Stochastic Biometric System Modelling with Rework Strategy

Mangey Ram*, Monika Manglik

Department of Mathematics
Graphic Era University, Dehradun, Uttarakhand-248002, India
Corresponding author: drmrswami@yahoo.com

Abstract
In this paper, the authors proposed the reliability mathematical modeling of a biometric system that computerizes the whole process of taking attendance and keeping its records in an academic institute. Manually taking attendance and sustaining it for a long time is very difficult as well as wastes a lot of time. For this cause, an efficient system has to be designed. This system takes attendance electronically with the help of a fingerprint scanner, and all the records are saved on a computer server. In order to mark the attendance, student or employee has to place his/her finger on the fingerprint sensor. On proof of identity student's or employee's record is well-run in the database, and he/she is reported through liquid-crystal display screens. Here, the authors evaluated reliability measures of the system such as availability, reliability, mean time to failure (MTTF), cost analysis and sensitivity analysis with the help of Laplace transformation, supplementary variable technique, and Markov technique.

Key words-biometric system, system modelling, availability, sensitivity analysis.

1. Introduction
Biometrics originates from the Greek word bios (life) and metricos (measure) (Schneier, 1999). It is basically a pattern-recognition system that is used to measure and analyze physiological and behavioral features. These features include fingerprints, voice patterns, hand geometry recognition, DNA (deoxyribonucleic acid) identification, gait recognition, signature verification, irises and others (Karray et al., 2007); all are used to identify human characteristics and to verify the identity. These biometrics or characteristics are strongly connected to an individual and cannot be forgotten, communed or simply hacked. These characteristics can uniquely identify a person. Biometrics give us another and higher security compared to password or pin identification. Biometric systems have been widely used for the purpose of recognition. These recognition methods refer to automatic recognition of people based on some definite physiological or behavioral features (Pankanti et al., 2002). There are many biometrics that can be used for some definite systems, but the basic configuration of a biometric system is always same.

Substantiation by biometric verification is becoming more and more mutual in commercial and public security systems, consumer electronics and point of sale applications. Biometric system deals a number of advantages over routine authentication methods (Weaver, 2006). Biometric statistics cannot be acquired by direct covert observation. It is impossible to share and difficult to make a replica. It improves user handiness by alleviating the need to remember long and casual passwords. It shields against denial by the user. Biometrics provide the same level of security for all users different passwords and is highly strong to brute force attacks. Furthermore, biometrics is one of the few methods that can be used for undesirable recognition where the system regulates whether the person is who he or she denies to be. Using biometrics through password-protected smart cards presents all three issues of authentication simultaneously (something you know, something you have and something you are) (Ambalakat, 2005).

Biometric time attendance systems are used to track each and every person coming to the destination is, in fact who one claims to be or not with its time and other detail. It uses finger and face recognition system to authenticate one's identity and record its time-in and time-out with the vital particulars.

For example, all educational institutes have certain measures for students and employees attendance. That is why keeping the correct attendance record is very important. At present, attendance is generally noted using paper sheets and old file system, this methodology is being used for a long time. It becomes very challenging to achieve and bring up-to-date the record frequently and manually analyze the percentage of attendance. Keeping the above facts in mind a system has designed to overcome the problems related to the attendance system (Navaz et al., 2009).

1.1 Structure of an Attendance Monitoring System
The attendance monitoring system generally consists of four modules like other biometric systems these are the basic modules of biometric (Ambalakat, 2005):

(*i*) *Enrollment Unit*
  The enrollment unit registers individual student or employee in the biometric system database. During this phase, a biometric reader scans the individual student's or employee's fingerprint to produce its digital representation.

(*ii*) *Feature Extraction Unit*
  This unit procedure the input sample to produce a compact representation called the template, which is then stored in a central database or a smart card issued to the single student or employee.

(*iii*) *Matching Unit*
  This unit compares the current input with the template. If the system performs identity verification, it compares the fingerprint to the student's or employee's master template and produces a score or match value (one to one matching).

(*iv*) *Decision Maker*
  This unit accepts or rejects the student or employee based upon a security threshold and matching score.

1.2 Attendance Monitoring System Performance
The performance evaluation of an attendance monitoring system be influenced by on two types of faults- matching errors and acquisition errors (Ambalakat, 2005). The matching errors consist of following:

(*i*) *False acceptance Rate (FAR)*
  ➢ Mistaking fingerprint measurements from two dissimilar students or employees to be from the same person.

(*ii*) *False rejection Rate (FRR)*
  ➢ Mistaking finger print measurements from the similar student or employee to be from two different persons.
  ➢ The acquisition errors consist of the following.

(*iii*) *Failure to Capture Rate (FTC)*
  ➢ Proportion of attempts for which an attendance monitoring system is important to capture a sample of finger print of adequate quality.

(*iv*) *Failure to Enroll Rate (FTE)*
> ➢ Proportion of the student or employee population for which the attendance monitoring system is unable to generate reference templates of sufficient quality.
> ➢ This contains those who, for physical or behavioral reasons like skin problems, are unable to present the finger print.

The entire system is used to compute the accuracy and performance of an attendance monitoring system. Lots of related work exists in the application of different approaches and principles (Shoewu and Idowu, 2012). To effectively monitor the attendance of students or employees, an embedded computer-based lecture attendance management system was proposed by Shoewu and Lawson (2011). A wireless attendance management system that validates using the iris of the individual is used by Kadry and Smaili (2013). Attendance management has also been carried out using attendance software that uses the password for authentication. A system designed and implemented by Cheng et al. (2005) that authenticates the user based on password, this kind of system allows for impression since the password can be shared or tampered with. The password could also be forgotten at times thereby preventing the user from accessing the system. An efficient automatic attendance system using a finger print verification technique has been developed by Saraswat and Kumar (2010).

