Viewpoint

Fingerprint Biometric System Hygiene and the Risk of COVID-19 Transmission

Kenneth Okereafor, HND, PGD, BSc, MSc, PhD, PhD; Iniobong Ekong, MPH, MBBS; Ini Okon Markson, MBBS; Kingsley Enwere, BSc

1 Department of Information & Communications Technology, National Health Insurance Scheme, Abuja, Nigeria
2 Department of Health Planning, Research & Statistics, Federal Capital Territory Health & Human Services Secretariat, Abuja, Nigeria
3 Evangelical Church Winning All (ECWA) Comprehensive Medical Centre, Karu, Abuja, Nigeria

* all authors contributed equally

Corresponding Author:
Kenneth Okereafor, HND, PGD, BSc, MSc, PhD
Department of Information & Communications Technology
National Health Insurance Scheme
NHIS Data Centre
Abuja
Nigeria
Phone: 234 8023148494
Email: nitelken@yahoo.com

Abstract

Biometric systems use scanners to verify the identity of human beings by measuring the patterns of their behavioral or physiological characteristics. Some biometric systems are contactless and do not require direct touch to perform these measurements; others, such as fingerprint verification systems, require the user to make direct physical contact with the scanner for a specified duration for the biometric pattern of the user to be properly read and measured. This may increase the possibility of contamination with harmful microbial pathogens or of cross-contamination of food and water by subsequent users. Physical contact also increases the likelihood of inoculation of harmful microbial pathogens into the respiratory tract, thereby triggering infectious diseases. In this viewpoint, we establish the likelihood of infectious disease transmission through touch-based fingerprint biometric devices and discuss control measures to curb the spread of infectious diseases, including COVID-19.


KEYWORDS
biometric; contact; contaminate; coronavirus; COVID-19; cybersecurity; disease; fingerprint; hygienic; infectious; pathogen; scanner; surface; verification

Introduction

The primary purpose of fingerprint recognition or identification systems is to provide trustworthy verification of users to control access to resources such as computers as well as to critical facilities such as offices and hospitals. These systems also provide useful data for generating summary periodic reports on usage statistics [1], including the number of participants inside a facility, frequency of entrances and exits, duration of stay, and other intelligence required for monitoring, surveillance, and security administration.

Despite their many benefits, fingerprint scanners are potential sources of disease transmission due to contamination from multiple touches by various users in a wide range of questionable hygienic conditions; as a result, these scanners pose potential transmission risks. Serial use of finger scanners in a given setting may play a more significant role in transmission, as latent prints left on the scanner surface by the deposition of finger moisture, sweat, or oils can soil the surface [2].

Unhygienic thumbs can potentially leave surviving bacteria [3], fungi, and viruses on the surface [4] of the scanner after use, thereby increasing the possibility of transmitting germs that cause illnesses [5], including COVID-19, which is predominantly spread via droplets and contaminated hands or surfaces [6].
Applications of Fingerprint Biometric Systems

Like other biometric devices, fingerprint systems provide a secure and facile means of verifying the identities of humans [7] using their unique finger attributes. These systems are used in a number of applications for various cybersecurity and access control purposes, as follows.

Employee Time and Attendance Systems

Traditional workplaces [8] use fingerprint biometric systems to identify personnel, grant authorized access to offices, and maintain accurate records of staff attendance [1,7,9].

Secure Login Access to Software and Electronic Systems

Fingerprints are used to control login access [10] to computers and mobile phones as well as to banking, accounting, and other software applications [11].

Vehicle Door and Access Control Systems

Increasing numbers of electronic automobile systems are incorporating biometric doors based on fingerprint technologies, enabling drivers to restrict, control, and track usage of their vehicles.

Access Control to Physical Facilities

Fingerprint biometrics are used to regulate access to and within secure environments [12], including airports, hospitals, stadiums, educational institutions [13], and shopping malls.

Verification for Civic Services

Biometric systems are used to control access to citizens’ benefits, including population demographics and patient verification, to prevent impersonation of health care beneficiaries by scammers [14].

Automatic Teller Machine Login Security

Many automatic teller machines (ATMs) and point-of-sale vendor systems contain embedded fingerprint biometric login functionalities to improve the security of web-based financial and banking transactions.

Immigration and Embassy Verification Systems

A biometric ePassport [15] contains the passport holder’s fingerprint records in line with the United Nations International Civil Aviation Organization (ICAO) 9303 [16] standard for machine-readable travel documents (MRTDs). Embassies and High Commissions also use automated fingerprint systems to capture, store, and exchange profiles for visa verification at border areas.

