METHOD AND SYSTEM TO DETERMINE RISKS ASSOCIATED WITH SPOOF ATTACKS

FIELD OF THE INVENTION

This invention relates to biometric device and more particularly, to a method and system to determine a risk associated with a spoof attack on the biometric device.

BACKGROUND OF THE INVENTION

A biometric device is a security identification and authentication device which uses automated methods of verifying or recognizing the identity of a person based on a physiological or behavioral characteristic. These characteristics may include but not limited to fingerprints, facial images, iris and voice recognition. The biometric devices are widely used to distinguish between authorized and unauthorized users. In one example, fingerprint sensors are used to determine whether a fingerprint provided by the user matches with a pre-stored fingerprint template in a database, and if a match is determined, then the user may be granted access to enter a building or room, or even the access to an electronic device such as a mobile phone or an application running on a mobile device.

Nowadays, the fingerprint sensors are widely used for the user identification and/or verification. However, the fingerprint sensor is subjected to various threats such as attacks at the sensor level, replay attacks on the data communication stream, and attacks on the database. A variety of fingerprint sensors may be spoofed through a fake biometric object such as a fake finger created resembling to the fingerprint of the authorized individual is made from different materials by using moldable plastic, clay, play-doh, wax or gelatine materials. Thereby, permits the unauthorized user to engage in an activity that is reserved for authorized users. For example, a latex spoof finger may be made to have ridges and valleys resembling the fingerprint of the authorized user. When such latex spoof is presented to the fingerprint sensor, the fingerprint sensor may falsely conclude that the latex spoof is the finger of the authorized user,

even though the latex spoof is not part of a living person. It is important to guard the biometric device from all these types of spoofs. Therefore, there is a need for a system that is able to detect the presence of the spoof or whether the biometric object is part of a live being.

There are several prior arts disclosing system and method on fingerprint liveness detection, some of which are listed below for reference. A prior art, the United State of America granted patent number US9633269B2 discloses a method to detect the liveness, comprises the steps to: obtain a single ultrasonic image of a biometric object; subdividing the single ultrasonic image into a plurality of overlapping sample blocks; extract feature vectors in a spatial domain and a frequency domain from each of the plurality of sample blocks, the feature vectors including a histogram feature, the histogram feature including ultrasonic impedance characteristics of ridges and valleys of the biometric object; and compare the feature vectors from each of the plurality of sample blocks to a classification model.

Another cited prior art, the United States of America granted patent number US9818020B2 discloses a method for determining fingerprint liveness, comprises the steps to: identify a plurality of ridge center pixels defining a centerline of a ridge segment in a gray scale fingerprint image; evaluate, for each of the plurality of ridge center pixels, gray scale values of pixels in the gray scale fingerprint image that are proximate to and located within a defined distance of that ridge center pixel to determine a center location of one or more local maxima in the gray scale fingerprint image, where the gray scale values are non-binary; evaluate the gray scale values of pixels of the gray scale fingerprint image located about the center location of at least one local maximum of the one or more local maxima to classify the at least one local maximum as a pore; determine features of each pore based upon an evaluation of the gray scale values of pixels of the gray scale fingerprint image that are located at a predefined radius around the center location of that pore; and determine liveness of the gray scale fingerprint image based at least in part upon distributions of the determined features.

However, the above mentioned cited prior arts doesn't disclose about analysis on a

risk associated with the spoof attack on the biometric device.

The present invention provides a method and system to perform the risk analysis associated with the spoof attacks due to use of the fake biometric object made from various materials and determine an impact of the risk on an organisation or individual due to the spoof attack.

SUMMARY OF THE INVENTION

The present invention provides a method to determine a risk associated with a spoof attack, the method comprises the steps: retrieve, by a biometric data acquisition module, a first biometric data from a biometric device accessed by an authorized user, whereby the first biometric data is a real biometric identification obtained from the authorized user; and retrieve, by a biometric data acquisition module, a second biometric data from the biometric device accessed by an unauthorized user using a fake biometric object, whereby the second biometric data is a fake biometric data obtained from the fake biometric object resembling the authorized user's real biometric identification, characterized in that the method further comprises the steps: compute, by a matching score computation module, a first matching score and a second matching score, by respectively comparing the first biometric data and the second biometric data against stored biometric identification data in a database; compute, by a threshold computation module, a threshold value for differentiating the real biometric data and the fake biometric data, by comparing the first similarity score with the second similarity score; and perform, by a risk analysis module, a risk analysis associated with the spoof attack which may be based on the identified fake biometric data, for determining a risk rating of the spoof attack.

Preferably, the method further comprises the step to analyse, by the risk analysis module, probability of potential spoof attack possible on the biometric device based on pre-determined factors which includes time taken to identify and exploit, expertise required, knowledge on design of the biometric device, window of access opportunity required for the attack and equipment required for exploitation.

Preferably, the method further comprises the step to calculate, by the risk analysis module, severity of impact caused by the spoof attack in an organisation.

Preferably, the risk rating of the spoof attack is determined based on the analysed probability and the calculated severity, by the risk analysis module.

Preferably, the method further comprises the step to configure, by a benchmark module, the biometric device with a benchmark matching score based on the determined threshold value, for mitigating the spoof attacks.

The present invention also provides a system to determine a risk associated with a spoof attack comprising: a biometric device, configured to collect a first biometric data and a second biometric data from a user, whereby the first biometric data is a real biometric identification obtained from the authorized user and the second biometric data is a fake biometric data obtained an unauthorized user using a fake biometric object resembling the authorized user's biometric identification; and, a computing device installed with an application module is connected to the biometric device via a communication channel comprising: a biometric data acquisition module, configured to retrieve the first biometric data and second biometric data from the biometric device, characterised in that, the application module further comprising: a matching score computation module, configured to compute a first matching score and a second matching score, by comparing the first biometric data and the second biometric data with stored biometric identification data in a database, whereby the application module is linked to the database; a threshold computation module, configured to compute a threshold value for differentiating the real biometric data and the fake biometric data, by comparing the first similarity score with the second similarity score; and a risk analysis module, configured to perform a risk analysis associated with the spoof attack which may be based on the identified fake biometric data, for determining a risk rating of the spoof attack.

Preferably, the risk analysis module is further configured to analyse a probability of

potential spoof attack possible on the biometric device based on pre-determined factors which includes time taken to identify and exploit, expertise required, knowledge on design of the biometric device, window of access opportunity required for the attack and equipment required for exploitation.

Preferably, the risk analysis module is further configured to calculate severity of impact caused by the spoof attack in an organisation

Preferably, the risk analysis module is further configured to determine the risk rating of the spoof attack, based on the analysed probability and the calculated severity.

Preferably, the application module further comprises a benchmark module configured to configure the biometric device with a benchmark matching score based on the determined threshold value, for mitigating the spoof attacks.

BRIEF DESCRIPTION OF DRAWINGS

These and other features, aspects, and advantages of the present invention will become better understood, when the following detailed description is read with reference to the accompanying drawings in which like characters represent like parts throughout the drawings, wherein:

Figure. 1 is a flow chart illustrating the process steps to determine a risk associated with a spoof attack.

Figure. 2 is a block diagram of a system to determine the risk associated with the spoof attack.

Figure. 3 illustrate an overall process of a biometric fingerprint spoofing.

Figure 4 illustrate a graph on material based average matching score.

Figure. 5 illustrate a block diagram on a risk analysis process flow.

DETAILED DESCRIPTION OF THE INVENTION

The present invention discloses to a method and a system to determine a risk associated with a spoof attack on a biometric device which includes but not limited to a fingerprint recognition device, a facial recognition device, an iris recognition device, a voice recognition device and any other biometric device known in the art.

The present invention also discloses about an application installed in a computing device configured to detect biometric liveness and determine risks associated with the spoof attack. The present invention can relate to any biometric identification which can be fingerprint, facial features, iris, and voice and any other biometric identification known in the art.

Referring to Figure 1, which illustrates the flowchart process steps (100 to 160) to determine the risk associated with a spoof attack on a biometric device (210), the process comprises the steps of: (Step 110) retrieve a first biometric data from the biometric device (210) accessed by an authorized user, by a biometric data acquisition module (231). The first biometric data is a real biometric identification obtained from the authorized user provided with an access to perform an activity. Next (Step 120) retrieve a second biometric data from the biometric device (210) accessed by an unauthorized user using a fake biometric object, by the biometric data acquisition module (231). Preferably, the fake biometric object is a fake biometric identification fabricated using at least one material to resemble the authorized user's real biometric identification. The materials can include latex, red silicone, pink silicone, wood glue, gelatin, epoxy, printed transparent paper or any other suitable material known in the art. The second biometric data is the fake biometric identification obtained from the unauthorized user using the fake biometric object. Next, process the first biometric data and the second biometric data, by a processing module (232). Preferably, in this step, noise filtering techniques and image processing techniques are performed on the retrieved first biometric data and second biometric data, by the processing module

(232). Then, store the processed data in a database (240). Next (Step 130) compute a first matching score, by a matching score computation module (233), by comparing the first biometric data with a plurality of reference biometric identification data stored in the database (240). Preferably, in this step, the authorized user identification is verified by comparing the first biometric data against all stored reference biometric data in the database (240). Next (Step 140) compute a second matching score, by the matching score computation module (233), by comparing the second biometric data against all the reference biometric data stored in the database (240). Preferably, in this step, the second matching score is computed, by the matching score computation module (233), for each material that is suitable to fabricate the fake biometric object. Next (Step 150) compute a threshold value to the step to differentiate the real biometric data and the fake biometric data, by a threshold computation module (234), by comparing the first similarity score with the second similarity score. Next (Step 160) Perform a risk analysis associated with the spoof attack which may be based on the identified fake biometric data, to determine a risk rating of the spoof attack, by a risk analysis module (235). Preferably, the risk analysis can be associated with the spoof attack when the following factors are being considered.