Other attendance solutions are radio-frequency identification technology: Development (RFID) - based student attendance system (Shoewu and Badejo, 2006) and Global System for Mobile communications (GSM) - General Packet Radio Service (GPRS) based student attendance system. These all are device based solutions. GSM-GPRS based systems use position of class for attendance marking, which is not dynamic as if schedule or location of the class changes; wrong attendance might be marked. Similarly, in RFID-based systems, students or employees have to carry RFID cards and also the RFID detectors are needed to be installed (Saraswat and Kumar, 2010). On the basis of previous study, we analyzed that many biometric systems have been developed for monitoring the attendance of students by using finger print verification techniques but no one analyzed reliability measures of the system such as availability, reliability, mean time to failure (MTTF) etc., which are the important aspects of any biometric system.

Observance the above facts in mind in the present paper, we have analyzed an attendance monitoring system for students or employees by using fingerprint recognition technique (Maltoni et al. (2009). A mathematical model for the above stated system has been developed and the reliability measures such as availability, reliability, mean time to failure (MTTF), cost analysis and sensitivity analysis are also evaluated by using Laplace transformation, supplementary variable technique and Markov technique. Although a remarkable work has been done by the various authors (Ram et al., 2008, 2010, 2013; Shoewu and Lawson, 2011; Park and Pham, 2010; Verma et al., 2010) but they did not analyze a biometric system under reliability context.

In this model, we have taken hardware equipment (finger print scanner), *n* nodes in the series, a switch which is connected to all of the nodes, and these all are connected with the server. The above stated system can completely be failing due to deliberate failure, catastrophic failure, switch failure and failure of all nodes connected in series. We also assumed that the system goes to the degraded state due to partial failure within the system. The general system configuration and working flowchart of a biometric system has been shown in Fig. 1(a) and (b) respectively. The transition diagram of the system has been shown in Fig. 1(c).
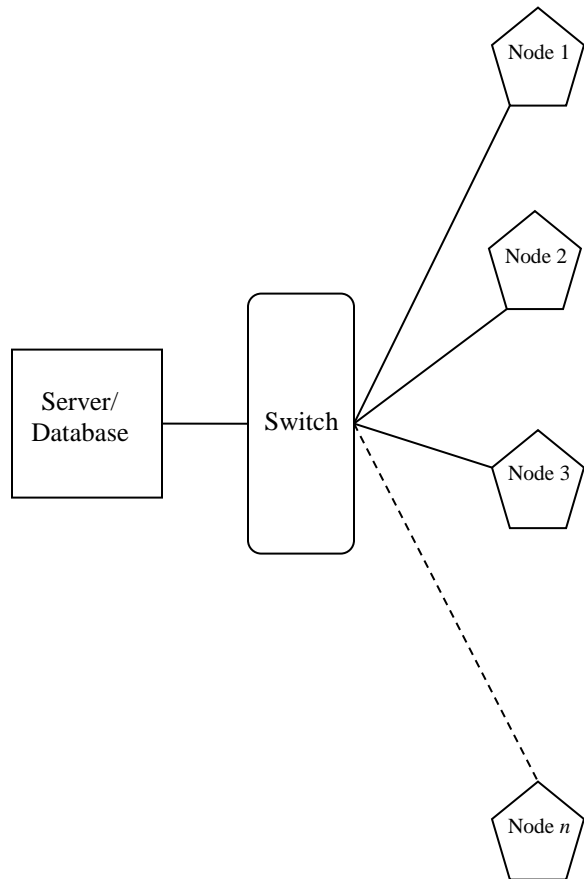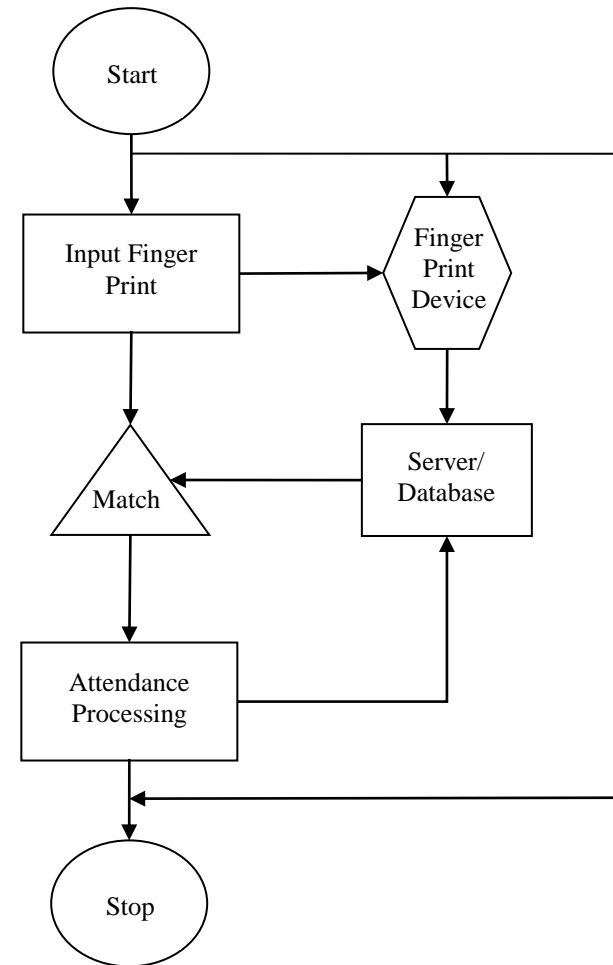
Fig. 1(a). System architecture

