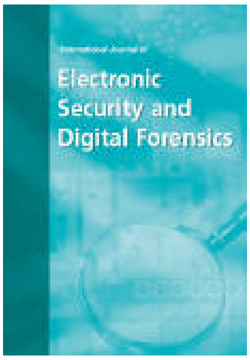


**International Journal of Electronic Security and Digital Forensics**

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

# Formulation of a two-level electronic security and protection system for malls

T. Thirumurugan, Leena Bojaraj, R. Lavanya, T.J. Nagalakshmi

**DOI:** 10.1504/IJESDF.2024.10053197

**Article History:**

| | |
|---|---|
| Received: | 13 July 2022 |
| Accepted: | 27 October 2022 |
| Published online: | 12 January 2024 |

# Formulation of a two-level electronic security and protection system for malls

T. Thirumurugan*

Department of Electronics and Communication Engineering,
Christ College of Engineering and Technology,
Puducherry, India
Email: thiru0809@gmail.com
*Corresponding author

Leena Bojaraj

Department of Electronics and Communication Engineering,
KGISL Institute of Technology,
Coimbatore, India
Email: sairamleena@gmail.com

R. Lavanya

Department of Electronics and Communication Engineering,
N.G.P Institute of Technology,
Coimbatore, India
Email: lavanyaraju4985@gmail.com

T.J. Nagalakshmi

Department of Electronics and Communication Engineering,
Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences,
Chennai, Tamil Nadu, India
Email: t.j.nagalakshmi@gmail.com

**Abstract:** Electronics are everywhere around us these days, and many of them help us maintain security in different locations. However, there are still numerous security issues that banks, residences, and other establishments must deal with. The real-time identification of possibly suspicious actions in shopping malls is the main goal of the comprehensive expert system we present in this article. Our video surveillance technique makes a number of creative suggestions that combine to create a solid application that effectively tracks people's movements and identifies suspicious activity in a retail setting. The discussion of several present and developing solutions aimed at obtaining a high level of trust in IoT applications follows the discussion of security concerns. Four potential technologies blockchain, edge devices, cloud technologies, and machine learning are examined. An experiment demonstrates that in the same dependable network environment of DCNs, our responsibility security routing system performs better.

**Keywords:** electrical gadgets; video monitoring in malls; background removal; RFID tags; barcode reader.

**Reference** to this paper should be made as follows: Thirumurugan, T., Bojaraj, L., Lavanya, R. and Nagalakshmi, T.J. (2024) 'Formulation of a two-level electronic security and protection system for malls', *Int. J. Electronic Security and Digital Forensics*, Vol. 16, No. 1, pp.63–72.

**Biographical notes:** T. Thirumurugan received his PhD from Anna University in Chennai in Information and Communication Engineering, and he has completed his BTech (ECE) and MTech (ECE) degrees from Pondicherry Engineering College. He is working as a Professor in the Department of Electronics and Communication Engineering at the Christ College of Engineering and Technology, Puducherry. He has been a teacher for 19 years. He is also a life member of the Indian Society for Technical Education (ISTE) and the Institution of Electronics and Telecommunication Engineers (IETE). He is currently the College Coordinator for the (ARIIA) Atal Ranking of Institutions on Innovation Achievements as a part of the Institution Innovation Council. He is also a reviewer for an international journal publication. He has published eight international papers in various refereed journals, and he has presented seven papers at international conferences.

Leena Bojaraj is an Assistant Professor in the Department of Electronics and Communication Engineering at KGISL Institute of Technology, Coimbatore. She has completed her PhD from Anna University, Chennai. She has published more than 20 papers in reputed journals like Annexure I, SCIE and Scopus Index and UGC Care. She has done many research and consultancy works.

R. Lavanya is an Assistant Professor in the Department of Electronics and Communication Engineering at Dr. N.G.P. Institute of Technology, Coimbatore .She holds Master of Engineering with specialisation in VLSI DESIGN at Anna University of Technology Coimbatore. She has completed her PhD from Anna University, Chennai. Her research areas are hardware security, IoT and signal processing. She has published many papers in reputed journals.

T.J. Nagalakshmi is currently working as an Associate Professor in Electronics and Communication Engineering Department, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India. She has more than 13 years of teaching experience and one year of research experience as SRF. She has published more than 50 papers both in reputed international and national journals. Her areas of research are communication, VLSI and image processing.