- Time taken to identify and exploit (Elapsed Time);
- Specialist technical expertise required (Expertise);
- Knowledge of the Target of Evaluation (TOE) design and operation (Knowledge of TOE);
- The access opportunity to the TOE that is required for the attack (Window of opportunity);
- IT hardware/software or other equipment required for exploitation (Equipment).

The method further includes steps to configure the biometric device (210) with a benchmark for the matching score based on the threshold value, by a benchmark module (236), to mitigate the spoof attacks on the biometric device (210).

The method also includes the steps to register or enroll the user, by a registration module with an application module (230) installed in a computing device (220) as the

authorized user comprises: upload an image of the identification card into the registration module to automatically key in the details or provides the user a form to manually key in the details for enrolment. Next, retrieve the user's biometric data stored in the database (240) or from a chip installed in the user's identification card, by the biometric data acquisition module (231). Then, compute the first matching score, by the matching score computation module (233), by comparing the retrieved biometric data against the first biometric data, to verify and identify the identity of the authorized user.

The method further includes the steps to perform risk analysis associated with spoof attack and determine the risk rating for each spoof attack, by the risk analysis module (235). Further, estimate the probability of potential spoof attack possible on the biometric device (210) and calculate severity of impact caused by the spoof attack in an organisation, by the risk analysis module (235). Further, determine a risk matrix calculation based on the probability and the severity, by the risk analysis module (235). Depending on the scenario, environment and organization interest, the risks associated with the spoof attack potential may differ.

Referring to Figure 2, illustrates the block diagram of the system (200) to determine the risk associated with the spoof attack comprises the biometric device (210), the computing device (220) and the database (240). Preferably, the biometric device (210) is connected to the computing device (220) via wired or wireless communication means.

The biometric device (210) can be any type of biometric system configured to provide access for the authorized and unauthorized users to verify their identity using the biometric identification. Preferably, the biometric device (210) is configured to capture the first biometric data from the authorized user and the second biometric data from the unauthorized user using the fake biometric object.

The database (240) is configured to store all the reference biometric identification data from the user. Preferably, the biometric identification data obtained from the user

during the registration process is collected and stored in the database (240) for the reference.

The computing device (220) can be a personal digital assistants (PDA), smart phones, tablets, laptops, netbooks, phablets, phoblets or any suitable devices which are capable of data processing and perform data transmission. Preferably, the computing device (220) is installed with the application module (230) is linked to the database (240). Preferably, the application module (230) can be a web application module or a mobile application module or a browser application installed in the computing device (220). The application module (230) comprises: the biometric data acquisition module (231), the processing module (232), the matching score computation module (233), the threshold computation module (234), the risk analysis module (235) and the benchmark module (236).

The biometric data acquisition module (231) is configured to retrieve the first biometric data and the second biometric data from the biometric device (210) accessed by the user. Preferably, the biometric data acquisition module (210) is configured to retrieve the first biometric data and the second biometric data in an image format.

The processing module (232) is configured to process the retrieved first biometric data and the second biometric data. Preferably, the processing module (232) is configured to perform filtering techniques and the image processing techniques on the retrieved first biometric data and the second biometric data. The image processing techniques can include sharpening, smoothening and high lightening of the details in the biometric data.

The matching score computation module (233) is configured to compute the first matching score, by comparing the first biometric data against the reference biometric identification data stored in the database (240), in order to identify and verify the authorized user identity. The matching score computation module (233) is also configured to check whether the authorized user is registered user or not, by looking

up to closest match with the first biometric data in the database (240). Further, the matching score computation module (233) is configured to compute the second matching score, by comparing the second biometric data against the stored biometric identification data in the database (240). Preferably, the matching score computation module (230) is configured to compute the second matching score for each material that is used to fabricate the fake biometric object. The matching score computation module (233) is also configured to determine high score and low score for the material used to fabricate resemblance of the real biometric identification. The high score indicates that the quality of the real biometric being replicated plays a significant role as model for fake biometric object fabrication. The higher the quality of real biometric, the higher the quality of the fake biometric data which contribute to a higher matching score. The matching score calculation is further explained detail below with respect to testing carried out.

The threshold computation module (234) is configured to compute the threshold value by comparing the first similarity score and the second similarity score, to identify the fake biometric data. Preferably, the threshold computation module (234) is configured to differentiate the fake biometric data and the real biometric data based on the computed threshold value.

The risk analysis module (235) is configured to perform risk analysis associated with spoof attack and determine the risk rating for each spoof attack. Further, the risk analysis module (235) is configured to estimate the probability of potential spoof attack possible and calculate severity of the spoof attack. Further, the risk analysis module (235) is also configured to determine a risk matrix calculation based on the probability and the severity. Depending on the scenario, environment and organization interest, the risks associated with the spoof attack potential may differ. The risk analysis is further explained in detail below.

The benchmark module (236) is configured to update the biometric device (210) with a benchmark score for the matching score based on the computed threshold value in order to mitigate the spoof attacks on the biometric device (210) using the fake

biometric object.

The application module (230) may further include the registration module configured to register or enroll the user with the application module (230) installed in a computing device (220) as the authorized user. The registration module is configured to provide the user a form to manually key in the details. The registration module can also be configured to receive an image of the identification card to automatically key in the details for enrolment.

In an exemplary embodiment, a penetration testing and an experiment for a biometric fingerprint spoofing was carried out. The system and the method of the present invention is now explained with respect to the testing and its results obtained from the testing.

The methodology of penetration testing for biometric fingerprint scanner (Biometric Fingerprint Spoofing). The biometric fingerprint scanner allows a person to be enrolled', and verified' and identified' based on his fingerprints, which is unique and specific to him. Therefore, spoofing the biometric fingerprint scanner is the process of providing a fake fingerprint cast (a look-alike original human fingerprint material) onto the biometric fingerprint scanner. This process is able to deceive the biometric fingerprint scanner by identifying/verifying the cast as a live human fingerprint.

The biometric device (210) is a biometric fingerprint scanner or Target of Evaluation (TOE). Preferably, the biometric fingerprint scanner is a touch-based optical biometric fingerprint scanner. This type of scanner is recommended to be used as an experimental target as it is being widely used in a large-scale identification system.

The test method comprises five stages namely:

i. Scope of testing.
ii. Testing environment including the configuration.
iii. Test environment preparation.
iv. Test execution.

v. Analysis of findings.

The scope of testing covers the penetration testing using biometric spoofing techniques on the biometric fingerprint scanner, which is the touch-based optical biometric fingerprint scanner.

The testing environment specifies the software and hardware configuration for the TOE deployment. It also describes the independent test tools (including the cast materials to produce fake fingerprints) used for the testing.

Additionally, before the testing is performed, it is required to conduct preparation of fake fingerprints that is described in the Test Environment Preparation. Test Environment Preparation defines the user database creation (i.e. using enrolment, verification and identification process) and the fabrication processes of fake fingerprint mould as well as casts using different types of materials.

The tests executed by following the description defined in the pre-test steps and test steps. Thus, the expected test results are specified as guidance for the penetration test results. Analysis of the findings shall discuss the comparison of the materials based on their matching score and analysis of the risks associated with the spoofing attack.

Objective:

The objective of this test is to provide guidance to researchers and evaluators to perform penetration testing on the TOE, which is focusing on touch-based optical fingerprint scanner.

Scope:

The scope of penetration testing covers the TOE using direct casting. The capabilities of the TOE as per details below:

i. Fingerprint enrolment. Software processes the fingerprint image, extracts features and writes them to the database.

ii. Fingerprint verification mode. This mode performs 1:1 (one to one)

fingerprints matching.

iii. Fingerprint identification mode. This mode performs 1:N (one to many) fingerprint matching.

The testing includes 'direct casting' method which makes use of the availability of the original finger to create a fake fingerprint. This technique is chosen due to its capability to create high quality' fake fingerprints (also known as casts) that are often used for testing the effectiveness of biometric fake fingerprint detection technology.

Before performing the spoof attack, the fake fingerprint mould and cast need to be fabricated. The cast is fabricated based on the mould. The materials used to make the fake fingerprint mould are moldable plastic, Blu Tack and Das, while the materials used to make the fake fingerprint cast are latex, wood glue, epoxy and transparent paper.