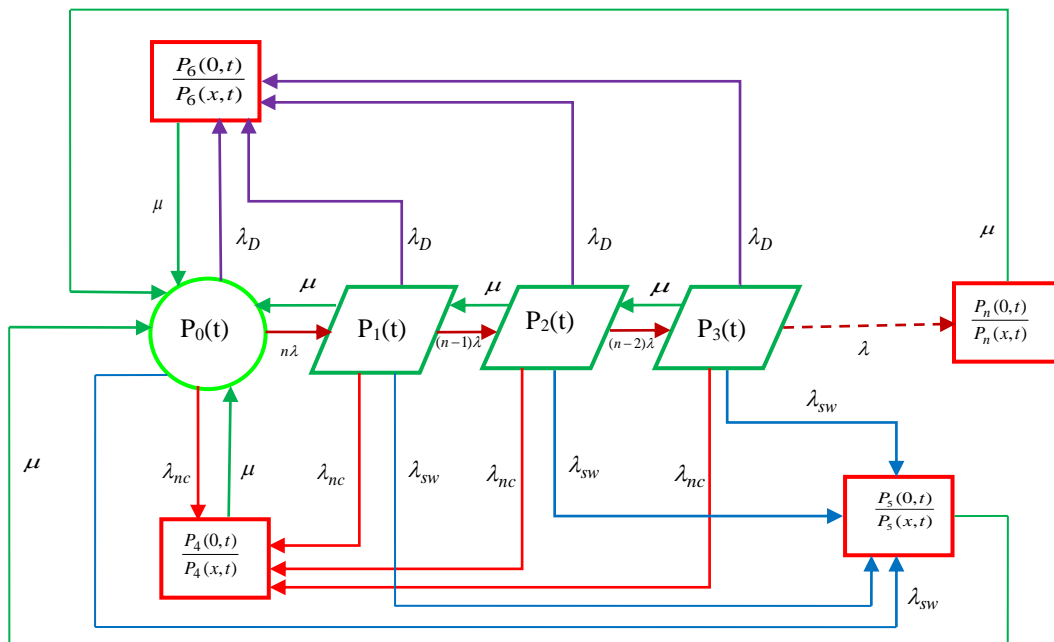Fig. 1(b). Flow chart of a biometric system

Fig. 1(c). State transition diagram of the biometric system

2. State Description

The following system states have been designed in the current model:

- S_0 The system is in the good working condition.
- S_1 The system is in the degraded state due to partial failure.
- S_2 The system is in the degraded state due to partial failure.
- S_3 The system is in the degraded state due to partial failure.
- S_4 The system is in the failed due to catastrophic failure.
- S_5 The system is in the failed state due to switch failure.
- S_6 The system is in the failed state due to deliberate failure.
- S_n The system is in the failed state due to failure of n nodes connected in series.

3. Assumptions and Notations

The following assumptions have been through for the design model:

- (i)   Initially, the system is in the good state.
- (ii)   The system has three states namely good, degraded, and failed.
- (iii)   In case of complete failure which can occur due to failure of the total number of nodes connected in parallel, catastrophic failure, switch failure, deliberate failure
- (iv)   All failure and repair rates are constant.
- (v)   System can be repair, when it is in completely failed mode.
- (vi)   The repaired system works like a new one.

The following notations are related to this model:

- t Time scale.
- s **Laplace transform variable.**

$\lambda, \lambda_D, \lambda_{nc}, \lambda_{sw}$	Unit failure, deliberate failure, catastrophic failure (n nodes) and switch failure rate respectively.
μ	Repair rates from all types of failures respectively.
$P_i(t)$	Transition state probabilities from state S_0 to S_7, where i=0, 1, 2, 3….., 4, 5, 6, n.
$P_j(x,t)$	The probability density function that the system is in the completely failed state S_j, at epoch t and has an elapsed repair time of x, where j=4, 5, 6, n.
n	Total number of nodes connected.
$E_p(t)$	Expected profit during up time.
K_1, K_2	Revenue and service cost per unit time.

4. Formulation and Solution of the Mathematical Model

By the probability of the considerations and continuity arguments, we can obtain the following set of differential equations governing the present mathematical model.

$$\left[\frac{\partial}{\partial t} + n\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}\right]P_0(t) = \mu(x)P_1(t) + \mu_2 P_6(t) + \int_0^\infty \mu(x)P_4(t)dx + \int_0^\infty \mu(x)P_5(t)dx$$

$$+ \int_0^\infty \mu(x)P_6(t)dx + \int_0^\infty \mu(x)P_n(t)dx \tag{1}$$

$$\left[\frac{\partial}{\partial t} + (n-1)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw} + \mu(x)\right]P_1(t) = n\lambda P_2(t) + \mu_3 P_0(t) + \mu(x)P_2(t) \tag{2}$$

$$\left[\frac{\partial}{\partial t} + (n-2)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw} + \mu(x)\right]P_2(t) = (n-1)\lambda P_1(t) + \mu(x)P_3(t) \tag{3}$$

$$\left[\frac{\partial}{\partial t} + \lambda + \lambda_D + \lambda_{nc} + \lambda_{sw} + \mu(x)\right]P_3(t) = (n-2)\lambda P_2(t) \tag{4}$$

$$\left[\frac{\partial}{\partial t} + \frac{\partial}{\partial x} + \mu(x)\right]P_4(t) = 0 \tag{5}$$

$$\left[\frac{\partial}{\partial t} + \frac{\partial}{\partial x} + \mu(x)\right]P_5(t) = 0 \tag{6}$$

$$\left[\frac{\partial}{\partial t} + \frac{\partial}{\partial x} + \mu(x)\right]P_6(t) = 0 \tag{7}$$

$$\left[\frac{\partial}{\partial t} + \frac{\partial}{\partial x} + \mu(x)\right]P_7(t) = 0 \tag{8}$$

Boundary conditions

$$P_4(0,t) = \lambda_{nc}[(P_0(t) + P_1(t) + P_2(t) + P_3(t)] \tag{9}$$

$$P_5(0,t) = \lambda_{sw}[P_0(t) + P_1(t) + P_2(t) + P_3(t)] \tag{10}$$

$$P_6(0,t) = \lambda_D[P_0(t) + P_1(t) + P_2(t) + P_3(t)] \tag{11}$$

$$P_n(0,t) = \lambda P_3(t) \tag{12}$$

Initial condition

$$P_i(t) = \left\{ \begin{matrix} 1 & \text{when } t=0 \\ 0 & \text{when } t>0 \end{matrix} \right. \tag{13}$$