Crime Investigation

Law enforcement agencies use automated fingerprint identification systems (AFISs) to manage fingerprint databases for crime investigation.

Figure 1 shows illustrations of the various applications of fingerprint biometric systems in commerce, industry, business, and government.

Overview of Fingerprint Scanners as a Potential Source of Harmful Microbial Transmission

Background and Concerns

Due to their simplicity, ease of use, and cost-effectiveness, the commercial applications of fingerprint systems for identity verification have become widespread. Although the popularity
of these systems suggests a high level of industrial endorsement and user acceptance, their frequent use under various environmental conditions also raises serious concerns regarding their hygienic safety [17] and risks of disease exposure.

A biometric scanner is the component of the biometric system that retrieves the electrical equivalent of the biometric sample for unique measurement. Physical contact is part of the normal operational routine of most biometric scanners. In the case of a fingerprint system, the user is required to touch the surface of the scanner to provide the biometric sample; the thumb must be directly placed in a certain manner for a specified duration to obtain a reliable measurement.

In the process of detecting and acquiring an electrical interpretation of the finger pattern, the structure of the fingertip (composed of ridges, valleys, and furrows) is scanned [18,19]. Directly touching the scanner surface with the thumb can potentially lead to exchange of particles; this can increase the chances of either acquiring or depositing harmful microorganisms, including pathogens that can spread bacterial, fungal, and viral infectious diseases, possibly including the novel COVID-19.

These germs may accumulate as deposits after each successive use, resulting in contamination of the surface of the fingerprint scanner [4]. According to Kramer and Assadian [20], contaminated surfaces can serve as important vectors for cross-transmission after hand contact, and in the case of frequent use, contamination can occur even more rapidly. This is particularly common in medical environments, where contaminated surfaces also play an important role in the transmission of hospital-acquired infections, also known as nosocomial infections [4].

Given their ability to retain microorganisms and germs, contaminated fingerprint scanner surfaces can become secondary reservoirs of infection that can in turn cross-contaminate food or water through hands or objects that come in contact with them [21].

Possible Disease Spread via Pathogenic Deposits on Fingerprint Scanner Surfaces

Microorganisms, including pathogens [22], can potentially be transmitted from animate sources to inanimate environmental sources through disease-carrying objects (fomites) or materials. As a result, pathogens can propagate among humans from touching communal surfaces in public places [3], including fingerprint scanner surfaces, where they can trigger the spread of infectious diseases. Contracting infectious diseases through fingerprint scanners is classified as an indirect means of transmission.

Depending on the infectious microorganism in question, and provided that the media or aerosol droplets remain alive on the surface, some pathogens can survive for only few seconds or minutes before dying. However, other pathogens can live on surfaces in wait for a potential new host for hours, days, weeks, or even months [23]; therefore, they remain a continuous source of transmission depending on frequency of use and whether regular preventive surface disinfection is performed. For example, studies [6,24] indicate that the novel coronavirus that causes COVID-19, SARS-CoV-2, can remain viable and infectious in aerosols for hours and on surfaces for up to days depending on the environmental temperature, humidity, and inoculum. Particularly, lower environmental temperatures increase the persistence of the COVID-19 pathogen and further prolong its survivability on external surfaces [6].

For these reasons, long-lasting pathogens found in body fluids and carried by fingertips are sources of concern in the administration of fingerprint scanners. Table 1 shows a partial listing of body fluids and secretions that can be deposited on or acquired from fingerprint scanners, alongside some of their commonly associated pathogenic isolates.
The various pathogenic isolates from common body fluids and secretions listed in Table 1 can potentially be retained on contaminated biometric fingerprint surfaces needs to be specifically determined. The following are some commonly associated microbial isolates capable of causing disease.

**Table 1.** List of body fluids and secretions and some commonly associated microbial isolates capable of causing disease.