The criteria for choosing the materials for the mould is based on its capability it to hold a sufficiently detailed impression of the original fingerprint. It is also chosen due to its availability in the market with affordable price.

Test Scenario:

Assumption: It is assumed the TOE is located within a building which is sheltered from the weather and supports the functionality of the biometric system (e.g.: integration with the building's physical structure and backend databases as door locks/access controller). Thus, the environment in which a TOE operates could be public area or restricted area but it is confined to a specific location within a building/premise. It is assumed that the attacker possesses relevant legitimate user fingerprint that is valid with the information stored in the backend databases system.

Threats: An attacker may use fake fingerprint to gain unauthorized authentication and accessibility.

Objectives of testing: To fabricate fake fingerprint for spoofing using mould and cast; to spoof the TOE using the fabricated fake fingerprint; and to determine which

cast material capable of spoofing the TOE.

Test Item and Test Equipment:

Test Item:

A biometric fingerprint scanner - fingerprint scanner.

Test Equipment:

A desktop installed with a testing application to verify the fingerprint. The testing application has following operation modes: enrolment, identification and verification.

Test Environment Preparation: Process of the biometric fingerprint spoofing

Referring to Figure 3 shows the overall process of the biometric fingerprint spoofing. Steps 301 to 303 are to ensure that the chosen fingerprint data is in the Testing app's database and has a reasonably good quality prior to testing it with fake fingerprints. Note that, good quality here refers to the matching score' (as a result of comparing the image obtained from a fake fingerprint of the same person) having a sufficiently high value compared to a fingerprint template. While steps 304 to 308 are the fake fingerprint fabrication processed. Finally, the biometric fingerprint spoofing processed is executed in steps 309 to 310. The researcher/ evaluator can repeat the steps 301 to 310 with other fingers to get more samples for the analysis. Then, store the fake fingerprint in an air-tight container to preserve its quality. However, after a certain amount of time (depending on material type) the quality of fake fingerprint might deteriorate depending on the material properties. Therefore, it is recommended that the researcher/ evaluator to prepare the fake fingerprint not more than five days before the actual testing begins.

User Fingerprint Database Creation and Pre-Authentication Process:

The biometric fingerprint systems can be used in two different modes. Identity verification process (also called one-to-one matching) includes the steps: first, the user presents his/her identity (e.g. shows his/her passport). Next, based on this identity the biometric data are recalled from the passport or from a database and then compared against the current biometric data of the user. Identification process (also called search, recognition or one-to-many matching) occurs when the identity of the

user is unknown. In this case, the current biometric data is matched against all records in the database.

Before the user can be successfully verified or identified by the system, he/she is registered with the biometric system. Then, the user's biometric data is captured, processed and stored. The process of the user's registration with the biometric fingerprint system is called enrolment.

The test steps in the enrolment process, assuming the user fingerprint data does not exist in the database, the identification and the verification process for the enrolled user. Successful pre-tests steps will be indicated as 'OK' and the failure/unexpected results of those steps will be indicated as 'X'. For pre-test steps indicated as "X", the results of the test step(s) do not meet the expected results defined by the developer or evaluators.

Enrolment Process:

The TOE driver and testing application are preinstalled in the desktop. To enrol a user in the Testing app database comprises following steps: first, start testing application in the desktop. Then, a testing window contains a menu bar and a toolbar at the top, and four child windows shall appear. Next, click on "Tools" then select "Options". An options window shall appear. Next, click "Reset" to set the default setting for "Enrolment" and "Matching" tab then click "OK". Next, connect the USB of the TOE to the desktop. Then, select "fingerprint scanner on the toolbar. Next, check the "Check for duplicates" box to ensure no duplicate. Then, click "Enroll" button on the toolbar. A window shall pop up to prompt user to key in a new Id. Then, key in a new Id for the user. <User><finger number ><L (left) / R (right)>. E.g. 011R. (User number 01, thumb, right hand). And, click "OK". Then, place user's thumb on the fingerprint scanner.

Note:

i. Ensure finger is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected.

ii. Finger is in good condition (i.e. clearly defined ridges and valleys, not dry

or wet). If too dry or wet, may result in failure to capture the fingerprint image. If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is enrolled'. If no image is displayed due to bad condition of the finger, kindly repeat the steps with another finger as sample. And, click on "Save image" to save fingerprint image.

Verification Process:

To verify a registered user in the Testing app database. For an example, to verify the user 011R has been previously enrolled in the TOE database. First, start the Testing application in Desktop. Then, connect the USB of the TOE to the desktop. Then, select "From fingerprint scanner on the toolbar. Next, click "Verify" button on the toolbar. A window shall pop up to prompt user to key in the Id. Then, key in Id "011R". Next, click "OK". Then, place user 011R's thumb on the TOE. Note: Ensure finger is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. Finger is in good condition (not too dry or wet). If too dry or wet, may result in failure to capture the fingerprint image.

If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is verified'. Then, click on "Save image" to save fingerprint image. Take note of the matching score for analysis.

Results: PASSED - Successfully verify user in the fingerprint application database. The following are displayed in three windows: i. Window A: Fingerprint image is displayed. ii. Window B: Subject '011R' is verified & iii. Window C: Matching score and user ID is displayed. FAILED - The application unable to verify user.

Identification Process:

Objective: To identify a registered user in the Testing application database.

Description: User 011R has been previously enrolled in the Testing application database.

Test Steps: First, click to start Testing application in Desktop. A testing window contains a menu bar and a toolbar at the top, and four child windows shall appear.

Then, connect the USB of the TOE to the desktop. The bottom left window shall display " fingerprint scanner connected." Then, select " fingerprint scanner on the toolbar. Then, click "Identify" button on the toolbar. Next, place user 011R's thumb on the TOE.

Note: i. Ensure finger is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. ii. Finger is in good condition (does not have any scar, not dry or wet). If too dry or wet, may result in failure to capture the fingerprint image.

If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is identified'. Then, click on "Save image" to save fingerprint image. Take note of the matching score for analysis.

Fabrication of Fake Fingerprint:

There are several methods to fabricate the fake fingerprint. However, in an exemplary embodiment the method to fabricate the fake fingerprint using various material includes steps: (i) Fabrication of Fingerprint mould; and (ii) Fabrication of Fingerprint cast.

(i) **Fabrication of Fingerprint Mould:**

The direct casting of the fake fingerprint is created by means of a mould using moldable materials such as (a) Plastic (b) Blu Tack and (c) Das. The mould material needs to be sufficiently soft so that the original finger can be pressed against it to create a negative of the original fingerprint. The finger needs to be pressed against the mould in a very careful manner so that all the fingerprint details are being preserved and lifted back; and the mould needs to be able to harden, providing the negative for the fake fingerprint fabrication.

(a) Fabricating Mould - Moldable Plastic:

Objective: Fabricating fake fingerprint mould using Hand Moldable Plastic (Moldable Plastic).

Environment Details: Ventilated room.

Supporting tools - Electronic kettle, mug, metal spoon, cold water, magnifier, water,

metal spoon, stirring rod.

Pre-Test Steps: First, protect work area with a baking paper. Then, heat some water in an electronic kettle until it boils. Then, fill in the boiling water into a suitable container made of glass or ceramic. Note: The container should not be made of plastic, as the plastic pallets can stick to the plastic container's surface. Next, add the desired number of Moldable Plastic pellets into the hot water. Note: Half a quarter of a tea spoon of pallets are enough to fabricate a finger. Next, allow the pellets to heat until clear in color and clump together. Note: If they haven't turned clear, try to add in more hot water. If pellets are not clumped together, stir it using a metal spoon or glass stirring rod. Note: Researcher/ evaluator can use other material that does not stick to the moudable plastic to remove the pellets. Then, remove pellets from water with a metal spoon or glass stirring rod. Caution: Pellets might still be hot. Get rid of any remaining liquid between the pellets. Then, start smooth out the clump pellets into a mould by hand once it is cool enough. Caution: Moulding process need to be executed before the plastic turns white/ opaque. If it turns white, put it back again into the hot water. Note: Ensure that no air bubble can be seen. Next, place a finger that has been enrolled and verified/identified to be replicated on to the plastic mould. Then, press the mould on a table to ensure that the mould is flat. Then, hold it for a minute until the plastic mould becomes white to ensure fingerprint pattern is replicated on the mould. Note: Press the mould on a flat surface to get a better replication of the ridges and valleys. Upon the fingerprint pattern is replicated on the mould. Then, remove the finger from the mould carefully and slowly. Next, allow to cool naturally within 1 to 2 minutes. Once completely cooled, plastic mould will then be as solid and strong as before it was heated. Then, inspect the mould created using a magnifier or under a light source. If ridges and valleys on the fingerprint mould cannot be seen clearly, then repeat process.

(b) Fabricating Mould using Blu Tack:

Objective: Fabricating fake fingerprint mould using Blu Tack.

Environment Details: Ventilated room.

Supporting Tools - Smooth surface, cutter, baking paper, and roller.