Taking Laplace transformation of the Equations (1-12), we get

$$[s+n\lambda+\lambda_D+\lambda_{nc}+\lambda_{sw}]\overline{P}_0(s) = \mu(x)\overline{P}_1(s)+\mu_2\overline{P}_6(s)+\int_0^\infty \mu(x)\overline{P}_4(s)dx+\int_0^\infty \mu(x)\overline{P}_5(s)dx$$

$$+\int_0^\infty \mu(x)\overline{P}_6(s)dx+\int_0^\infty \mu(x)\overline{P}_n(s)dx \tag{14}$$

$$[s+(n-1)\lambda+\lambda_D+\lambda_{nc}+\lambda_{sw}+\mu(x)]\overline{P}_1(s) = n\lambda\overline{P}_2(s)+\mu_3\overline{P}_0(s)+\mu(x)\overline{P}_2(s) \tag{15}$$

$$[s+(n-2)\lambda+\lambda_D+\lambda_{nc}+\lambda_{sw}+\mu(x)]\overline{P}_2(s) = (n-1)\lambda\overline{P}_1(s)+\mu(x)\overline{P}_3(s) \tag{16}$$

$$[s+\lambda+\lambda_D+\lambda_{nc}+\lambda_{sw}+\mu(x)]\overline{P}_3(s) = (n-2)\lambda\overline{P}_2(s) \tag{17}$$

$$\left[s+\frac{\partial}{\partial x}+\mu(x)\right]\overline{P}_4(s) = 0 \tag{18}$$

$$\left[s+\frac{\partial}{\partial x}+\mu(x)\right]\overline{P}_5(s) = 0 \tag{19}$$

$$\left[s+\frac{\partial}{\partial x}+\mu(x)\right]\overline{P}_6(s) = 0 \tag{20}$$

$$\left[s+\frac{\partial}{\partial x}+\mu(x)\right]\overline{P}_n(s) = 0 \tag{21}$$

$$\overline{P}_4(0,s) = \lambda_{nc}[\overline{P}_0(s)+\overline{P}_1(s)+\overline{P}_2(s)+\overline{P}_3(s)] \tag{22}$$

$$\overline{P}_5(0,s) = \lambda_{sw}[(\overline{P}_0(s)+\overline{P}_1(s)+\overline{P}_2(s)+\overline{P}_3(s)] \tag{23}$$

$$\overline{P}_6(0,s) = \lambda_D(\overline{P}_0(s)+\overline{P}_1(s)+\overline{P}_2(s)+\overline{P}_3(s)) \tag{24}$$

$$\overline{P}_n(0,s) = \lambda\overline{P}_3(s) \tag{25}$$

Solving (14-21) with the help of (22-25) and (13), one may get various state probabilities.

$$\overline{P}_0(s) = \frac{1}{G} \tag{26}$$

$$\overline{P}_1(s) = \left[\frac{n\lambda}{(s+d_1)}-\frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right]\overline{P}_0(s) \tag{27}$$

$$\overline{P}_2(s) = \left[\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda}\right]\left[\frac{n\lambda}{(s+d_1)}-\frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right]\overline{P}_0(s) \tag{28}$$

$$\overline{P_3}(s) = \left[\frac{(n-2)\lambda}{(s+d_3)}\right]\left[\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda}\right]\left[\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right]\overline{P_0}(s)$$

(29)

$$\overline{P_4}(s) = \lambda_{nc}\left(\frac{1-\overline{S_\mu}(s)}{s}\right)\left[1 + \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)\right.$$
$$+ \left(\frac{\mu(x)(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda}\right)\left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)$$
$$+ \left(\frac{(n-2)\lambda}{(s+d_3)}\right)\left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda}\right)\left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)\right]$$

(30)

$$\overline{P_5}(s) = \lambda_{sw}\left(\frac{1-\overline{S_\mu}(s)}{s}\right)\left[1 + \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)\right.$$
$$+ \left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda}\right)\left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)$$
$$+ \left(\frac{(n-2)\lambda}{(s+d_3)}\right)\left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda}\right)\left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)\right]\overline{P_0}(s)$$

(31)

$$\overline{P_6}(s) = \lambda_D\left(\frac{1-\overline{S_\mu}(s)}{s}\right)\left[1 + \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)\right.$$
$$+ \left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda}\right)\left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)$$
$$+ \left(\frac{(n-2)\lambda}{(s+d_3)}\right)\left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda}\right)\left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)\right]$$

(32)

$$\overline{P_n}(s) = \lambda\left(\frac{1-\overline{S_\mu}(s)}{s}\right)\left[\left(\frac{(n-2)\lambda}{(s+d_3)}\right)\left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda}\right)\right.$$
$$\times \left.\left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3)-\mu(x)(n-2)\lambda\}}\right)\right]\overline{P_0}(s)$$

(33)

Where

$$d = n\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}, \ d_1 = (n-1)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw} + \mu(x),$$
$$d_2 = (n-2)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw} + \mu(x), \ d_3 = \lambda + \lambda_D + \lambda_{nc} + \lambda_{sw} + \mu(x),$$
$$\overline{S_\mu}(s) = \int_0^\infty \mu(x)\exp\left\{-sx - \int_0^x \mu(x)dx\right\}dx$$

$$F = 1 + \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda\}} \right)$$

$$+ \left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda} \right) \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda\}} \right)$$

$$+ \left(\frac{(n-2)\lambda}{(s+d_3)} \right) \left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda} \right) \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda\}} \right)$$

$$G = (s+d) - \mu(x) \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda\}} \right) - F\overline{S}_\mu(s)\{\lambda_{nc} + \lambda_{sw} + \lambda_D\}$$

$$- \lambda \left(\frac{(n-2)\lambda}{(s+d_3)} \right) \left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda} \right) \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda\}} \right)$$

The Laplace transformations of the probabilities that the system is in the up (either good or degraded state) and down (failed) state at any time are as follows:

$$\overline{P}_{up}(s) = \overline{P}_0(s) + \overline{P}_1(s) + \overline{P}_2(s) + \overline{P}_3(s)$$

$$= \left[1 + \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda\}} \right) \right.$$

$$+ \left(\frac{(n-1)\lambda(s+d_3)}{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda} \right) \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda\}} \right)$$

$$+ \left. \left(\frac{(n-1)(n-2)\lambda^2}{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda} \right) \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda\}} \right) \right] \overline{P}_0(s)$$

