =input('enter myour message:')

context = ssl.create_default_context()
with smtplib.SMTP_SSL(smtp_server, port, context=context) as server:
    server.login(sender_email, password)
    server.sendmail(sender_email, receiver_email, message)
```

```
... enter receiver mail address:nafizalasad007@gmail.com
```

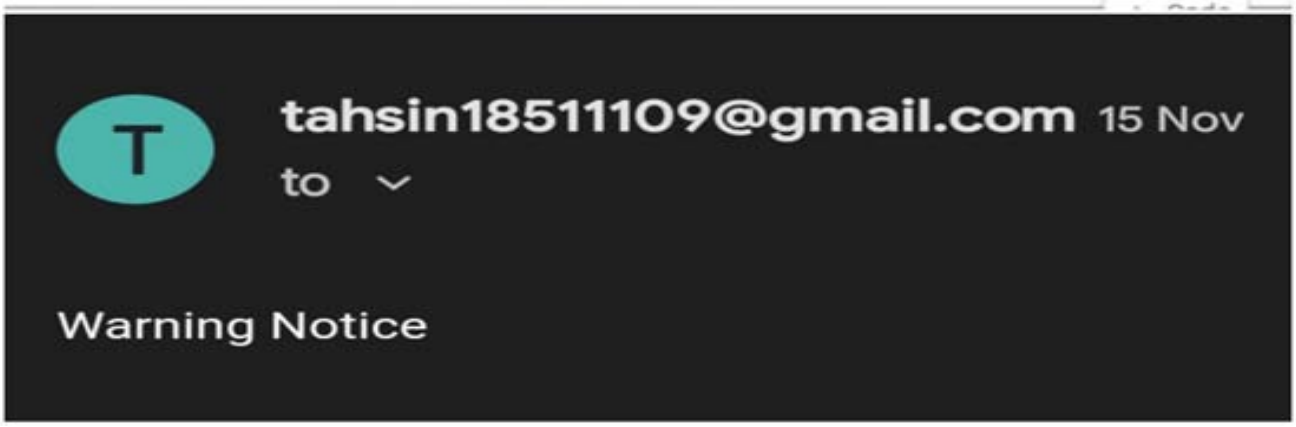

Fig. 3.11: Warning message sent to the specific mail address

VI. Proposed System Security Discussion

Security analysis is the process of examining and evaluating a wide range of factors that can impact the overall security of a system. A system intruder or an unauthorized individual will not be able to access any of the system's components or data until and unless the task is completed. In other words, the system will be wholly protected from any acts that could be particularly disastrous. The tag is the primary provider of protection. The whirlpool algorithm is deployed to construct the tag in this context, with a key length of 512 bits and a tag range of 512 bits [16].

Due to a failed tag verification, any forging of the message, whether malicious or unintended because of transmission errors, will be detected by the destination and reported to the source. The MAC considers each element of the message to be critically important. The root of concern is the shared secret key, which is indeed transferred utilizing secure protocol called Diffe-Hellman. An arbitrary large prime figure with a value of at least 1024 bits is used in the system to offer strong security. The whirlpool algorithm, in addition, has a reliable overall structure operating on messages less than in length that is resistant to the traditional threats directed at block-cipher-based hashes. The collision resistance of this method is. Whirlpool seems to be more robust than most modern hashing algorithms, providing for large-scale component mapping simultaneous execution. Furthermore, it does not necessitate a significant quantity of storage space. As a result, it may be deployed effectively in various applications despite few resources. This could, meanwhile, take advantage of the larger memory space afforded on modern CPUs to gain even greater speed. Because of the hash's increased size, not only would it be more secure towards birthday attacks, yet it allows for a larger inner state for randomness containment, that is required with certain types of pseudo-random number generators [16]. Moreover, the construction adopted from PGV hash functions for generating the MAC is also collision resistant in an extraordinarily powerful way.