Pre-Test Steps: First, begin working over a smooth, clean, nonporous surface. Ensure

user's fingers are clean and dry before taking a mould. It is advisable to ensure fingernails are trimmed as well. Then, roll the Blu Tack into a smooth ball. Then, flatten and smooth it between two sheets of paper. Next, lift the top paper and make a fingerprint impression on the top surface. Note that the finger must be from the enrolled and verified/identified user. Then, keep the finger straight and press deep into the mould without going all the way through, this gives a good deep impression. Then, press the mould on a table to ensure that the mould is flat. Then, hold for 30-40 seconds to ensure fingerprint is replicated on the mould. Upon the fingerprint pattern is replicated on the mould, then remove the finger carefully and slowly. Then, inspect the mould created using a magnifier or under a light source.

(c) Fabricating Mould using Das:

Objective: Fabricating fake fingerprint mould using Das - Modelling Material (Das)

Environment Details: Ventilated room.

Supporting Tools - Smooth surface, cutter, baking paper, and roller.

Pre-Test Step: First, begin working over a smooth, clean, nonporous surface. Then, ensure user's fingers are clean and dry before taking a mould. It is advisable to ensure fingernails are trimmed as well. Then, open the sealed bag of clay and pinch off or cut off the amount of clay needed. Then, knead the clay until it is soft. Note: Kneading and massaging the clay will soften it and make it easier to work with. The warmth of the hands will spread to the clay and make it malleable. Then, condition the clay for proper use. If using paper based clay, add in a one or two teaspoon of water to additionally soften the clay. Then, roll the clay into a smooth ball. Then, flatten and smooth it between two sheets of baking paper. Then, lift the top paper and make a fingerprint impression on the top surface. Then, finger must be from the enrolled and verified/identified user. Next, keep the finger straight and press deep into the clay for 45 seconds to 1 minute to ensure fingerprint is replicated on the clay properly. Note: Press the mould on a table to get a better replication of the ridges and valleys. Ensure the mould is flat. Upon the fingerprint pattern is replicated on the mould, then remove the finger carefully and slowly. Next, allow the clay mould to harden for 10 to 15 minutes before putting in the cast. Then, inspect the mould created using a magnifier or under a light source. If ridges and valleys on the fingerprint mould cannot be seen

clearly then repeat the process.

(ii) Fabrication of Fake Fingerprint Cast:

The materials used for the fabrication of the fake fingerprint cast are but not limiting to (a) silicone, (b) latex, (c) wood glue, (d) epoxy resin and (e) transparent paper, it is also necessary to take the mould material into consideration as well. Preferably, two types of silicone materials are used, they are (a1) pink silicone and (a2) red silicone. The mould and the fake fingerprint cast material are not allowed to be held together during the fake fingerprint hardening process, else they will chemically react and the quality of the resulting finger would be impaired. Carefully remove the hardened fake fingerprint from the mould without having bits of the mould stuck in the resulting 3D fingerprint pattern. The cast shall retain the exact replica of the fingerprint's pattern including its ridges and valleys. Once the creation of a fake fingerprint is completed, they are ready to be tested on a targeted biometric scanner using define test steps in the later section.

(a1) Fabricating cast using Pink Silicone:

Fabricating Cast Test steps - Pink Silicone

Objective: Fabricating fake fingerprint cast using Silicone Mould making Rubber (Pink Silicone).

Environment Details: Ventilated room.

Supporting Tools: Latex gloves, clothing, eye and face protection. Digital scale, plastic cups, syringe, paint brush. Recommended mould - Moldable Plastic, Blu Tack and DAS.

Pre-Test Step: First, protect work area with a freezer paper, newspaper or wax paper. Then, work in a ventilated and above 20 °C temperature room. Next, shake the Pink Silicone base container well before use. Next, weigh the desired amount of base into a clean mixing container (plastic cup) and put it on a digital scaling machine. Then, shake the catalyst container well before use. Then, put in the right catalyst volume into a mixing container using a syringe. Note: Always weight the silicone and catalyst precisely before mixing otherwise the silicone may not cure. The two components mix easily and is widely used without a vacuum chamber. For best result ensure materials

are at temperature above 20 before using, using at a colder temperature will affect cured characteristics and may inhibit cure. Next, stir the mixture well. Then, choose a mould (either Moudable plastic, DAS or Blu Tack) Note: Ensure moulds are free from dust and other contaminants. Next, pour the mixture prepared in above into the desired mould. Note: Pouring gently at the lowest point and in a long streaky stream in mould box helps to ensure bubble burst. Then, flatten and distribute the mixture uniformly with a brush. Note: Ensure that the mixture is as thin as possible (approximately 1-2 mm). However, the thickness of the cast depends on the material, throughout trial and error the researcher/ evaluator shall be able to estimate the thickness most suitable for spoofing. Let the mixture dry to become a cast in room temperature (25°C) for 24 hours before removing it from the mould. Note: i. Working time: 40 - 60 minutes. ii. Curing time 25C: 6 - 8 Hours (Even though a product can be demoulded and feels cured, curing may continue for up to one week.) iii. Demould Time: 12 - 24 Hours (This is the soonest recommended time a cured part can be removed from the mould if the mould was cured at room temperature.). Then, remove the cast from the mould slowly and carefully using a cutter. The cast is now ready to be a fake fingerprint. Next, inspect the fake fingerprint created using a magnifier. If the ridges and valleys could not be seen, then repeat above steps.

(a2) Fabricating cast using Red Silicone:

Objective: Fabricating fake fingerprint cast using RTV Silicone Mould Making Rubber (Red Silicone)

Environment Details: Ventilated room.

Supporting Tools: Latex gloves, clothing, eye and face protection. Digital scale, plastic cups, syringe, paint brush. Recommended mould - Plastic, Blu Tack and DAS mould.

Pre-Test Step: First, protect work area with a freezer paper, newspaper or wax paper. Then, wear suitable protective gloves and eye/face detection. Next, shake the Red Silicone base container well before use. Then, weigh the desired amount of base into a clean mixing container and put it on a digital scaling machine. Next, shake the Red Silicone catalyst container well before use. Then, pour the catalyst on the base mixing container using a syringe and gently mix together avoiding as much air entrapment as

possible. Then, mix ratio: 100 bases: catalyst by weight. Caution: Always weight the silicone and catalyst precisely before mixing otherwise the silicone may not cure. As the mixed material becomes more intermixed you can employ more vigor. Then, choose a mould (either plastic, DAS or Blu Tack) Note: Ensure moulds are free from dust and other contaminants. Then, pour the mixture prepared in above steps into the desired mould. Note: Pouring gently at the lowest point and in a long streaky stream in mould box helps to ensure bubble burst. Next, flatten and distribute the mixture uniformly with a brush. Note: Ensure that the mixture is as thin as possible (approximately 1-2 mm). However, the thickness of the cast depends on the material, throughout trial and error the researcher/ evaluator shall be able to estimate the thickness most suitable for spoofing. Then, let the mixture hardens to become a cast in room temperature (25°C) for 24 hours before removing it from the mould. Next, remove the cast from the mould slowly and carefully using a cutter. The cast is now ready to be a fake fingerprint. Next, inspect the fake fingerprint created using a magnifier. If the ridges and valleys could not be seen, then repeat steps above.

(b) Fabricating cast using Latex:

Fabricating Cast Test steps - Latex

Objective: Fabricating fake fingerprint cast using Liquid Latex Rubber (Latex).

Environment Details: Ventilated room.

Supporting Tools: Latex gloves, mask. Paint brush, cutter, baking paper. Recommended mould - Plastic mould.

Pre-Test Step: First, use a well-ventilated room. Then, protect work area with a freezer paper, newspaper or wax paper. Next, apply the Latex in the desired mould (plastic) by using a brush. Then, ensure the layer is thin and flat. Note: Ensure that the mixture is as thin as possible (approximately 1-2 mm). However, the thickness of the cast depends on the material, throughout trial and error the researcher/ evaluator shall be able to estimate the thickness most suitable for spoofing. Then, let the cast dried for a few hours (4-6 hours). Then, ensure that the cast has fully dried. Next, remove the cast from the mould slowly and carefully. The cast is now ready to be a fake fingerprint. Next, inspect the fake fingerprint created using a magnifier. If the ridges and valleys could not be seen, then repeat steps mentioned above.

(c) Fabricating cast using Wood Glue:

Fabricating Cast Test steps - Wood Glue

Objective: Fabricating fake fingerprint cast using Wood Glue

Environment Details: Ventilated room.

Supporting Tools: Latex gloves, mask. Paint brush, cutter, baking paper. Ventilated room. Recommended mould - Moldable Plastic.