(34)

$$\overline{P}_{down}(s) = \overline{P}_4(s) + \overline{P}_5(s) + \overline{P}_6(s) + \overline{P}_7(s)$$

$$= \left(\frac{1 - \overline{S}_\mu(s)}{s} \right) \left[(\lambda_{nc} + \lambda_{sw} + \lambda_D)F \right.$$

$$+ \left. \left(\frac{(n-1)(n-2)\lambda^2}{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda} \right) \left(\frac{n\lambda}{(s+d_1)} - \frac{\mu(x)(n-1)\lambda(s+d_3)}{\{(s+d_2)(s+d_3) - \mu(x)(n-2)\lambda\}} \right) \right] \overline{P}_0(s)$$

(35)

5. Particular Cases
5.1 Availability Analysis
Taking and substituting the values of different parameters as $\lambda = 0.010, \lambda_D = 0.020, \lambda_{nc} = 0.030, \lambda_{sw} = 0.040, \mu = 1, n = 10$ in Equation (34) and then taking the inverse Laplace transform, we get

$$P_{up}(t) = 0.00003130566920 e^{-1.594209327\,t} + 0.0007360983537 e^{-1.184703955\,t}$$
$$+ 0.081806229956 e^{-1.089526493\,t} + 0.00006194556732 e^{-0.7715602242\,t} + 0.9174270322 \quad (36)$$

Varying the time scale t from 0 to 15 in Equation (36), we obtain Table 1 and correspondingly Fig. 2, representing the behavior of availability of the biometric system with respect to time.

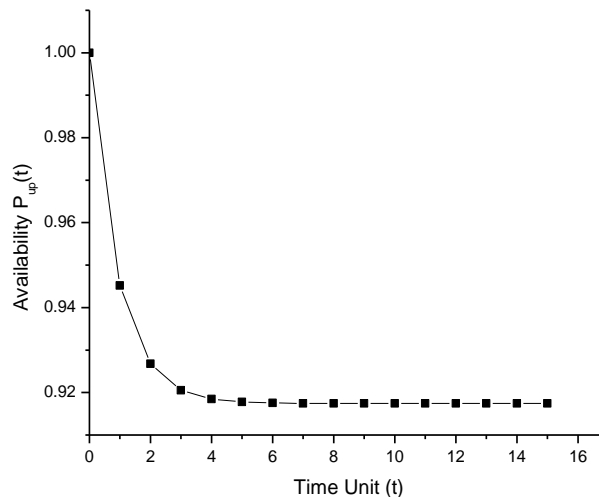| Time (t)	$P_{up}(t)$
0	1.00000
1	0.94519
2	0.92676
3	0.92056
4	0.91848
5	0.91778
6	0.91754
7	0.91746
8	0.91744
9	0.91743
10	0.91742
11	0.91742
12	0.91742
13	0.91742
14	0.91742
15	0.91742

Table 1. Availability vs. time unit

Fig. 2. Availability vs. time unit

5.2 Reliability Analysis
For reliability, taking all repairs rates zero in (34), the reliability expression of the system as:

$$R(s) = \left(\frac{1}{\lambda n + \lambda_D + \lambda_{nc} + \lambda_{sw}} \right)$$
$$\times \left(1 + \frac{n\lambda}{s + (n-1)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}} + \frac{n(n-1)\lambda^2}{\left(s + (n-2)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}\right)\left(s + (n-1)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}\right)} \right.$$

$$+\frac{n\lambda^3(n-1)(n-2)}{\left(s+\lambda+\lambda_D+\lambda_{nc}+\lambda_{sw}\right)\left(s+(n-2)\lambda+\lambda_D+\lambda_{nc}+\lambda_{sw}\right)\left(s+(n-1)\lambda+\lambda_D+\lambda_{nc}+\lambda_{sw}\right)}\right) \quad (37)$$

Taking the inverse Laplace of Equation (37), we get

$$R(t)=\frac{-(n-2)e^{-(n\lambda+\lambda_D+\lambda_{nc}+\lambda_{sw})t}}{2}$$
$$+\frac{1}{2(n-3)}\left\{n\left(2e^{-(\lambda+\lambda_D+\lambda_{nc}+\lambda_{sw})t}+2e^{-(n\lambda+\lambda-\lambda_D-\lambda_{nc}-\lambda_{sw})t}(n-3)-e^{-(n\lambda+2\lambda-\lambda_D-\lambda_{nc}-\lambda_{sw})t}\right)\right\} \quad (37a)$$

Let us fix and putting the failure rates as $\lambda=0.010, \lambda_D=0.020, \lambda_{nc}=0.030, \lambda_{sw}=0.040, n=10$ in Equation (37a) and setting time unit t=0 to 15, one can obtain Table 2 and Fig. 3, which represents how reliability varies as the time increases.

Time (t)	Reliability $R(t)$
0	1.00000
1	0.91393
2	0.83526
3	0.76336
4	0.69763
5	0.63753
6	0.58258
7	0.53233
8	0.48636
9	0.44432
10	0.40586
11	0.37067
12	0.33849
13	0.30904
14	0.28211
15	0.25748

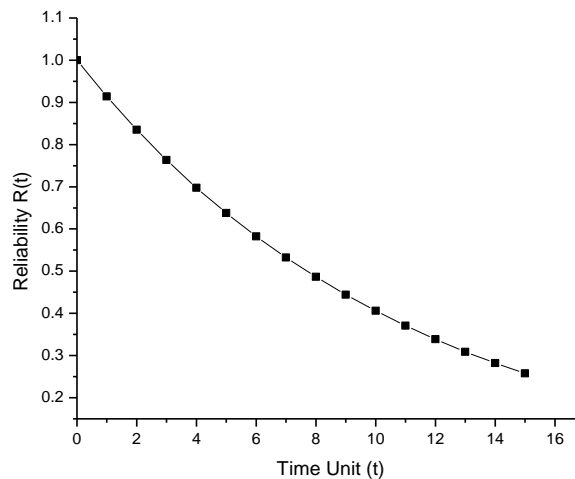Table 2. Reliability vs. time unit

Fig. 3. Reliability vs. time unit

5.3 Expected Profit

Let the service facility be always available, then expected profit during the interval (0, t] is given by

$$E_p(t) = K_1 \int_0^t P_{up}(t)dt - tK_2 \tag{38}$$

Using Equation (36), the expected profit for the same set of parameters is given by (38). Setting $K_1 = 1$, $K_2 = 0.1, 0.2, 0.3, 0.4, 0.5$, and $t = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$; one may get Table 3 and Fig. 4.