## 1 Introduction

Many different kinds of sensor devices are available, like motion sensors to measure the accelerator, rotational, velocity, inclination, torsion, vibrations, and resonance. Recently, the idea of the internet of things (IoT) has gained interest, particularly when merging IPv4 and IPv6 networks. The gases, oxygen, heat, humidity, vacuum, pressure, and wind are all measured by atmosphere sensors. Position sensors take measurements of distance, position, proximity, and level difference. As retail malls increasingly incorporate a large number of private properties, corporate security, whether on an internal or contract level, has become crucial in the private sector. The corporate security in shopping malls is the main topic of this chapter. We start by looking at the history and different kinds of retail malls. Today, the key component of every security system is the video footage obtained from carefully placed cameras. Because of this, computer vision processing may be used to extract meaningful data from these films and interpret this data to automate a variety of video-surveillance duties by sounding alerts when danger occurrences are found.

Awati and Awati (2013) presented the 'Intelligent Shopping Cart', which aims to decrease and maybe eliminate consumer wait times altogether, lessen the need for market labour, and increase overall effectiveness. Additionally, more digital gadgets are essential to the future of the retail sector. The direction of approach, the date and time, the time difference between arrivals, and the transmission power indicator data are crucial factors in the implementation of DD. All of these metrics are susceptible to S&P, which results in incorrect DD.

According to recent research by Aguia (2016), the enhanced 5G services will facilitate network-based discovery. The application-specific discovery precision varies. On the currently installed IoT apps, there have been several security and privacy threats from all over the globe. It was believed that the Mirai assault in the fourth quarter of 2016 infected around 2.5 million internet-connected devices and launched a Mirai Botnet distributed denial of service (DDoS) attack. Based on approximative directed routable probabilities, Duong and Kaneko (2014) created two novel fault-tolerant networking algorithms for hypercubes and tested them using a computer simulation. Similar to this, Park et al. (2015) published results of a computer experiment demonstrating improved performance of their method and offered a fault-tolerant routing protocol in a dual-cube using the same concept. Xu et al. (2006) suggested the edge fault-tolerant features of hypercubes and folded hypercubes, and these findings provide a strong theoretical foundation for fault-tolerant routing methods.

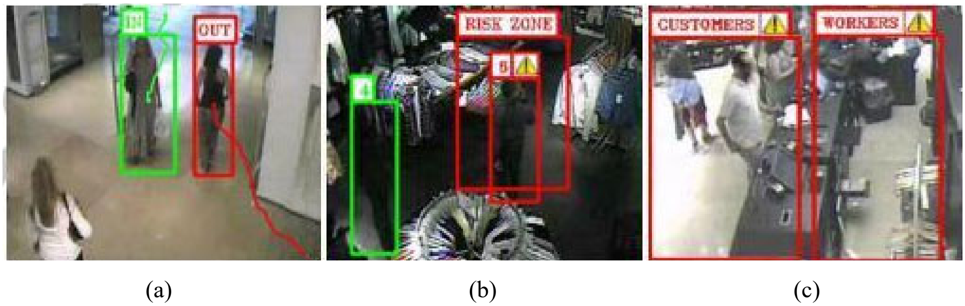
## 2 Literature survey

Video surveillance systems have developed since the 1960s in a manner analogous to the degree of automation they have reached:

- first (1960–1980), low levels of automation and analogue CCTVs
- digital CCTVs and machine learning processing (second) (1980–2000)
- semi-automated video surveillance systems (from 2000 to the present).

A considerable level of automation has been achieved by the third generation of security solutions, enabling it to recognise certain dubious human actions and sound the relevant warnings. But certain traditional segmentation techniques, such as those derived from fuzzy models (Zhang and Xu, 2006; Baf et al., 2008b) or Gaussian mixture models (Grimson and Stauffer, 1999; Zivkovic, 2004; Baf et al., 2008a), continue to be commonly used (Baf et al., 2008c). Additionally, various approximations, including the multi-layer edge detection based on colour and texture proposed by Odobez and Yao (2007), might be intriguing.

**Figure 1** Alarms discovered by our professional monitoring system in marketplaces, (a) entry and exit (b) loitering event (c) unattended cash desk (see online version for colours)



(a) (b) (c)

A microprocessor in a product identification device (PID), an LCD, an RFID reader, an EEPROM, and a ZigBee module were used in this model of the ‘smart shopping cart with automated billing system using RFID and ZigBee’. This essay focuses on a particular use of video surveillance: identifying potentially troubling human activity in malls. As indicated in Figure 1, there are several specific circumstances in this scenario that must be examined, such as store admission or leave, loitering incidents that might result in theft, or circumstances when a cash desk is left unattended.