VII. Conclusion

The study concludes a secure mechanism against COVID-19 by detecting whether the public is wearing masks [17]. The study adopts MAC to safeguard the personal information of the user against any kind of alteration as it ensures transparency,

security, and immutability. The proposed work is not only a compelling effort to reduce COVID-19 transmission through monitoring an individual's mask use but also an implementation protecting the individual's personal information. This research was inspired by a study conducted in Bangladesh to raise public knowledge about COVID transmission to minimize breakouts while also safeguarding personal information security. Higher authorities can adapt the system to preserve the authenticity of sensitive information, and manage security threats of high priority information such as the NID of citizens used for identification.

a) Future Work

The section on future work presents the findings as well as how to improve and extending current project work, methodologies, or assessments. It is equivocal how well it will operate in hardware because it hasn't been tried in the real world. A proposed paradigm has been recently presented [17] and this is an implementation with the local resources where it performs impeccably. However, it is yet to be assessed with a real-time dataset. Depending on the practical use, the system accuracy rate may vary. With key generation and a message authentication code method, we focused primarily on providing security for file sharing. In the future development of this system, maintenance in other sectors, such as face mask detection and person recognition, might be more precise. There are numerous fields in which progress can be made. In the future, the accuracy of mask detection and accurately detecting the person can be increased. Warnings are sent through email to be going on with but for more efficiency, it could be more practical to send alerting messages through a mobile number SMS system. Dataset diversity can enhance a research project. In real-world cryptography applications, message authentication is crucial. Simulations of the more innovative and valuable concepts could be performed and compared to those evaluated. This project has more potential in the future.

References Références Referencias

1. P. Venkatesan," NICE guideline on long COVID," vol.9, no 2, p.129, 2021.
2. L.S.B.J.P. Janet Green, "Implications of face masks for babies and families during the COVID-19 pandemic: A discussion paper, "Journal of Neonatal Nursing, vol.27, no. 1, pp. 21-25, 2021.
3. M. N. J. H. Saeed Anwar, "COVID-19 and Bangladesh: Challenges and How to Address Them," 30 April 2020.
4. "Message Authentication,"[Online]. Available: https://www.tutorialspoint.com/cryptography/message_authentication.htm. [Accessed 10 april 2021].
5. Y. Alkhurayyif, "National id cards," International Journal of Computing Science and Information Technology, vol. 1 (02), no. ISSN: 2278-9669, pp. 44-48, 2013.
6. C. M. W. Rajat Mittal, "A mathematical framework for estimating risk of airborne transmission of COVID-19 with application to face mask use and social distancing," Physics of Fluids, vol. 32(10), 2020.
7. [Online]. Available: https://docs.opencv.org/. [Accessed 5 june 2021].
8. "Keras API reference," [Online]. Available: https://keras.io/api/. [Accessed 25 july 2021].
9. B. Preneel, "Hash functions and MAC algorithms based on block ciphers," IMA International Conference on Cryptography and Coding, vol. 1355, pp. 270-282, 1997.
10. J. P. Christ of Paar, Understanding cryptography: a textbook for students and practitioners., Germany: Springer Science & Business Media, 2009.
11. P. R. T. S. John Black, "Black-box analysis of the block-cipher-based hash-function constructions from pgv," Annual International Cryptology Conference, Springer, pp. 320-335, 2002.
12. "Socket Programmingin Python, "Geeks for Geeks,[Online]. Available: https://www.geeksforgeeks.org/socket-programming-python/. [Accessed 25 june 2021].
13. "How to Transfer Files in the Network using Sockets in Python," [Online]. Available: https://www.thepythoncode.com/article/send-receive-files-using-sockets-python. [Accessed 31 july 2021].
14. "SDLC Waterfall Model, "[Online]. Available: https://www.tutorialspoint.com/tutorial_view.htm?cid=sdlc&pid=sdlc_waterfall_model.htm. [Accessed 20 august 2021].
15. W. Stallings, Cryptography and network security, India: Pearson Education, 2006.
16. V. R.,. S. T. S. A.,. C. N. by Paulo S. L. M. Barreto, "The Whirlpool Hashing Function," In First open NESSIE, 2000.
17. Sultana, S., Taspia, R., Hossain, M., Nahiduzzaman, M., 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. doi: 10.4236/etsn.2022.111003.