Time	Expected Profits				
(t)	$K_2= 0.1$	$K_2=0.2$	$K_2=0.3$	$K_2=0.4$	$K_2=0.5$
0	0	0	0	0	0
1	0.86771	0.76771	0.66771	0.56771	0.46771
2	1.70205	1.50205	1.30205	1.10205	0.90205
3	2.52516	2.22516	1.92516	1.62516	1.32516
4	3.34450	2.94450	2.54450	2.14450	1.74450
5	4.16257	3.66257	3.16257	2.66257	2.16257
6	4.98021	4.38021	3.78021	3.18021	2.58021
7	5.79771	5.09771	4.39771	3.69771	2.99771
8	6.61516	5.81516	5.01516	4.21516	3.41516
9	7.43260	6.53260	5.63260	4.73260	3.83260

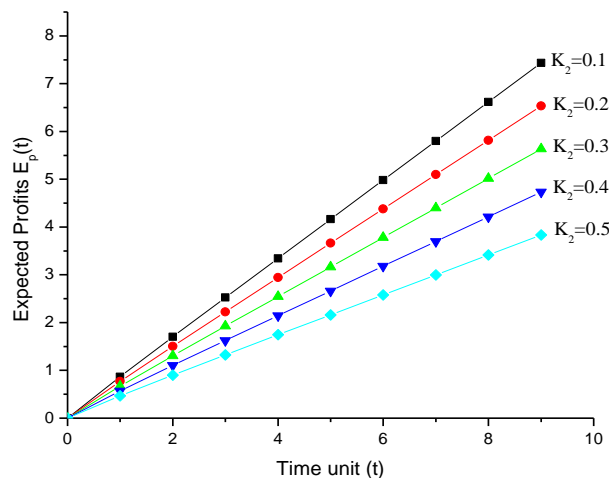Table 3. Expected profit as function of failure rates

Fig. 4. Expected profit as function of failure rates

5.4 Mean Time to Failure (MTTF) Analysis

Taking all repairs to zero Equation (34) as s tends to zero, one can obtain the MTTF as:

$$MTTF = \left(\frac{1}{\lambda n + \lambda_D + \lambda_{nc} + \lambda_{sw}} \right) \left(1 + \frac{n\lambda}{(n-1)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}} + \frac{n\lambda^2(n-1)}{\left((n-2)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}\right)\left((n-1)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}\right)} \right.$$
$$\left. + \frac{n\lambda^3(n-1)(n-2)}{\left(\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}\right)\left((n-2)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}\right)\left((n-1)\lambda + \lambda_D + \lambda_{nc} + \lambda_{sw}\right)} \right) \tag{39}$$

Setting $\lambda = 0.010, \lambda_D = 0.020, \lambda_{nc} = 0.030, \lambda_{sw} = 0.040, n = 10$ and varying $\lambda, \lambda_D, \lambda_{nc}, \lambda_{sw}$ one by one respectively as 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9 in Equation (39), one may obtain the variation of MTTF with respect to failure rates as shown in Table 4 and Fig. 5.

| Variation in Failure rates $\lambda, \lambda_D, \lambda_{nc}, \lambda_{sw}$	MTTF			
	λ	λ_D	λ_{nc}	λ_{sw}
0.1	6.72696	5.86894	6.23303	6.64492
0.2	4.49934	3.70166	3.84375	3.99717
0.3	3.37097	2.70217	2.77718	2.85647
0.4	2.69351	2.12747	2.17371	2.22200
0.5	2.24232	1.75431	1.78563	1.81809
0.6	1.92043	1.49250	1.51511	1.53842
0.7	1.67928	1.29868	1.31576	1.33331
0.8	1.49190	1.14941	1.16277	1.17645
0.9	1.34212	1.03092	1.04165	1.05262

Table 4. MTTF as a function of failure rates
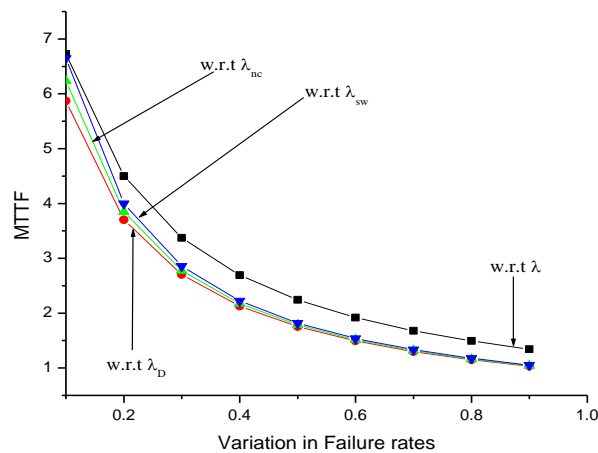
Fig. 5. MTTF as a function of failure rates

5.5 Sensitivity Analysis
The sensitivity of the reliability by a fastidious input factor is most regularly defined as the partial derivative of the reliability with respect to that factor. This measure is then used to estimate the outcome of factor changes with the model result without necessitating a full model solution for each factor change (Henley and Kumamoto, 1992; Andrews and Moss, 1993). These input factors are such as, failure rates and component type. Similarly, we can define sensitivity of MTTF w. r. t input factor.

(*i*) *Sensitivity of Reliability*
We first perform a sensitivity analysis for changes in *R*(*t*) resulting from changes in system parameters $\lambda, \lambda_D, \lambda_{nc}, \lambda_{sw}$ and by differentiating (37) with respect to failure rates $\lambda, \lambda_D, \lambda_{nc}, \lambda_{sw}$ respectively we get the values of $\dfrac{\partial R(t)}{\partial \lambda}, \dfrac{\partial R(t)}{\partial \lambda_D}, \dfrac{\partial R(t)}{\partial \lambda_{nc}}, \dfrac{\partial R(t)}{\partial \lambda_{sw}}$ now by

setting $\lambda = 0.010, \lambda_D = 0.020, \lambda_{nc} = 0.030, \lambda_{sw} = 0.040$, n=10 taking t=0 to 15 one may obtain Table 5 and Fig. 6.