Furthermore, the covert filming of people in public raises concerns about privacy rights (Hier and Walby, 2011). Since 1980, this sector has been steadily expanding, despite encountering challenges brought on by the rise of internet trade and, more recently, the COVID-19 epidemic. Because of this, there was a decrease of 34% in the number of individuals who went to shopping centres in 2020, as well as a decrease of 28.9% in sales as compared to the previous year. Customers seek out new experiences inside shopping centres as a result of the extensive selection of products and services already available, as well as the severe level of rivalry for sales that exists across a range of distribution channels. As a result of the COVID-19 issue and the growth of business conducted online, customers have grown more particular about the amenities they want from a shopping centre in order to enjoy their time there. Services such as fashion, grocery stores, and movie theatres are examples of industries that are failing to match the requirements of today’s client, who values uniqueness (Man and Qiu, 2021).

Certain shopping centres provide a greater allure than others, both to the final customer as well as to the companies that may be housed there (Grimmer et al., 2016). In and of itself, the notion is shrouded in a certain air of mystery in terms of how it should be managed and coordinated (Bagdare and Jain, 2013). The promotion of unity under a single management is seen as a difficult undertaking, which makes the administration of a shopping centre, which is where a concentration of various stores and brands are engaged in fierce rivalry (Katrodia et al., 2018), a challenging endeavour. There is a widespread recognition in the academic literature on the study of shopping centres regarding the level of gratification experienced by end consumers (Blešic et al., 2014) and the management of stores that are located within them (Teller and Alexander, 2014; Jaravaza and Chitando, 2013), with a particular emphasis placed on the image that is portrayed in the minds of consumers. On the other hand, there is no study that has been identified that discusses the administration of the centre by the manager and the interaction with the three tiers of customers, which are ownership, retailers, and end consumers.

## 3 Methodology

Encryption, as in regular wireless communication, is often used to implement security in D2D communication. However, physical-layer security provides additional security via network evaluations that fits well enough in the D2D communication models proposed by Dabbagh and Rayes (2019). When using cellular systems with a receiver, physical-layer security is taken into account for D2D communication. Apart from 5G, these sorts of security problems affect other networks as well, both in terms of communication and detection.

Attacks that eavesdrop specifically into a device's stream to get sensitive information also use in-band and out-band techniques. Impersonate attacks, which use both in-band and out-of-band techniques, might present themselves as legitimate tools to access data traffic information. Equipment tampering is when the attacker attempts to get physical access but only affects the out band. The S&P is dependent on the in-band and out-of-band D2D, which is detailed together with the generational development.

### *3.1 Existence of malicious devices in the network*

In the next-generation networking, producing and spoof devices that communicate inaccurate discovery measurements are examples of hostile devices that provide false information to the LISP. The term 'beaconing' refers to the situation in which a malicious device retransmits a discovery signal that has been delayed but is otherwise the same in order to confuse navigation system unit recipient devices. The term 'spoofing' refers to the situation in which a malicious device transmits a fake navigation signal in order to trick a mobile navigation receiver into using the false signals and making a false discovery.

### *3.2 Network-assisted database deterioration*

An electronic toll road's Received Signal Strength (RSS)-based approaches, for instance, are affected by a database degradation because the bill could be easily sent with another device, as shown in Table 1. This applies to discovery techniques that rely on a pairing database.

### *3.3 Insufficient privacy policies*

A LBSP makes use of discovery data to provide a web-based service. Its creators often rely on sources from other parties. For instance, location-aware advertising may make use of details about various store promotions in a certain mall, together with customer loyalty cards for that particular store. Because the third-party unit relies on the discovery data, these requirements can conflict with LBSP policy, which states that the discovery data can only be used anonymously. The amount and kind of discovery data that is obtained by the third parties should be made explicit in the LBSP. If such information relates to a specific device profile, the devices should be made aware of it according to the LBSP policy. The devices might choose and use their own discovery information using this mechanism. The proper use of the finding information may be strengthened and confirmed in a variety of ways.