<table>
<thead>
<tr>
<th>Body fluid/secretion</th>
<th>Implicated pathogenic isolates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweat</td>
<td><em>Staphylococcus</em> species [25,26], <em>Ebola virus</em> [27], HBV&lt;sup&gt;a&lt;/sup&gt; [28]</td>
</tr>
<tr>
<td>Tears</td>
<td>Unconfirmed pathogenic association with tears, although chronic HBV has been found in the tears of children [29]</td>
</tr>
<tr>
<td>Saliva</td>
<td>SARS-CoV-2 [30,31], filoviruses [32,33], HBV [34], HSV&lt;sup&gt;b&lt;/sup&gt; [35], <em>Escherichia coli</em> [36]</td>
</tr>
<tr>
<td>Nasal mucus fluid</td>
<td>SARS-CoV-2 [37], filoviruses [33], <em>Streptococcus</em> [38], <em>Haemophilus influenzae</em> [39,40], parainfluenza [41,42], <em>Mirabilia catarrahi</em> [43], Actinomyces [44,45], <em>Mycoplasma pneumoniae</em> [46]</td>
</tr>
<tr>
<td>Pus</td>
<td><em>Staphylococcus</em> [26], <em>Klebsiella</em> species [47-49], <em>Pseudomonas</em> species [50], <em>E coli</em> [36], <em>Proteus</em> species [51]</td>
</tr>
<tr>
<td>Hemoglobin/blood</td>
<td>SARS-CoV-2 [52], filoviruses [33], HBV [26,28]</td>
</tr>
<tr>
<td>Semen</td>
<td><em>E coli</em> [53], hepatitis C [54,55], HSV [56], SARS-CoV-2 [57,58], Zika virus [59-61], <em>Ureaplasma urealyticum</em> [62,63], <em>Enterococcus faecalis</em> [64], alpha-hemolytic streptococci [46], Lassa virus [65], Marburg virus [66], <em>E bola virus</em> [66], Chikungunya virus [56]</td>
</tr>
<tr>
<td>Vaginal swab</td>
<td><em>Candida albicans</em> [67,68], <em>Trichomonas vaginalis</em> [69], <em>Neisseria gonorrhoeae</em> [70,71], yeast cells [72], Group B streptococci [38,46,73], E coli [74], <em>Klebsiella</em> [48], HSV [56], warts [46]</td>
</tr>
<tr>
<td>Urine</td>
<td>Yeast cells [72], adenovirus [75], BK virus [76,77], <em>Schistosoma</em> [78], E coli [79-81], <em>Klebsiella</em> [48], Zika virus [61], Cossackievirus [82], <em>Proteus</em> [43], <em>Staphylococcus saprophyticus</em> [26], <em>Candida albicans</em> [67]</td>
</tr>
<tr>
<td>Feces</td>
<td><em>Salmonella</em> [83], paratyphoid [41], <em>Entamoeba histolytica</em> [84]</td>
</tr>
<tr>
<td>Sputum</td>
<td>SARS-CoV-2 [85,86], <em>Haemophilus influenzae</em> [39], parainfluenza [41], <em>E coli</em> [87], <em>Streptococcus pneumoniae</em> [38], Actinomyces [46]</td>
</tr>
<tr>
<td>Nasal swabs</td>
<td>SARS-CoV-2 [30,31], Zika virus [61], <em>Haemophilus influenzae</em> [39], parainfluenza [41]</td>
</tr>
<tr>
<td>Urinary tract swabs</td>
<td><em>Chlamydia trachomatiss</em> [88,89], <em>Mycoplasma</em> [90,91], HSV [92,93], <em>Streptococcus saprophyticus</em> [38], <em>Neisseria gonorrhoeae</em> [46,94], <em>Pseudomonas aeruginosa</em> [95]</td>
</tr>
<tr>
<td>Ear wax</td>
<td>Usually sterile, but yeast cells may be present [96]</td>
</tr>
<tr>
<td>Eye secretion</td>
<td><em>Neisseria gonorrhoeae</em> [97], <em>Chlamydia trachomatiss</em> [94], HSV [98], <em>Pseudomonas aeruginosa</em> [99,100], <em>Staphylococcus aureus</em> [101,102]</td>
</tr>
<tr>
<td>Vomit</td>
<td>Norovirus in viral gastroenteritis [103,104]</td>
</tr>
<tr>
<td>Secretion from wounds and sores</td>
<td><em>Pseudomonas aeruginosa</em> [105], <em>Enterobacteriaceae</em> [105], HBV [28], HSV [26,51]</td>
</tr>
</tbody>
</table>

<sup>a</sup>HBV: hepatitis B virus.

<sup>b</sup>HSV: herpes simplex virus.

The various pathogenic isolates from common body fluids and secretions listed in Table 1 can potentially be retained on surfaces that are frequently touched; this raises major hygienic concerns, including possible transmission of respiratory viruses [106]. However, the transmissibility of these pathogens through contaminated biometric fingerprint surfaces needs to be specifically determined.

**Sources of Fingerprint Scanner Surface Contamination**

Essentially, persons who are nasal carriers of *Staphylococcus aureus*, whose hands are soiled with *S aureus*, or who exudate *S aureus* from skin lesions such as pimples, boils, infected cuts, and burns may contaminate fingerprint biometric surfaces through contact. An exposed injury that leaks pus-like or clear fluid composed of serum, fibrin, and white blood cells can also contaminate surfaces through contact. Contamination has also been shown to occur from persons in incubatory stages of hepatitis A infection, persons infected with norovirus or who have come in contact with excreta of persons with salmonellosis or cholera, and persons who are intestinal carriers of *Shigella* species [4,107-109].