Time (t)	$\dfrac{\partial R(t)}{\partial \lambda}$	$\dfrac{\partial R(t)}{\partial \lambda_D}$	$\dfrac{\partial R(t)}{\partial \lambda_{nc}}$	$\dfrac{\partial R(t)}{\partial \lambda_{sw}}$
0	0	0	0	0
1	-0.00010	-0.91393	-0.91393	-0.91393
2	-0.00139	-1.67053	-1.67053	-1.67053
3	-0.00602	-2.29009	-2.29009	-2.29009
4	-0.01623	-2.79053	-2.79053	-2.79053
5	-0.03380	-3.18768	-3.18768	-3.18768
6	-0.05982	-3.49551	-3.49551	-3.49551
7	-0.09460	-3.72631	-3.72631	-3.72631
8	-0.13779	-3.89093	-3.89093	-3.89093
9	-0.18850	-3.99890	-3.99890	-3.99890
10	-0.24544	-4.05863	-4.05863	-4.05863
11	-0.30707	-4.07746	-4.07746	-4.07746
12	-0.37175	-4.06191	-4.06191	-4.06191
13	-0.43779	-4.01764	-4.01764	-4.01764
14	-0.50362	-3.94963	-3.94963	-3.94963
15	-0.56778	-3.86222	-3.86222	-3.86222

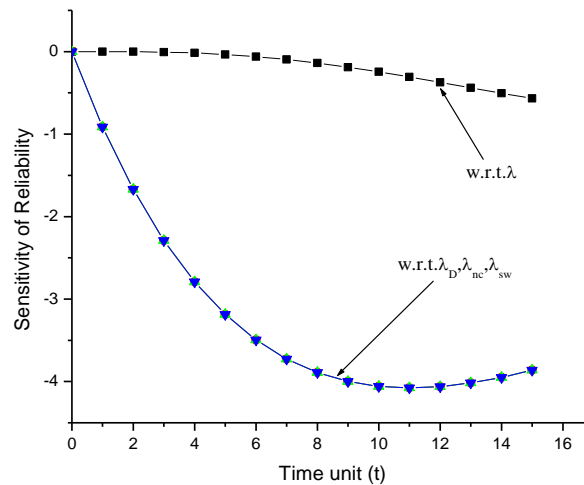Table 5. Sensitivity of reliability as function of time

Fig. 6. Sensitivity of reliability as function of time

(*ii*) *Sensitivity of MTTF*
Sensitivity analysis for changes in MTTF resulting from changes with the system parameters $\lambda, \lambda_D, \lambda_{nc}, \lambda_{sw}$. By differentiating (39) with respect to failure rates $\lambda, \lambda_D, \lambda_{nc}, \lambda_{sw}$ respectively,

we get the values of $\dfrac{\partial MTTF}{\partial \lambda}, \dfrac{\partial MTTF}{\partial \lambda_D}, \dfrac{\partial MTTF}{\partial \lambda_{nc}}, \dfrac{\partial MTTF}{\partial \lambda_{sw}}$.

Setting $\lambda = 0.010, \lambda_D = 0.020, \lambda_{nc} = 0.030, \lambda_{sw} = 0.040$, n=10 and varying $\lambda, \lambda_D, \lambda_{nc}, \lambda_{sw}$ one by one respectively as 0.1 to 0.9, one may obtain Table 6 and Fig. 7.

Variation in failure rates $\lambda, \lambda_D, \lambda_{nc}, \lambda_{sw}$	$\dfrac{\partial MTTF}{\partial \lambda}$	$\dfrac{\partial MTTF}{\partial \lambda_D}$	$\dfrac{\partial MTTF}{\partial \lambda_{nc}}$	$\dfrac{\partial MTTF}{\partial \lambda_{sw}}$
0.10	-32.80591	-34.29387	-38.65279	-43.89159
0.20	-15.01797	-13.68552	-14.75429	-15.95296
0.30	-8.47023	-7.29836	-7.70883	-8.15490
0.40	-5.41723	-4.52519	-4.72394	-4.93607
0.50	-3.75747	-3.07726	-3.18810	-3.30504
0.60	-2.75737	-2.22741	-2.29541	-2.36656
0.70	-2.10895	-1.68651	-1.73117	-1.77764
0.80	-1.66486	-1.32112	-1.35202	-1.38401
0.90	-1.34752	-1.06278	-1.08503	-1.10799

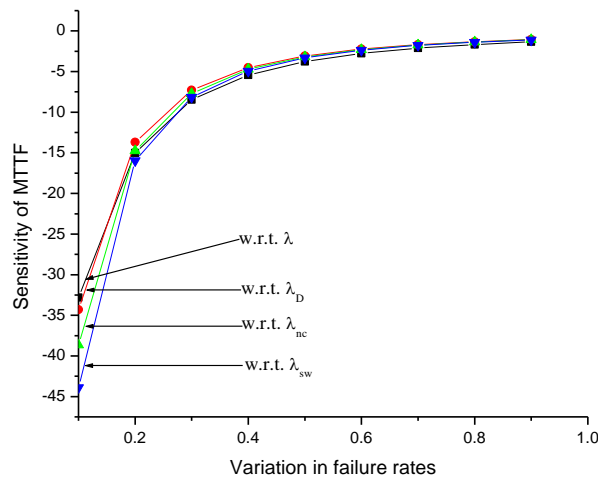Table 6. Sensitivity of MTTF as function of failure rates

Fig. 7. Sensitivity of MTTF as function of failure rates

6. Results Discussion and Conclusion

In this paper, an attendance monitoring (biometric) system using finger print verification techniques and four types of failures has been considered and reliability measures such as availability, reliability, MTTF, cost analysis and sensitivity analysis have been evaluated.

Availability is the probability that the system is operating satisfactorily at any time it refers to the system survival for the repairable system. The present study revealed that the availability of the biometric system decreases as the time increases and being constant after a certain value of time as shown in Fig. 2.