**Table 1** Externally and internally threats on safety and privacy within IEEE802.11p and LTE-X2X

| *Threats* | *IEEE802.11p* | | *LTE-X2X* | | | |
|---|---|---|---|---|---|---|
| | | | *Cellular-based* | | *D2D-based* | |
| | *External* | *Internal* | *External* | *Internal* | *External* | *Internal* |
| Hole attacks (Black&Grey) | ✓ | × | ✓ | × | × | × |
| Jamming attacks | × | × | × | × | × | × |
| Flooding attacks | ✓ | × | ✓ | × | × | × |
| Coalition attack | ✓ | × | ✓ | × | ✓ | × |
| Signal alteration attacks | ✓ | ✓ | ✓ | × | ✓ | × |
| Inject false signal attack | ✓ | × | × | × | ✓ | × |
| Echo attack | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| GPS hoaxing attack | × | × | × | × | × | × |
| Eavesdropping attack | ✓ | × | ✓ | × | × | × |
| Location tracking | × | × | × | × | × | × |
| Certificate duplication attack | ✓ | ✓ | ✓ | ✓ | × | × |
| Sybil attack | ✓ | ✓ | ✓ | ✓ | × | × |
| Camouflaged take-off attack | ✓ | ✓ | ✓ | ✓ | × | × |
| Multiple | - | ✓ | - | ✓ | - | ✓ |

## 4 Result and discussion

Shops all throughout the world draw diverse groups of hundreds and thousands of shoppers every year. Potential criminals of all types may be drawn to a given property depending on its setting, design, and target audience. Sadly, because of the development and phenomenal expansion of retail complexes, crime has begun to increase there. The variety of retail complexes that are there, as mentioned previously, makes this issue even more complicated. Security professionals are faced with a variety of challenges that must change along with the retail malls' constantly evolving features. Figure 3 displays the results of our method's testing employing the various visual appearance aspects designated for occlusion management.

An illustration of a tracking assessment for the movie 'ShopAssistant1cor.mpg' from the open CAVIAR dataset is as follows: T1 and T2 first arrive on the scene.

1 T1 and T2's paths cross and become occluded.

2 The blockage goes away, and T1 and T2 are given their proper labels once again. T3 also shows up on the scene.

3 T1 and T2 vanish from the scene.

4 T3 is leaving the area.

5 A trio of three occluded persons identified as T4 leave the store after many still frames.

6 Once the interference between the three members of the T4 group is identified, each member of the group begins to be monitored separately as T6, T7 and T8.

7 T9 shows up on the scene.

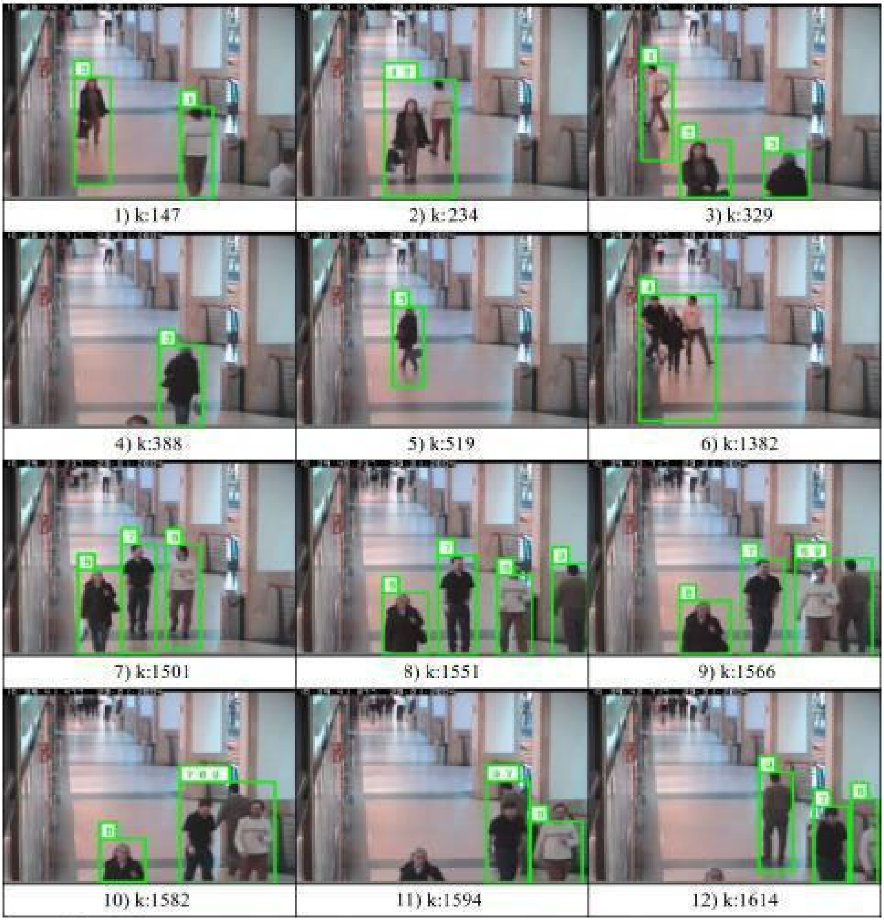
8 Between T6 and T9, an obstruction begins.