Other sources of contamination include persons whose hands are soiled with raw poultry, pork, beef, and other meats contaminated with *Salmonella*, *Campylobacter jejuni*, *Yersinia enterocolitica*, *Clostridium perfringens*, *S aureus*, *Escherichia coli*, etc.

It should be noted, however, that the pathogenicity of any disease-causing microbe will depend not only on its transmissibility from a host (human user of the fingerprint device) to the reservoir (fingerprint device) and to a fresh host (another user of the device) but also on its survivability [107] in the new host, its ability to breach the host’s immune system (infectivity), and its capacity to harm the host (virulence) [56].

**Factors That Influence Infectious Disease Transmission via Direct Contact With Fingerprint Scanner Surfaces**

**Frequency of Use and Location of the Device**

By virtue of their function, fingerprint scanners constitute frequently touched surfaces and are used by a large number of people on a continuous basis. The greater the number of people
who use a scanner, the higher the risk of contamination. The location of the devices also significantly affects the likelihood of contamination and disease transmission; for example, surfaces in hospital settings and microbiology or biomedical laboratories are more likely to be contaminated because of their proximity to patients and their body secretions [19] or samples [20], with a high probability of nosocomial infections.

Personal Hygiene of Users
Kramer and Assadian [20] showed that a single hand contact with a contaminated surface can result in different levels of potential microbe transfer from the surface to the hand. The risks of this cross-contamination of hands were shown to be higher with *E coli*, *Salmonella* species, *S aureus* (all 100%), *C albicans* (90%), rhinovirus (61%), hepatitis A virus (22% to 33%), and rotavirus (16%).

In addition to transmission through food or water, certain microbes spread through direct inoculation into the respiratory tract from contaminated hands. For example, influenza A [110] viruses, in addition to transmission through aerosol, are believed to spread between humans through contact and large respiratory droplets; these droplets can settle on the ground or other environmental surfaces within 1 to 2 meters [111], including nearby fingerprint biometric surfaces.

Pathogenic Potential of the Microorganism and Level of Infective Inoculum
The ability to contract disease from cross-contamination of food or water from the use of a contaminated biometric fingerprint scanner will depend on several factors, including the pathogenic potential or virulence of the microorganism [108]. This potential varies between microorganisms and is directly proportional to the size of the infective inoculum irrespective of whether this inoculum is a preformed toxin, such as in botulism and staphylococcal food poisoning, or requires direct microbial inoculation, such as *Salmonella* serovar Typhi or hepatitis A. Similarly, the immunity of the individual host plays an important role in the eventual development of the disease.

Extent of Microbial Survival on Environmental Surfaces
Several complex factors influence the survivability of microorganisms on environmental surfaces [20]; the longer the organisms persist on a surface, the longer the contaminated surface can remain a reservoir and a source of transmission to individuals who come in contact with the surfaces.

While the literature is limited on this topic, available studies have shown varying results. However, many bacteria, fungi, and viruses can persist for durations of hours to days and months on environmental surfaces depending on certain environmental conditions, including but not limited to temperature, humidity, and biofilm formation.

Notably, fungi can persist for a few days; other spore-forming organisms can persist for longer periods due to the thermotolerant properties of the spores [20]. It is currently uncertain how long SARS-CoV-2 survives on surfaces; however, preliminary studies [6,23,24,112,113] suggest that this novel coronavirus may survive on surfaces for periods ranging from a few hours to several days, weeks, or longer.

Relative Humidity, Temperature, and Biofilm Formation
Although the amount of moisture on users’ fingers has an impact on overall biometric performance [114], the effects of humidity on the survival of microorganisms on environmental surfaces such as fingerprint scanners vary greatly between different classes of microorganisms and are significantly influenced by the presence of a cell wall or protective membrane.

While viruses with lipid envelopes, such as influenza virus or coronaviruses, tend to survive longer in low relative humidity (20% to 30%), some viruses survive longer in moist surfaces with higher relative humidity (70% to 90%). This is also true for different types of bacteria, such as gram-positive bacteria (eg, *Staphylococcus* species), which survive better at low humidity than gram-negative bacteria such as *E coli*. However, in some cases, the results inexplicably conflict, including the variability in fingerprint performance [115] with temperature and humidity [116].

Higher temperatures affect the integrity of viral proteins and enzymes as well as viral genomes (DNA or RNA) and will reduce the survival of viruses on surfaces.