Pre-Test Step: Use a well-ventilated room. First, protect work area with a freezer paper, newspaper or wax paper. Then, apply the Wood glue in the desired mould by using a brush. Then, ensure the layer is thin and flat and no bubbles can be seen. Note: Ensure that the mixture is as thin as possible (approximately 1-2 mm). However, the thickness of the cast depends on the material, throughout trial and error the researcher/ evaluator shall be able to estimate the thickness most suitable for spoofing. Then, let the cast dried for a few days (3-4 days). Next, ensure that the cast has fully dried. Remove the cast from the mould slowly and carefully using a cutter. The cast is now ready to be a fake fingerprint. Note: Do not remove the cast from the mould if tester is not ready to use it in order to avoid the cast drying out. Then, keep the cast intact to the mould and store it in air-tight container. Next, inspect the fake fingerprint created using a magnifier. If the ridges and valleys could not be seen, then repeat steps as above mentioned.

(d) Fabricating Cast using Epoxy:

Fabricating Cast Test steps - Epoxy

Objective: Fabricating fake fingerprint cast using Hard Epoxy Resin (Epoxy)

Environment Details: Ventilated room.

Supporting Tools: Latex gloves, mask. Paint brush. Recommended mould - Moldable Plastic.

Pre-Test Step: Use a well-ventilated room. First, protect work area with a freezer paper, newspaper or wax paper. Then, take two-part epoxy and mix together using 1:1 ratio. Next, apply the mixture in the desired mould (plastic). Then, ensure the layer is thin and flat. Note: Ensure that the mixture is as thin as possible (approximately 1-2 mm). However, the thickness of the cast depends on the material, throughout trial and

error the researcher/ evaluator shall be able to estimate the thickness most suitable for spoofing. Then, let the cast dried for a few days (3-4 days). Then, ensure that the cast has fully dried. Next, remove the cast from the mould slowly and carefully using a cutter. The cast is ready to be used as fake fingerprint. Next, inspect the fake fingerprint created using a magnifier. If the ridges and valleys could not be seen, then repeat steps mentioned above.

(e) Fabricating Cast using Printed Transparent Paper:

Fabricating Cast Test steps - Printed Transparent Paper

Objective: Fabricating fake fingerprint cast using printed transparent paper

Environment Details: Ventilated room.

Supporting Tools: Laser Jet Printer, transparent paper and previously enrolled fingerprint image

Pre- Test Step: First, open the user's fingerprint images that have been saved during the enrolment. Then, copy the image into word document. Next, resize the image too approximately to a fingerprint size around 1 inch of height and 3/4 inch of length. Then, print the image using transparent paper that is meant for Laser Jet Printer. Then, cut the printed copy to match finger print size. Next, inspect the cast created using a magnifier. If the ridges and valleys could not be seen, then repeat steps as mentioned above.

Using the fabricated fake fingerprint mould and cast the spoof attack test was executed on the TOE. In an exemplary embodiment, the spoof attack was executed by using the various combinations of materials used for the fabricated fake fingerprint cast and mould as following: (a) Test Group - Moldable Plastic and Pink Silicone; (b) Test Group - Moldable Plastic and Red Silicone; (c) Test Group - Moldable Plastic and Latex; (d) Test Group - Moldable Plastic and Wood Glue Table; (e) Test Group - Moldable Plastic and Epoxy; (f) Test Group - Blu Tack with Pink Silicone; (g) Test Group - Blu Tack with Red Silicone; (h) Test Group - DAS and Pink Silicone; and (i) Test Group - Printed fingerprint on Transparent Paper.

(a) Test Group - Moldable Plastic and Pink Silicone:

Objective: To spoof a TOE using fabricated fake fingerprint Pink Silicone as cast in order to gain access to biometric fingerprint system.

Environment Details: Ventilated room.

Supporting Tools: TOE driver and Testing app should be installed in desktop. Moldable Plastic as mould and Pink Silicone as cast.

Pre-Test Step: First, prepare the mould using the steps in test preparation for Plastic Mould. Then, pour in the cast made from user enrolled which is made using the steps in test preparation for Pink Silicone Cast into the mould.

Test Step: First, click to start testing application in Desktop. Then, connect the USB of the TOE to the desktop. The bottom left window shall display "fingerprint scanner connected." Then, select "fingerprint scanner on the toolbar. Then, click "Identify" button on the toolbar. Next, place the prepared fake fingerprint cast on the TOE. Note: Ensure thumb is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is identified'. Next, take note of the matching score for analysis. Result: Passed - Spoofing attack using Pink Silicone as fake fingerprint cast on a previously enrolled user is successful.

(b) Test Group - Moldable Plastic and Red Silicone:

Objective: To spoof a TOE using fabricated fake fingerprint Red Silicone as cast in order to gain access to biometric fingerprint system.

Environment Details: Ventilated room.

Supporting Tools: The TOE driver and Testing app installed in desktop. Moldable Plastic as mould and Red Silicone as cast.

Pre-Test Step: First, prepare the mould using the steps in test preparation for Moldable Plastic. Then, pour in the cast which is made using the steps in test preparation for Red Silicone into the mould as mentioned above. Then, ensure that the cast pass the test.

Test Step: First, click to start testing application in Desktop. Then, connect the USB of the TOE to the desktop. The bottom left window shall display "fingerprint scanner connected." Then, select "fingerprint scanner on the toolbar. Next, click "Identify"

button on the toolbar. Then, place the prepared fake fingerprint cast on the TOE. Note: Ensure thumb is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is identified'. Then, take note of the matching score for analysis.

(c) Test Group - Moldable Plastic and Latex:

Objective: To spoof a TOE using fake fingerprint Latex as cast in order to gain access to biometric fingerprint system.

Environment Details: Ventilated room.

Supporting Tools: The TOE driver and testing app should be installed in desktop. Moudable Plastic as mould and Latex as cast.

Pre-Test Step: First, prepare the mould using the steps in test preparation for Mould Plastic. Then, pour in the cast which is made using the steps in test preparation for Latex Cast into the mould as mentioned above. Next, ensure that the cast pass the test.

Test Step: First, click to start testing application in Desktop. A testing window contains a menu bar and a toolbar at the top, and four child windows shall appear. Then, connect the USB of the TOE to the desktop. The bottom left window shall display "fingerprint scanner connected." Then, select " fingerprint scanner " on the toolbar. Then, click "Identify" button on the toolbar. Then, place the prepared fake fingerprint cast on the TOE. Note: Ensure thumb is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is identified'. Then, take note of the matching score for analysis.

(d) Test Group - Moldable Plastic and Wood Glue Table:

Objective: To spoof a TOE using fake fingerprint Wood glue as cast in order to gain access to biometric fingerprint system.

Environment Details: Ventilated room.

Supporting Tools: The TOE driver and Testing app should be installed in desktop. Moldable Plastic as mould and Wood glue as cast.

Pre-Test Step: First, prepare the mould using the steps in test preparation for Plastic Mould. Then, pour in the cast which is made using the steps in test preparation for Wood Glue Cast into the mould as mentioned above. Next, ensure that the cast pass the test.

Test Step: First, click to start testing application in Desktop. A testing window contains a menu bar and a toolbar at the top, and four child windows shall appear. Then, connect the USB of the TOE to the desktop. The bottom left window shall display " fingerprint scanner connected." Then, select " fingerprint scanner on the toolbar. Then, click "Identify" button on the toolbar. Next, place the prepared fake fingerprint cast on the TOE. Note: Ensure thumb is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is identified'. Then, take note of the matching score.

(e) Test Group - Moldable Plastic and Epoxy:

Objective: To spoof a TOE using fake fingerprint Epoxy as cast in order to gain access to biometric fingerprint system.

Environment Details: Ventilated room.

Supporting Tools: The TOE driver and Testing app should be installed in desktop. Moldable Plastic as mould and as Epoxy as cast.

Pre-Test Step: First, prepare the mould using the steps in test preparation for Plastic Mould. Then, pour in the cast which is made using the steps in test preparation for Epoxy Cast into the mould as mentioned above. Next, ensure that the cast pass the test.

Test Step: First, click to start testing application in Desktop. A testing window contains a menu bar and a toolbar at the top, and four child windows shall appear. Then, connect the USB of the TOE to the desktop. The bottom left window shall display " fingerprint scanner connected." Then, select " fingerprint scanner on the toolbar. Then, click "Identify" button on the toolbar. Then, place the prepared fake fingerprint cast on the TOE. Note: Ensure thumb is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not

detected. If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is identified'. Then, take note of the matching score. The system should indicate identification process is successful.

(f) Test Group - Blu Tack with Pink Silicone:

Objective: To spoof a TOE using fake fingerprint Pink Silicone as cast in order to gain access to biometric fingerprint system.

Environment Details: Ventilated room.

Supporting Tools: The TOE driver and Testing app should be installed in desktop. Blu Tack as mould and Pink Silicone as cast.

Pre-Test Step: First, prepare the mould using the steps in test preparation for Blu Tack Mould. Then, pour in the cast which is made using the steps in test preparation for Pink Silicone into the mould as mentioned above. Next, ensure that the cast pass the test.

Test Step: First, click to start testing application in Desktop. A testing window contains a menu bar and a toolbar at the top, and four child windows shall appear. Then, connect the USB of the TOE to the desktop. The bottom left window shall display " fingerprint scanner connected." Then, select " fingerprint scanner on the toolbar. Then, click "Identify" button on the toolbar. Next, place the prepared fake fingerprint cast on the TOE. Note: Ensure thumb is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is identified'. Then, take note of the matching score.