9 T7 enters the space between T6 and T9 that is blocked.

10 The occlusion is dropped, and T6 is appropriately re identified.

11 The obstruction between T7 and T9 is completed, and both are given their proper identities once again.

**Figure 2** For detecting alarms in stores (see online version for colours)



1) k:147

2) k:234

3) k:329

4) k:388

5) k:519

6) k:1382

7) k:1501

8) k:1551

9) k:1566

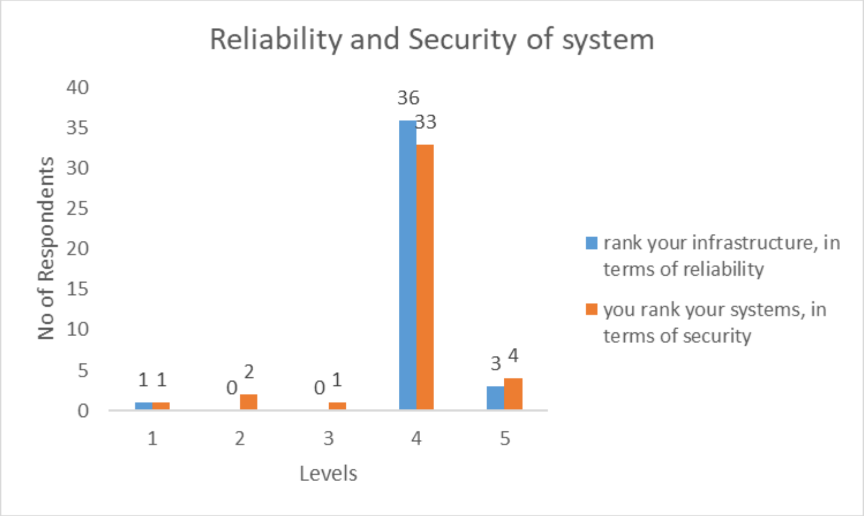
10) k:1582

11) k:1594

12) k:1614

The scene then comes to a close. The trolley's commercial usefulness will be the first of its type. With the assistance of the appropriate sensors, such as RFID Tags, this gadget captures the data of the various items. With the use of a computer and a printout of the collected data, the store owner may analyse consumer buying patterns and preferences in great detail. With an automatic trolley, there is no need to lift a heavy cart, wait in a billing line, or consider your spending plan.

**Figure 3** Reliability and security of a system (see online version for colours)



The client is automatically followed by the trolley built on a microcontroller. The three tiers of D2D S&P issues are lower, moderate, and high level. Physical and data connectivity layers are impacted by low-level attacks. These include jammer assaults, spoofing attacks, sleep deprivation attacks, susceptible device setup, and insufficient physical interface security. The processing power and memory limitations of the D2D S&P design are requirements. It is the main bottleneck in the development of a potent S&P system. The reliability and the security of a system are shown in figure 3. These specifications must be followed while running cryptographic algorithms. Security managers have been forced to adjust security planning requirements in accordance with the tenants, customers, and surrounding region of a shopping mall. The major findings of this study support the effectiveness of our high quality video alarm system for malls.

## 5 Conclusions

Thus, we deduced from this study that many security sensor kinds, including accelerometers, glass break detectors, doors and windows detectors, LDR, etc., are used in security systems. Future study is advised, particularly on the best proactive measures entertainment areas might take to deter crime and violent behaviour. Obtaining a greater degree of automation in the monitoring operations described in this paper, for example, might result in some additional intriguing future research topics for the society of expert systems with applications. Our system now relies on human supervision to control the alerts that are triggered when suspicious behaviours are found. However, in the future, it may be possible to fully automate all surveillance tasks by using potent machine learning algorithms. Our further research will concentrate on enhancing the present system, such as by lowering computing overhead at the smart shopping trolley side for greater efficiency and figuring out how to boost communication effectiveness while maintaining security features. To safeguard the S&P of the gadget, it may be divided into four categories. There have also been discussions about a number of unresolved difficulties and problems that stem from the solution itself. The most recent developments in IoT security have also been reviewed, along with some potential future research topics. This method is anticipated to be a useful tool for future IoT applications looking to improve security.