Biofilms are a collection of two or more types of microorganisms (bacteria, fungi, and protists) that can grow on many different external surfaces, including on glass or plastic fingerprint scanner materials. A biofilm is an enclosure of microbial cells in environmental surfaces composed of an extracellular polymeric substance that protects the microorganisms from environmental influences [109] and can potentially prolong their survival, enabling them to live longer as contaminants on fingerprint scanner surfaces.

Intrinsic Properties of Surfaces
The physiochemical properties of surfaces define the rate and extent of attachment and the retention of microorganisms to form biofilms. Flagellate motile organisms attach to surfaces more readily than nonmotile organisms. According to Donlan [109], microbes attach more frequently to hydrophobic, nonpolar surfaces such as plastics than to hydrophilic materials such as glass and metals. In another study [117], surfaces lacking pores, such as plastics, were found to allow microorganisms to remain on the surface, thereby facilitating cross-contamination. Microorganisms entrapped in pores are more subject to lysis, particularly in the absence of water and nutrients.

Meanwhile, the upper surface of a fingerprint scanner is composed of a very small piece of plain glass or transparent plastic material that is used to capture the electrical equivalent of the finger pattern. The act of touching leaves an impression of the person’s finger on the scanner surface, which the system interprets as an electrical representation of the user’s unique finger pattern. It is a theoretical possibility that in the touch-dependent capture process, the scanner surface can also retain surviving microorganisms or germs (eg, bacteria, viruses, fungi, and protozoa) that can potentially contaminate the surface.
with disease-causing pathogens that are transmissible from person to person through direct contact and serial use.

Other Influential Factors

Other subtle factors that favor transfer of microorganisms across fingerprint biometric system users are the large skin-surface contact of flat fingers, type of fingerprint-capturing device, nonporous contact surface, large overlap of users’ contact areas on the surface, short turnaround time between successive users, and high contact pressure on the surface [106].

Recommendations

Universal Hygiene Measures

Universal hygiene measures are highly necessary to control disease transmission through fingerprint devices. These measures should be adopted by the facilities in which these scanners are used, particularly those in high-touch areas and in areas with close proximity to infectious patients, such as hospital settings and microbiology and biomedical laboratories. The adopted hygienic measures should ensure that the fingerprint systems are safely decontaminated for use in all circumstances on a continuous basis without compromising their integrity and biometric functionality.

For instance, while the use of gloves would be ideal for preventing contamination of a fingerprint device surface or cross-contamination of food and water [19], the glove obliterates the physiological patterns of the natural fingertips, rendering them unreadable and thus completely defeating the operational purpose of unique biometric identification. The use of gloves is therefore not a suitable means of controlling disease transmission by fingerprint systems.

Furthermore, some fingerprint biometric systems are capable of liveness detection [115,118-120], which is the ability to verify that the finger presented to the scanner is a natural, live human finger possessing all the attributes of vitality, including the presence of normal human temperature, normal pulse beat rate, and natural blood flow. With these systems, the use of gloves could operationally return a “fake finger detected” result due to the inanimate nature of the glove.

In keeping with global cybersecurity standards, measurement of liveness (ie, liveness detection) is a means to verify that the finger presented by a user is not a dummy [115], fake, cloned from a molded artefact, or cut from a corpse/cadaver. In a biometric spoofing attack [119,121], an impostor masquerades as an authentic user by replicating a legitimate user’s biometrics (eg, with a counterfeit finger); therefore, the system could likely interpret the wearing of gloves as a typical biometric spoofing attack.

Table 2 indicates liveness parameters that can be measured on a fingerprint biometric system and demonstrates why the use of gloves to prevent infectious diseases can have a negative impact on the cybersecurity performance and overall accuracy of the fingerprint system and is thus discouraged.

Table 2. Effects of glove use for minimizing fingerprint contamination on the pattern obtained by a fingerprint biometric system.

<table>
<thead>
<tr>
<th>Measurable liveness parameter</th>
<th>Biometric pattern</th>
<th>With hand in glove</th>
</tr>
</thead>
<tbody>
<tr>
<td>Texture</td>
<td>Natural human body tissue</td>
<td>Latex or rubber</td>
</tr>
<tr>
<td>Temperature</td>
<td>37±0.5 °C (human range)</td>
<td>Inconsistent</td>
</tr>
<tr>
<td>Pulse</td>
<td>60 to 100 beats per minute (human rate)</td>
<td>None</td>
</tr>
<tr>
<td>Pattern</td>
<td>Human finger ridges, valleys, and furrows [19,115]</td>
<td>Smooth</td>
</tr>
<tr>
<td>Blood flow</td>
<td>Evidence of natural human blood flow</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 2 shows that on the basis of biometric functionality, a finger in a glove could be misinterpreted as a fake or spoofed finger; therefore, wearing gloves is completely unsuitable because it prevents the system from accurately detecting the biometric parameters of the real finger required for unique human identity verification and identification.