(g) Test Group - Blu Tack with Red Silicone:

Objective: To spoof a TOE using fake fingerprint Red Silicone as cast in order to gain access to biometric fingerprint system.

Environment Details: Ventilated room.

Supporting Tools: The TOE driver and Testing app should be installed in desktop. Blu Tack as mould and Red Silicone as cast

Pre-Test Step: First, prepare the mould using the steps in test preparation for Blu Tack

Mould. Then, pour in the cast which is made using the steps in test preparation for Red Silicone into the mould as mentioned above. Next, ensure that the cast pass the test.

Test Step: First, click to start testing application in Desktop. A testing window contains a menu bar and a toolbar at the top, and four child windows shall appear. Then, connect the USB of the TOE to the desktop. The bottom left window shall display " fingerprint scanner connected." Then, select fingerprint scanner on the toolbar. Click "Identify" button on the toolbar. Next, place the prepared fake fingerprint cast on the TOE. Note: Ensure thumb is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is identified'. Then, take note of the matching score. The system should indicate identification process is successful.

(h) Test Group - DAS and Pink Silicone:

Objective: To spoof a TOE using fake fingerprint Pink Silicone as cast in order to gain access to biometric fingerprint system.

Environment Details: Ventilated room.

Supporting Tools: The TOE driver and Testing app should be installed in desktop. DAS as mould and Pink Silicone as cast.

Pre-Test Step: First, prepare the mould using the steps in test preparation for DAS Mould. Then, pour in the cast which is made using the steps in test preparation for Pink Silicone into the mould as mentioned above. Next, ensure that the cast pass the test.

Test Step: First, click to start testing application in Desktop. A testing window contains a menu bar and a toolbar at the top, and four child windows shall appear. Then, connect the USB of the TOE to the desktop. The bottom left window shall display " fingerprint scanner connected." Then, select " fingerprint scanner on the toolbar. Then, click "Identify" button on the toolbar. Then, place the prepared fake fingerprint prepared on the TOE. Note: Ensure thumb is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. If successful, Window A shall display the original fingerprint

image and Window B shall state 'Subject 011R is identified'. Then, take note of the matching score.

(i) Test Group - Printed fingerprint on Transparent Paper:

Objective: To spoof a TOE using fake fingerprint Transparent Paper in order to gain access to biometric fingerprint system.

Environment Details: Ventilated room.

Supporting Tools: The TOE driver and Testing app should be installed in desktop. Printed fingerprint on transparent paper as cast. Latex gloves.

Pre-Test Step: First, prepare the fake fingerprint using the steps in test preparation for Printed Transparent paper. Then, ensure that the cast pass the test.

Test Step: First, click to start testing application in Desktop. A testing window contains a menu bar and a toolbar at the top, and four child windows shall appear. Then, connect the USB of the TOE to the desktop. The bottom left window shall display " fingerprint scanner connected." Then, select " fingerprint scanner on the toolbar. Click "Identify" button on the toolbar. Then, place the printed fingerprint prepared on the TOE. Note: i. Wear a latex glove to cover the printed fingerprint. ii. Ensure thumb is pressed uniformly on the scanner. Too much pressure makes the image blur while too low pressure will cause finger not detected. If successful, Window A shall display the original fingerprint image and Window B shall state 'Subject 011R is identified'. Then, take note of the matching score.

Upon the spoof attack execution completed, the risk analysis is performed for the spoof attack. Before performing the risk analysis following steps are performed: (a) data required for the analysis; and (b) material based matching score comparison.

(a) Data Required for Analysis:

In order to find out what affects the performance and which material is the best for making the fake fingerprint, the data required for analysis are as below:

i. The matching score for ten (10) real fingerprints of one person from the left and right hands (thumb, index, middle, ring and little finger). Score can be obtained during verification/ identification process. These fingers are name as fingers

sequence.

ii. The matching score from four (4) samples of Latex fake fingerprint cast using the same fingers.

iii. The matching score from four (4) samples of Pink Silicone fake fingerprint cast using the same fingers.

iv. The matching score from four (4) samples of Red Silicone fake fingerprint cast using the same fingers.

v. The matching score from four (4) samples of Wood Glue fake fingerprint cast using the same fingers.

Note: The mould used for fabricating each fake fingerprint above is the Moldable plastic. This is due to the following reasons:

i. Plastic mould is easy to prepare and required short drying time (1-2 minutes). ii. Suitable to be used for all cast material presented in this document i.e. Pink Silicone, Red Silicone, Latex and Wood Glue due to its hard and non-stick properties.

(b) Material Based Average Matching Score Comparison:

Referring to Figure. 4, the graph shows the average matching score for five fingers (1 - Thumb, 2- Index, 3-Middle, 4-Ring, 5-Little) of the left and right hands using four different fake fingerprint materials (Latex, Red Silicone, Pink Silicone and Wood glue) compared against the matching score of a real finger using the same fingers, by the matching score computation module (233). Based on the graph, the high score is categorized as 400 and above and low score is categorized as 399 and below, by the matching score computation module (233). It can be observed that the overall fake fingerprint matching score is lower than the matching score of the real fingers. However, the matching score trend of the real fingers that is the index finger has the highest score for both left and right hands, while, the little finger has the lowest score. This score correlates to the score of the real index finger which is high as well. The high score indicates that the quality of the real finger being replicated plays a significant role as model for fake fingerprint fabrication. The higher the quality of real finger, the higher the matching scores of the fake fingerprint. The graphs also show the Pink Silicone fake fingerprint for the left index finger has the highest average matching score (339), which indicates this material higher capacity at capturing the

fine details of human fingerprints. Whereas, the wood glue fake fingerprint has the lowest average matching score (0) for left and right thumb, middle and index fingers. This might be due to the fact that Wood glue is not flexible and easily dried up thus, not following the elasticity properties of a human finger. Another area that can be analysed from the graph is the matching score range of real finger compared to the fake fingerprint. The real fingers have the range between 219 to 576, while the fake fingerprint have the range between 0 to 219. Therefore, the threshold for matching score can be set to 200 and above in order to mitigate the probability of spoofing attacks, by the threshold computation module (234).

Risk Analysis:

There are many different approaches to perform the risk analysis. Depending on the scenario, environment and organization interest, the risks associated with the attack potential may differ. Therefore, the evaluator/researcher has to gauge which approaches that meet the condition of their testing scenarios. The method used to analyse risks associated with spoofing attack is as shown in the Figure. 5.

In an exemplary, the risk analysis is performed by the following steps: (a) TOE attack potential calculation; (b) Probability of attack potential estimation; (c) Severity Calculation; (d) Risk Matrix; and (e) Risk Rating.

(a) TOE Attack Potential Calculation:

The spoof attack potential is numerically expressed as the unauthorized user's potential that is required to execute the spoof attack scenarios for exploiting vulnerabilities. Preferably, the risk rating is expressed as the sum of the numerical values calculated for each of the pre-determined factors as stated: a. Time taken to identify and exploit (Elapsed Time); b. Specialist technical expertise required; c. Knowledge of the TOE design and operation; d. The access opportunity to the biometric device that is required for the attack (window of opportunity); and e. IT hardware/software or other equipment required for exploitation as shown in Table 1 & Table 2 below.

Factor	Value
Elapsed Time	
≤ one day	0
≤ one week	1
≤ two weeks	2
≤ one month	4
≤ two months	7
≤ three months	10
≤ four months	13
≤ five months	15
≤ six months	17
> six months	19
Expertise	
Layman	0
Proficient	3
Expert	6
Multiple Expert	8
Knowledge of Biometric Device	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary/Unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	-
Equipment	
Standard	0
Specialized	4
Bespoke	7
Multiple Bespoke	9

Table 1: Attack Potential Ratings

Values	Attack Potential required to identify and exploit vulnerability
0-9	Basic
10-13	Enhanced-Basic
14-19	Moderate
20-24	High
=>25	Beyond High

Table 2: Attack Potential Ratings

Depending on the situation, the spoof attack potential may be different. The risk analysis module (235) is configured to determine the type of the spoof attack potential in various scenarios based on the biometric device configurations. Below are examples of the spoof attack potentials for different kind of scenarios 1 to 3:

Scenario 1: Enhanced basic spoof attack potential

The risk analysis module (235) is configured to perform the risk analysis in the scenario, where the TOE is not configured with the liveness detection. In this scenario, the knowledge of the TOE is sufficient enough to spoof it using certain kind of fake fingerprint (e.g. wood glue material). However, the unauthorized user/attacker needs to learn and fabricate the fake fingerprint. This might require more time (one month below) as the attacker needs time for trial and error. By the time the attacker managed to spoof he/she is considered proficient. If the TOE is in the possession of the attacker, the window of opportunity may be considered unnecessary/unlimited. While, some specialized equipment (e.g. the different materials of fake fingerprint) is needed. Given these conditions, the attack potential is considered as basic as shown in the Table 3 below.