The probability of the system being in upstate is characterized by the reliability. It refers to the system survival before the first failure. The variation of reliability with respect to time has shown in Fig. 3. From the figure, one can easily observe that the reliability of the biometric system decreases as the time increases. For the safe operation and assure the quality of the components of the system in the sense that they perform their work perfectly, a repairable system should be highly reliable.

Reliability and cost are competing constraints in all manufactured systems. Reliability is essential for achieving a desired level of customer satisfaction. On the other hand, cost control is critical to maintain product reliability. Clearly, reliability alone will not guarantee product viability. Similarly, arbitrary cost cutting can be detrimental to profit when the relating system reliabilities too low. Thus, a comparison between these two factors is necessary to optimize profitability. Fig. 4 represents the graph of the cost function versus time. In this figure, we plotted a cost function for different values of cost K_1 and K_2. From the graph, one can easily observe that increasing service cost leads decrement into expected profit.

MTTF refers the expected time of failure during the operation. Variation of MTTF with respect to failure rates has shown in Fig. 5. From the graph, we observe that MTTF of the system decreases with respect to all failure rates that is the time span of failures decreases with increment in failure rates.

The sensitivities of the system reliability with respect to $\lambda, \lambda_D, \lambda_{nc}$ and λ_{sw} are shown in Fig. 6. It reveals that the sensitivity of the system decreases with respect to λ and remains constant with respect to $\lambda_D, \lambda_{nc}, \lambda_{sw}$. Also from the graph, one may easily obtain that system reliability is more sensitive w. r. t. λ. Fig .7 also indicates the sensitivity of MTTF with respect to $\lambda, \lambda_D, \lambda_{nc}$ and λ_{sw}, which clear further that it increases with increment in $\lambda, \lambda_D, \lambda_{nc}$ and λ_{sw}. Critical observation of the graph pointed out that MTTF of the system is more sensitive with respect to λ. From the sensitivity analysis, we can conclude that the system can be made less sensitive by controlling its failure rates.

Finally, we concluded upon the basis of the above discussion that a reliable, secure, fast and an efficient biometric system has been developed in place of a manual and unreliable system and we may also predict availability, reliability, failure time and sensitivity of the system. Results have shown that implementation of this biometric system reduce amount of work and time of the administration in an academic institute or any organization.

References

Ambalakat, P. (2005). Security of biometric authentication systems. *21st Computer Science Seminar*.

Andrews, J. D., & Moss, T. R. (1993). *Reliability and risk assessment*. Longman Scientific & Technical.

Cheng, K., Xiang, L., Hirota, T., & Ushijima, K. (2005). Effective teaching for large classes with rental PCs by web system WTS. In *Proc. Data Engineering Workshop* (Vol. 2005).

Henley, E. J. & Kumamoto H. (1992). *Probabilistic Risk Assessment*: IEEE Press.

Kadry, S., & Smaili, M. (2013). Wireless attendance management system based on iris recognition. *Scientific Research and Essays*, *5*(12), 1428-1435.

Karray, F., Saleh, J. A., Arab, M. N. and Alemzadeh, M. (2007). *Multi Modal Biometric Systems: A State of Art Survey*. Pattern Analysis and Machine Intelligence Laboratory, University of Waterloo, Waterloo Canada.

Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media.

Navaz, T., Pervaiz, S., Korrani, A.K. and Azhar-Ud-Din (2009). Development of Academic Attendance Monitoring System Using Fingerprint Identification. *International Journal of Computer Science and Network Security*, *9*(5), 164-168.

Pankanti, S., Prabhakar, S., & Jain, A. K. (2002). On the individuality of fingerprints. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *24*(8), 1010-1025.

Park, M., & Pham, H. (2010). Warranty cost analyses using quasi-renewal processes for multicomponent systems. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, *40*(6), 1329-1340.

Ram, M. (2010). Reliability measures of a three-state complex system: a copula approach. *Applications and Applied Mathematics: An International Journal*, *5*(10), 1483-1492.

Ram, M., & Singh, S. B. (2008). Availability and cost analysis of a parallel redundant complex system with two types of failure under preemptive-resume repair discipline using Gumbel-Hougaard family copula in repair. *International Journal of Reliability, Quality and Safety Engineering*, *15*(04), 341-365.

Ram, M., & Singh, S. B. (2010). Analysis of a complex system with common cause failure and two types of repair facilities with different distributions in failure. *International Journal of Reliability and Safety*, *4*(4), 381-392.

Ram, M., & Singh, S. B. (2010). Availability, MTTF and cost analysis of complex system under preemptive-repeat repair discipline using Gumbel-Hougaard family copula. *International Journal of Quality & Reliability Management*, *27*(5), 576-595.

Ram, M., Singh, S. B., & Singh, V. V. (2013). Stochastic analysis of a standby system with waiting repair strategy. *Systems, Man, and Cybernetics: Systems, IEEE Transactions on*, *43*(3), 698-707.

Saraswat, C., & Kumar, A. (2010). An efficient automatic attendance system using fingerprint verification technique. *International Journal on Computer Science and Engineering*, *2*(02), 264-269.

Schneier, B. (1999). Biometrics: uses and abuses. *Communications of the ACM*, *42*(8), 58.

Shoewu, O. S. O., & Lawson, A. L. A. (2011). Embedded Computer-Based Lecture Attendance Based Lecture Attendance Management System Management System. *African Journal of Computing & ICT September*, *4*(3), 27-36.

Shoewu, O., & Badejo, O. (2006). Radio frequency identification technology: development, application, and security issues. *The Pacific Journal of Science and Technology*, *7*(2), 144-15.

Shoewu, O., & Idowu, O. A. (2012). Development of attendance management system using biometrics. *The Pacific Journal of Science and Technology*, *13*(1), 300-307.

Singh, V. V., Ram, M., & Rawal, D. K. (2013). Cost analysis of an engineering system involving subsystems in series configuration. *Automation Science and Engineering, IEEE Transactions on*, *10*(4), 1124-1130.

Verma, A. K., Srividya, A., & Karanki, D. R. (2010). *Reliability and safety engineering* (pp. 5-7). London: Springer.

Weaver, A. C. (2006). Biometric authentication, *Computer*. *39*(2), 96-97.