Clean the Scanner Surface Regularly

The surface of a fingerprint biometric device should be regularly decontaminated with disinfectants. The scanner surface should be cleaned after each use, either by designating a human assistant to manually disinfect it on a regular basis using a recommended cleaning agent with a damp nonabrasive cloth or a paper towel or by compelling each user to clean the scanner after use with a damp wipe soaked with an approved cleaning agent such as those contained in the US Environmental Protection Agency (EPA) [122] list of products for use against emerging viral pathogens.

In environments of heavy use, an automated spray and wipe mechanism can be set up to automatically scrub and disinfect the scanner surface between successive uses. Any combination of these measures will leave a safe fingerprint surface for subsequent users. Automating the postuse sanitization of fingerprint scanner surface may require additional investment, which will increase the total cost of biometric deployment and maintenance.

Use Alcohol-Based Cleaning Fluid

Alcohol-based cleaning agents should be used to enable rapid drying of the scanner surface through evaporation, as a wet scanner surface will introduce numerous errors. These errors include false negatives, where legitimate persons are wrongly denied access, and false positives, where unauthorized users are granted access. Both false negatives and false positives have cybersecurity implications in the management of fingerprint biometric systems in addition to user apathy, and they should be avoided. Furthermore, wet surfaces can encourage the growth
of pathogens and increase their survival on the device; thus, they should be avoided.

The recommendation of alcohol-based sanitizers is occasioned by the wide range of germ-killing efficacy of these sanitizers as well as their rapid evaporation without leaving wet surfaces, which can impact the biometric performance of the scanners and lead to operational failures.

**Use Noncorrosive Cleaning Fluid**

When choosing a suitable cleaning fluid for scanners, harsh products containing high levels of acidic constituents should be avoided. These products can corrode the scanner surface and alter its sensitivity, negatively impacting the biometric performance of the system with inaccurate readings including high probabilities of false positives (false acceptance) and false negatives (false rejection) [14,123].

The use of a highly corrosive cleansing agent (liquid, gel, or powder) is discouraged as a cleanser for the fingerprint scanner surface because the corrosive nature of the agent could damage the surface structure of the scanner, resulting in a decrease of its ability to function as a biometric device for validating users.

### Table 3. List of recommended cleaners for scanner surfaces.

<table>
<thead>
<tr>
<th>Surface type [124]</th>
<th>Composition</th>
<th>Recommended cleaners [122]</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonporous</td>
<td>Glass, marble, metal, and plastic</td>
<td>Fiberlock IAQ 2500, CA-MRSA disinfectant spray, Clorox commercial solution hydrogen peroxide cleaner disinfectant</td>
<td>Contains noncorrosive chlorine, which does not alter the biometric functionality of the fingerprint scanner surface.</td>
</tr>
<tr>
<td>Porous</td>
<td>Fabric, unfinished wood, and paper</td>
<td>Clorox broad spectrum quaternary disinfectant cleaner, germicidal cleaner and disinfectant, detergent disinfectant pump spray</td>
<td>Antibacterial quaternary ammonium compounds with no harsh phenolics. Suitable for absorbent surfaces.</td>
</tr>
<tr>
<td>Textured</td>
<td>Rough, hard coating</td>
<td>Solucide hard surface disinfectant spray, Opti-Cide3 surface wipes, peroxide multisurface cleaner and disinfectant</td>
<td>The hydrogen peroxide constituent is very effective against fungi, viruses, bacteria, and other germs on rough and cracked surfaces.</td>
</tr>
</tbody>
</table>

**Adjust the Scanner Sensitivity**

The sensitivity of a biometric scanner determines how easily it can extract a fingerprint image or template from a user. A highly sensitive scanner has a tendency to reject user attempts, while a less sensitive scanner can be too porous; hence, a balance is necessary. The sensitivity of the fingerprint scanner should be adjusted to a level that minimizes the duration of contact required to read the finger sample and reduces the likelihood of germ transmission.

**Deploy Multifactor Authentication**

A multifactor authentication system includes an additional means of verification, such as a password or token. This system is beneficial to prevent overreliance on single-factor fingerprint authentication, which can be relaxed in emergency health situations such as the COVID-19 pandemic when the risk of propagating infectious diseases is high. By adding a second or third factor of authentication, an alternative system can be proactively prepared to switch modes in accordance with the demands of the moment.