Attack	Elapsed time	Expertise	Knowledge of TOE	Window of opportunity	Equipment	Required attack potential	
						Sum	Rating
Scenario 1	4	3	0	0	4	11	Enhanced basic

Table 3: Example of enhance basic attack potential rating calculation

Scenario 2: Moderate spoof attack potential

In this scenario, the TOE is set with high quality threshold value without liveness detection. The attacker has to fabricate the fake fingerprint with greater details, therefore specialised skill is needed. Training is required to know how to fabricate, therefore the time taken might be below one month. Some specialized equipment (e.g. the different materials) is also needed. The window of opportunity is easy to get if the sensor is unattended example in attendance system. Given these conditions, the attack potential is considered as moderate as shown in the Table 4 below.

Attack	Elapsed time	Expertise	Knowledge of TOE	Window of opportunity	Equipment	Required attack potential	
						Sum	Rating
Scenario 2	4	6	3	0	4	17	Moderate

Table 4: Example of moderate attack potential rating calculation

Scenario 3: High spoof attack potential

In this scenario, the biometric fingerprint scanner is configured with the liveliness detection (or spoof detection) and its measures incorporated in it. Usually, these measures are useful only as long as the attacker does not know their functional principle and are kept secret as intellectual property. Hence, expertise and knowledge of the TOE are vital to deceive the liveliness detection. The unauthorized user either needs to produce a fake fingerprint replicating the liveliness features or to manipulate the sensor so that the liveliness detection is deactivated. In this case, some special equipment may be needed. If the TOE is at the border control or at the work station, the window of opportunity is difficult. In total, it can be considered the attack potential for circumventing liveliness detection as high as shown in Table 5 below.

Spoof Attack	Elapsed time	Expertise	Knowledge of TOE	Window of opportunity	Equipment	Required attack potential	
						Sum	Rating
Scenario 3	7	6	7	4	4	25	High

Table 5: Example of moderate attack potential rating calculation

(b) Probability of Attack Potential Estimation:

The probability of the spoof attack depends on the attack potential that the TOE is

able to withstand. A low attack potential corresponds to a high probability of successful attacks since many possible unauthorized user will have the necessary attack potentials. Conversely, a high attack potential suggests a low probability of successful attacks since the number of the unauthorized user with the necessary attack potential is expected to be comparatively small as shown in Table 6 below.

Values	Attack potential required to identify and exploit vulnerability	Probability for the TOE to be exploited
0-9	Basic	Very High (Most likely to happen)
10-13	Enhanced Basic	High (Very likely to happen)
14-19	Moderate	Moderate (Likely to happen)
20-24	High	Low (Unlikely to happen)
=>25	Beyond High	Very Low (Very unlikely to happen)

Table 6: Attack potential relationship with probability/frequency

(c) Severity Calculation:

The risk analysis module (235) configured to calculate the severity of the spoof attack depending on type of the impact and the seriousness of each impact on individual/ organization/ nation. The risk analysis module (235) is also configured to classify the degree of seriousness of each impact as low, medium, high, severe and emergency. Based on the individual/ organization/ nation, the severity rating may be different. The risk analysis module (235) is further configured to calculate the severity for different stakeholders by using methods as explained below as an example:

a. Common Vulnerability Scoring System (CVSS) for the TOE usage that has an impact on individual/ organization. The risk analysis module (235) is configured to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. Preferably, the risk analysis module (235) configured to translate the numerical score into a qualitative representation

(such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

b. National Cybersecurity and Communication Integration Centre (NCCIC) Cyber Incident Scoring System for the TOE usage that has an impact on public health or safety/ national security/ economic security/ foreign relations/ civil liberties or public confidence.

This method addresses incident from a nationwide perspective, which may involve large number of enterprises. It also permits a similar incident experienced by two different stakeholders to have significantly different scores based on the national-level potential impact of each affected entity. The NCISS uses a weighted arithmetic mean to produce score from 0 to 100. However, this system is not intended to be the complete scoring of the risk associated with an incident.

However, the above mentioned methods are not the only methods to calculate the severity.

(d) Risk Matrix:

The risk analysis module (235) is configured to calculate the risk matrix based on the probability and severity of the spoof attack. The risk matrix is a matrix that is used during risk analysis to define the level of risk by considering the category of probability or likelihood against the category of consequence severity. This is a simple mechanism to increase visibility of risks and assist management decision making. The followings are two risk matrixes for researcher/evaluator's reference.

i. Risk Matrix for the TOE that impact on individual or organization as shown in Table 7 below.

	SEVERITY

		None (Unlikely to impact individual or organization)	Low (May impact to individual or organisation)	Medium (Likely to result in a demonstrate impact to individual or organisation)	High (Likely to result in a significant impact to individual or organisation)	Critical (Poses an imminent threat to the lives of individual or organisation)
PROBABILITY	**Very Low (Very unlikely to happen)**	Low	Low	Low	Low	Medium
	Low (Unlikely to happen)	Low	Low	Medium	Medium	High
	Moderate (Likely to happen)	Low	Medium	Medium	High	Critical
	High (Very likely to happen)	Low	Medium	High	Critical	Critical
	Very High (Most likely to happen)	Medium	High	Critical	Critical	Critical

Table 7: Risk Matrix for the TOE that impact on individual or organisation

ii. Risk Matrix for TOE that impact Public Health or Safety, national security, economic security, foreign relations, civil liberties or public confidence as shown in Table 8 below.

	SEVERITY					
		Low (Unlikely to impact public health or safety, national security, foreign relations, civil libraries or public confidence)	**Medium (May impact public health or safety, national security, foreign relations, civil libraries or public confidence)**	**High (Likely to result in a demonstrate impact to public health or safety, national security, foreign relations, civil libraries or public confidence)**	**Severe (Likely to result in a significant impact to public health or safety, national security, foreign relations, civil libraries or public confidence)**	**Emergency (Poses an imminent threat to the lives of impact public health or safety, national security, foreign relations, civil libraries or public confidence)**

PROBABILITY						
	Very Low (Very unlikely to happen)	Low	Low	Low	Low	Medium
	Low (Unlikely to happen)	Low	Low	Medium	Medium	High
	Moderate (Likely to happen)	Low	Medium	Medium	High	Critical
	High (Very likely to happen)	Low	Medium	High	Critical	Critical
	Very High (Most likely to happen)	Medium	High	Critical	Critical	Critical

Table 7: Risk Matrix for the TOE that impact on public health or safety, national security, foreign relations, civil libraries or public confidence

(e) Risk rating: By cross-matching the probability and severity, the risk rating is determined. Each risk rating definition is described as shown in Table 9 below.

Definition of Risk Rating	
Low	• No mitigation required or risk mitigation has implemented successfully. • Actions must be taken to maintain the risk level and implemented in long-term plan.
Medium	• Management attention needed. • Risk mitigation is required to lower the risk to an acceptable level. • Risk mitigation plan must be developed and implemented in mid-term plan (six months)
High	• Management attention needed. • Risk mitigation is required to lower the risk to an acceptable level. • Risk mitigation plan must be developed and implemented in short-term plan (three months).

Critical	• Management attention needed. • Risk mitigation is required to lower the risk to an acceptable level. • Risk mitigation plan must be developed and implemented immediately (less than one month).

Table 9: Definition of Risk Rating

In an exemplary embodiment, the risk analysis is further explained in detail below:

a. **Test Scenario A:** Biometric fingerprint scanner for typical organisation usage (i.e. office) spoof using Latex fake fingerprint:
Assuming that this scenario has an enhanced basic attack potential, the probability of it to happen would be high as shown in Table 6. The severity calculation will be using CVSS method as it is assumed that the attack will only effect individual/ organisation as shown in Table 10 and Table 11. Finally, by using the matrix as shown in Table 12, the risk rate is determined and tabulated Table T.1.