## References

Aguia, R.L. (2016) 'White paper for research beyond 5G (final edit)', *Net World*, October, Vol. 1, No. 2016, pp.1–43.

Awati, J.S. and Awati, S.B. (2013) Smart trolley in mega mall', in Karmouche, A. and Salih-Alj, Y. (Eds.): *IJETAE-0312-82, Aisle-level Scanning for Pervasive RFID-based Shopping Applications*, IEEE.

Baf, F.E., Bouwmans, T. and Vachon, B. (2008a) 'Background modeling using mixture of Gaussians for foreground detection – a survey', *Recent Patents on Computer Science (RPCS)*, Vol. 1, No. 3, pp.219–237.

Baf, F.E., Bouwmans, T. and Vachon, B. (2008b) 'Fuzzy integral for moving object detection', *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, pp.1729–1736.

Baf, F.E., Bouwmans, T. and Vachon, B. (2008c) 'Type-2 fuzzy mixture of Gaussians model: application to background modeling', *International Symposium on Visual Computing (ISVC)*, Vol. 2, pp.772–781.

Bagdare, S. and Jain, R. (2013) 'Measuring retail customer experience', *Int. J. Retail. Distrib. Manag.*, Vol. 41, No. 9, pp.790–804.

Blešic, I., Dragin, A., Markovic, J., Cerovic, S. and Deri, L. (2014) 'Relationships among shopping quality and corporate social responsibility of shopping centers and consumer satisfaction: case from Novi Sad (Serbia)', *Amfiteatru Econ. J.*, Vol. 16, No. 3, pp.415–429.

Dabbagh, M. and Rayes, A. (2019) 'Internet of things security and privacy', *Internet Things From Hype to Reality*, pp.211–238, Springer, Cham, Switzerland.

Duong, D.T. and Kaneko, K. (2014) 'Fault-tolerant routing based on approximate directed routable probabilities for hypercubes', *Future Generation Computer Systems*, July, Vol. 37, pp.88–96.

Grimmer, M., Kilburn, A.P. and Miles, M.P. (2016) 'The effect of purchase situation on realized pro-environmental consumer behavior', *J. Bus. Res.*, Vol. 69, No. 5, pp.1582–1586.

Grimson, L. and Stauffer, C. (1999) 'Adaptive background mixture models for real-time tracking', *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp.2246–2252.

Hier, S.P. and Walby, K. (2011) 'Privacy pragmatism and streetscape video surveillance in canada', *International Sociology*, Vol. 26, No. 6, pp.844–861.

Jaravaza, D.C. and Chitando, P. (2013) 'The role of store location in influencing customers' store choice', *J. Emerg. Trends Econ. Manag. Sci.*, Vol. 6, No. 4, pp.302–307.

Katrodia, A., Naude, M. and Soni, S. (2018) 'Determinants of shopping and buying behaviour: a case at Durban shopping malls', *Afr. J. Bus. Econ. Res.*, Vol. 1, No. 1, pp.219–241.

Man, M.M.K. and Qiu, R.C.Q. (2021) 'An empirical study of factors influencing consumers' purchasing behaviours in shopping malls'. *Int. J. Mark. Stud.*, Vol. 13, No. 1, p.14.

Odobez, J.M. and Yao, J. (2007) 'Multi-layer background subtraction based on color and texture', *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.

Park, J., Hirai, Y. and Kaneko, K. (2015) 'Fault-tolerant routing in dual-cubes based on routing probabilities', *Procedia Computer Science*, 1 January, Vol. 69, pp.66–75.

Teller, C. and Alexander, A. (2014) 'Store managers – the seismographs in shopping centres', *Eur. J. Mark.*, 4 November, Vol. 48, pp.2127–2152.

Xu, J., Ma, M. and Du, Z. (2006) 'Edge-fault-tolerant properties of hypercubes and folded hypercubes', *Australasian Journal of Combinatorics*, 1 June, Vol. 25, pp.7–16.

Zhang, H. and Xu, D. (2006) 'Fusing color and texture features for background model', *International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, pp.887–893).

Zivkovic, Z. (2004) 'Improved adaptive Gaussian mixture model for background subtraction', *International Conference on Pattern Recognition (ICPR)*, pp.28–31.