**Enforce Finger Hygiene and Hand Sanitization Culture Through Education**

It is essential to educate users on handwashing, cleaning of fingernails, and strict hygienic behaviors as well as the dangers of using a fingerprint scanning device with exposed skin and after contact with mouth, nose, or eye infections and uncovered wounds. This can prevent contamination of the scanner and avert cross-contamination of food or water [18,21,22,117].

Users should be compelled through frequent sensitization to use an antimicrobial substance that is effective in killing microorganisms or stopping their growth, such as alcohol-based hand sanitizers applied on the palm and thumbs before and after each use of the fingerprint device.

The EPA has provided a recommended list of approved tier 1 products [122] for cleaning touch devices and open surfaces. The products are in compliance with the EPA’s Emerging Viral Pathogen Guidance for Antimicrobial Pesticides. Table 3 shows a partial listing of EPA-recommended cleaners for emerging enveloped viral pathogens, including SARS-CoV-2, which can be used for each type of finger scanner surface.

**Use an Alternative Means of Authentication**

In the absence of multifactor authentication, other standalone but temporary means of authentication can be used, including password verification, personal identification numbers, and tokens.

**Temporarily Disable Biometric Sign-In**

For environments that rely on fingerprint biometrics as the only user access verification technique, temporary suspension and deactivation is highly recommended to enable the establishment of the preventive surface disinfection actions discussed above, particularly those that relate to the hygiene of the scanner surface. Biometric use can resume after these countermeasures have been established.

**Use Contactless Biometric Technologies**

Although many biometric systems require physical contact with the scanner to obtain the user’s biometric image, research on completely contactless fingerprint scanners is ongoing at different stages among technology vendors. Contactless identification of fingerprints has gained considerable attention [125] for a number of reasons, including limiting the transmission and spread of touch-dependent infectious diseases.
While the prospects are high for fingerprint systems that can acquire biometric samples without compelling the user to touch the scanner surface, studies [17,126,127] have shown that the achievement of a highly accurate contactless fingerprint recognition system is challenged by possible delays and recognition errors. Research in this area is advancing, and some prototypes may soon be commercially available; therefore, contactless fingerprint biometric systems will hopefully address hygiene concerns by eliminating contamination from frequent direct touching.

Shifting to contactless biometric systems such as iris recognition appears to be an alternative approach. Despite cost considerations, iris recognition is a faster and more accurate biometric modality than fingerprint recognition. Iris cameras are technologically advanced and are suitable for use in health care, laboratory and medical research facilities, and other environments where poor hygiene exposes users to significant health risks. Iris recognition alternatives are also used in airports and military bases, where fast and reliable human identification is both an operational requirement and a security imperative. Other contactless options include vascular biometrics (finger vein and palm vein), voice biometrics, and gait recognition.

Limitations and Further Research

Potential Setbacks of Incorporating Automatic Sanitization in Fingerprint Systems

Incorporating the autosanitizer framework proposed in this work into pre-existing fingerprint biometric systems may be difficult to achieve. Future research and development efforts could include investigating ways to integrate automatic sanitization directly into the design of new fingerprint recognition systems in a vendor-neutral manner to ensure interoperability without impacting performance and convenience.

Extensive Study on Transmissibility of Isolated Pathogens

The list of microbial isolates that can be found in common body fluids and secretions as considered in this work appears to be nonexhaustive because of the limited literature and research associating the identified pathogens with known infectious diseases that can be transmitted via fingerprint scanners.

This creates a window of opportunity for focused research to investigate pathogenic linkages with infectious disease, including COVID-19. Research in this area is currently scarce but is certainly expedient and in high demand.

It is likely that a study in which each pathogenic isolate is matched to a corresponding infectious disease condition will become increasingly complex, with conflicting overlaps. This could lead to a shift of focus from fingerprint scanner surface contamination to disease mapping; this could be addressed by applying a phased research methodology in which each pathogen or group of microbial isolates is studied in isolation to facilitate research data interpretation.

Elucidation of Microbial Infectivity and Virulence in Relation to the Size of the Inoculum

While other complex factors are involved in the pathogenicity of diseases in users of biometric fingerprint scanner devices, further studies are needed to isolate specific pathogens on these devices, profile the common pathogens, identify their sources, and demonstrate the extent to which they cause disease in other users of the devices.