Metric	Value	Comments
Attack Vector	Physical	The attacker requires physical access to the device
Attack Complexity	High	The attacking steps are simple but required specialized tools
Privileges Required	None	An attacker requires no privileges to mount an attack
User interaction	None	No other user interaction is required for this attack
Scope	Unchanged	The vulnerable and impacted components are the same
Confidentiality Impact	High	The attacker is identified/verified as the authorised user
Integrity Impact	None	The biometric fingerprint image still remains the same
Availability Impact	None	Other users are able to access the testing application with their own biometric fingerprint

Table 10: Comments for CVSS chosen CVSS metric values

Rating	CVSS Score
None	0.0

Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Table 11: CVSS Score Rating

		SEVERITY				
		None (Unlikely to impact individual or organization)	Low (May impact to individual or organisation)	Medium (Likely to result in a demonstrate impact to individual or organisation)	High (Likely to result in a significant impact to individual or organisation)	Critical (Poses an imminent threat to the lives of individual or organisation)
PROBABILITY	Very Low (Very unlikely to happen)	Low	Low	Low	Low	Medium
	Low (Unlikely to happen)	Low	Low	Medium	Medium	High
	Moderate (Likely to happen)	Low	Medium	Medium	High	Critical
	High (Very likely to happen)	Low	Medium	High	Critical	Critical
	Very High (Most likely to happen)	Medium	High	Critical	Critical	Critical

Table 12: Example of risk rating for enhance basic attack potential scenario

5

Scope of Testing		1. Spoofing an optical fingerprint sensor using fake fingerprint (Latex)				
No	Test	Details	Pro	Severity	Risk	Impact
1	A	Findings: The biometric device failed to detect the fake fingerprint during the verification process for existing data. The fake fingerprint used be latex.	High	Medium	High	Using this fake fingerprint, users can be successfully authenticated as genuine user.
Recommendation		Fake fingerprint detection functionality: • Increase the quality threshold and the minutia count in order to stringent the enrolment process. This helps to ensure fingerprints quality are high and filter out low quality fingerprints. • It is required that the fake fingerprint (liveness) detection functionality (i.e. algorithm, threshold) in the biometric to be enabled. • As new fake fingerprint technologies evolve and new spoofing mechanisms are developed, it is required that the fake fingerprint (liveness) detection functionality (i.e. algorithm, threshold) in the biometric device to be device to be regularly updated and re-evaluated.				
Developer's Response		For researcher/evaluator, kindly state the response by the developer whether he/she agrees or not and the mitigation plan.				

Table T.1: Summary of Test result for penetration testing biometric fingerprint scanner for typical organisation usage.

b. **Test scenario B** – Biometric fingerprint scanner for public health or safety, national security, economic security, foreign relations, civil liberates or public confidence (i.e. border control) spoofing using latex fake fingerprint:

Assuming that this scenario has a moderate attack potential, the probability of it to happen would be moderate as shown in the Table 6. The severity calculation will be using NCCIC incident scoring method as it is assumed that the attack will has an effect on national security as shown in Table 13. Finally, by using the matrix in Table 14, the risk rate is determined and tabulated in Table T.2.

Contributors	Score	Comments
Functional Impact	70	Significant impact to critical services due to border control concern on national security perspective.
Observed Activity	100	Effects are outcomes of a threat actor's actions on a victim's physical or virtual computer or information systems, networks and data stores
Location of Observed Activity	80	Critical System Management Activity was observed in high-level critical system management such as human-machine interfaces (HMIs) in industrial control systems
Actor Characterization	100	Targeted – Specific target systems such as industrial control environments
Information Impact	80	Core credential compromise
Recoverability	60	Extended – Time to recovery is unpredictable; additional resources and outside assistance may be required

Cross-Sector Dependency	75	Transportation Systems
Potential Impact	75	High – number of authorized users in the organization and size of customers base or population served

Table 13: List of contributors for NCISS Incident Score

		SEVERITY				
		Low (Unlikely to impact public health or safety, national security, foreign relations, civil libraries or public confidence)	Medium (May impact public health or safety, national security, foreign relations, civil libraries or public confidence)	High (Likely to result in a demonstrate impact to public health or safety, national security, foreign relations, civil libraries or public confidence)	Severe (Likely to result in a significant impact to public health or safety, national security, foreign relations, civil libraries or public confidence)	Emergency (Poses an imminent threat to the lives of impact public health or safety, national security, foreign relations, civil libraries or public confidence)
PROBABILITY	Very Low (Very unlikely to happen)	Low	Low	Low	Low	Medium
	Low (Unlikely to happen)	Low	Low	Medium	Medium	High
	Moderate (Likely to happen)	Low	Medium	Medium	High	Critical
	High (Very likely to happen)	Low	Medium	High	Critical	Critical
	Very High (Most likely to happen)	Medium	High	Critical	Critical	Critical

5

Table 14: Risk Matrix for TOE that impact public health or safety, national security, economic security, foreign relations, civil libraries or public confidence

Table T.2: Summary of test result for penetration testing biometric fingerprint scanner for public health or safety, national security, economic security, foreign relations, civil liberties or public confidence

Scope of Testing		1. Spoofing an optical fingerprint sensor using fake fingerprint (Latex)				
No	Test	Details	Pro	Severity	Risk	Impact
1	B	Findings: Through fingerprint spoofing performed by researcher/evaluator, the biometric device failed to detect the fake fingerprint during the verification process for existing data. The fake fingerprint used be latex.	Mod	High	High	Using this fake fingerprint, users can be successfully authenticated as genuine user.
Recommendation		Fake fingerprint detection functionality: • It is required that the fake fingerprint (liveness) detection functionality (i.e. algorithm, threshold) in the biometric device to be updated. • As new fake fingerprint technologies evolve and new spoofing mechanisms are developed, it is required that the fake fingerprint (liveness) detection functionality (i.e. algorithm, threshold) in the biometric device to be device to be regularly updated and re-evaluated.				
Developer's Response		For researcher/evaluator, kindly state the response by the developer whether he/she agrees or not and the mitigation plan.				

Table T.2: Summary of test result for penetration testing biometric fingerprint scanner for public health or safety, national security, economic security, foreign relations, civil liberties or public confidence.

The present disclosure includes as contained in the appended claims, as well as that of the foregoing description. Although this invention has been described in its preferred form with a degree of particularity, it is understood that the present disclosure of the preferred form has been made only by way of example and that numerous changes in the details of construction and the combination and arrangements of parts may be resorted to without departing from the scope of the invention.

CLAIMS

1. A method for determining a risk associated with a spoof attack, the method comprising the steps of:

retrieving, by a biometric data acquisition module (231), a first biometric data from a biometric device (210) accessed by an authorized user, whereby the first biometric data is a real biometric identification obtained from the authorized user; and

retrieving, by a biometric data acquisition module (231), a second biometric data from the biometric device (210) accessed by an unauthorized user using a fake biometric object, whereby the second biometric data is a fake biometric data obtained from the fake biometric object resembling the authorized user's real biometric identification,

characterized in that the method further comprising the steps:

computing, by a matching score computation module (233), a first matching score and a second matching score, by respectively comparing the first biometric data and the second biometric data against stored biometric identification data in a database (240);

computing, by a threshold computation module (234), a threshold value for differentiating the real biometric data and the fake biometric data, by comparing the first similarity score with the second similarity score; and

performing, by a risk analysis module (235), a risk analysis associated with the spoof attack which may be based on the identified fake biometric data.

2. The method according to claim 1, further comprising the step of analysing, by the risk analysis module (235), probability of potential spoof attack possible on the biometric device (210) based on pre-determined factors which includes time taken to identify and exploit, expertise required, knowledge on design of the biometric device, window of access opportunity required for the attack and equipment required for exploitation.

3. The method according to any one of preceding claims, further comprising the step of calculating, by the risk analysis module (235), severity of impact caused by the spoof attack in an organisation.

4. The method according to any one of preceding claims, wherein the risk rating of the spoof attack is determined based on the analysed probability and the calculated severity, by the risk analysis module (235).

5. The method according to any one of preceding claims, further comprising the step of configuring, by a benchmark module (236), the biometric device (210) with a benchmark matching score based on the determined threshold value, for mitigating the spoof attacks.

6. A system (200) for determining a risk associated with a spoof attack comprising:

a biometric device (210), configured to collect a first biometric data and a second biometric data from a user, whereby the first biometric data is a real biometric identification obtained from the authorized user and the second biometric data is a fake biometric data obtained an unauthorized user using a fake biometric object resembling the authorized user's biometric identification; and,

a computing device (220) installed with an application module (230) is connected to the biometric device (210) via a communication channel comprising:

a biometric data acquisition module (231), configured to retrieve the first biometric data and second biometric data from the biometric device (210),

characterised in that, the application module (230) further comprising:

a matching score computation module (233), configured to compute a first matching score and a second matching score, by comparing the first biometric data and the second biometric data with stored biometric identification data in a database (240), whereby the application module (230) is linked to the database (240) via the

communication channel;

a threshold computation module (234), configured to compute a threshold value for differentiating the real biometric data and the fake biometric data, by comparing the first similarity score with the second similarity score; and

a risk analysis module (235), configured to perform a risk analysis associated with the spoof attack based on the identified fake biometric data, for determining a risk rating of the spoof attack.

7. The system (200) according to claim 6, wherein the risk analysis module (235) is further configured to analyse a probability of potential spoof attack possible on the biometric device (210) based on pre-determined factors which includes time taken to identify and exploit, expertise required, knowledge on design of the biometric device, window of access opportunity required for the attack and equipment required for exploitation.

8. The system (200) according to any one of the claims 6 to 7, wherein the risk analysis module (235) is further configured to calculate severity of impact caused by the spoof attack in an organisation

9. The system (200) according to any one of the claims 6 to 8, wherein the risk analysis module (235) is further configured to determine the risk rating of the spoof attack, based on the analysed probability and the calculated severity.

10. The system (200) according to any one of the claims 6 to 9, wherein the application module (230) further comprising a benchmark module (236) configured to configure the biometric device (210) with a benchmark matching score based on the determined threshold value, for mitigating the spoof attacks.