Infectious Disease Transmission via Other Touch-Based Devices

This study primarily focused on hygiene concerns related to fingerprint devices. It has therefore suggested further research opportunities to investigate the likelihood of transmission of the novel COVID-19 pathogen via other electronic surfaces and touch-based devices, including but not limited to ATM keypads, touch screen computer monitors, computer keyboards, touch screen phone buttons, elevator control keypads, machinery buttons, as well as shared surfaces including shopping carts, stairway rails, door handles, currency notes, table tops, fabrics, papers, cardboard, and plastics.

Conclusion

Principal Findings

Physical contact has been proven to be the most common source of surface contamination, depositing harmful microbial pathogens that can be directly inoculated into the respiratory tract of another person or cross-contaminate food and water, triggering infectious disease [111]. These disease-causing pathogens vary from bacteria and fungi to viruses, including SARS-CoV-2, the novel pathogen that causes COVID-19.

Fingerprint scanners are often repeatedly touched by multiple users, thereby raising serious issues of hygiene as their use exposes the risk of contracting and transmitting harmful diseases [19,128] due to direct finger vs scanner contact while extracting the biometric image [10]. These devices are increasingly hazardous, particularly when used in health, medical, or diagnostic facilities where aerosolized droplets and body secretions of sick patients can be easily deposited on them; thus, they may play an important role in the transmission of hospital-acquired infections [4].

While the physiochemical properties of the device material, the environmental conditions, and the survival ability as well as the virulence of the disease pathogen significantly contribute to the risk of disease transmission, several hygienic measures have been shown to be effective in controlling disease transmission from these surfaces. Other approaches and strategies can also be adopted to control and prevent transmission of infectious disease through use of fingerprint systems; however, these approaches must not interfere with the primary biometric performance of the systems. Poor hand washing after defecation and urination as well as contact with infected body fluids, foods, soil, or surfaces can lead to contamination of fingerprint scanner surfaces, which then serve as vectors of disease-carrying pathogens.
Because there are indications of prolonged longevity of the novel SARS-CoV-2 pathogen on certain external surfaces [6,112,113], there is a theoretical risk of transmitting COVID-19 via contaminated or unhygienic fingerprint surfaces because the pathogen may remain alive on the surfaces. In this paper, we proposed ideas for preventing contamination of fingerprint scanners with germs without compromising their primary biometric performance.

As a way of controlling the spread of COVID-19, this paper proposes the adoption of a defense-in-depth approach to managing fingerprint scanner cleanliness to reduce the propensity of these scanners to harbor pathogens that could lead to disease transmission. This approach involves the simultaneous application of recommended measures, all of which aim to make fingerprint systems more hygienic and safer to use while retaining their optimal functions as a biometric verification technique. Beyond the present COVID-19 pandemic, a defense-in-depth approach to managing fingerprint cleanliness will improve overall biometric acceptability and minimize user apathy related hygiene.

Acknowledgments
The logistic support of the management of the NHIS, the Federal Capital Territory Administration (FCTA), and the ECWA Comprehensive Medical Centre, all in Abuja, are appreciated. The authors value the immense input from the NHIS Department of Information and Communications Technology. The conclusions and views expressed in this paper are those of the authors and do not necessarily represent the official positions of the NHIS, the FCTA, or the ECWA Comprehensive Medical Centre. Names of specific vendors, manufacturers, or products, wherever expressly mentioned or implied, are for public health educational and informational purposes only; implicit or expressed inclusion does not suggest endorsement of the vendors, manufacturers, or products by the NHIS, FCTA, or ECWA Comprehensive Medical Centre.

Conflicts of Interest
None declared.

References


83. Okereafor et al. JMIR Biomed Eng 2020 | vol. 5 | iss. 1 | e19623 | p. 12

http://biomedeng.jmir.org/2020/1/e19623/


120. Okereafor KU, Osuagwu OE, Onime C. Biometric Anti-spoofing Technique Using Randomized 3D Multi-Modal Traits. IJSSST 2018;19(5):5.1-5.8. [doi: 10.5013/ijssst.a.19.05.05]


**Abbreviations**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>automatic teller machine</td>
</tr>
<tr>
<td>ECWA</td>
<td>Evangelical Church Winning All</td>
</tr>
<tr>
<td>eHealth</td>
<td>electronic health</td>
</tr>
<tr>
<td>EPA</td>
<td>Environmental Protection Agency</td>
</tr>
<tr>
<td>FCT</td>
<td>Federal Capital Territory</td>
</tr>
<tr>
<td>FCTA</td>
<td>Federal Capital Territory Administration</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>NHIS</td>
<td>National Health Insurance Scheme</td>
</tr>
<tr>
<td>NMC</td>
<td>National Mirror Committee</td>
</tr>
<tr>
<td>TC</td>
<td>Technical Committee</td>
</tr>
</tbody>
</table>