The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/2634-2499.htm

Deployment of physical access control (PAC) devices in university settings in Ghana

Edward Ayebeng Botchway
Department of Architecture, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
Kofi Agyekum and Hayford Pittri
Building Science, Engineering and Materials Research Team, Department of Construction Technology and Management, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana, and
Anthony Lamina
Department of Architecture, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

Received 19 January 2023
Revised 4 March 2023
15 May 2023
Accepted 17 May 2023

Abstract

Purpose – This study explores the importance of and vulnerabilities in deploying physical access control (PAC) devices in a typical university setting.

Design/methodology/approach – The study adopts face-to-face and telephone interviews. This study uses a semi-structured interview guide to solicit the views of 25 interviewees on the subject under consideration. Qualitative responses to the interview are thematically analyzed using NVivo 11 Pro analysis application software.

Findings – The findings reveal five importance and seven vulnerabilities in the deployment of PAC devices in the institution. Key among the importance of deploying the devices are "prevent unwanted premise access or intrusions," "prevent disruptions to university/staff operations on campus" and "protect students and staff from outside intruders." Key among the identified vulnerabilities are "tailgating", "delay in emergent cases" and "power outage may affect its usage."

Originality/value – This study offers insight into a rare area of study, especially in the Sub-Saharan Africa region. Furthermore, the study contributes to the state-of-the-art importance and vulnerabilities in deploying PAC devices in daily human activities. The study is valuable in that it has the potential to establish a foundation for future studies that may delve into investigating issues associated with the deployment of PAC devices.

Keywords Physical access control system (PACS), University setting, Physical access control, Devices, University campus, Security

Paper type Research paper

1. Introduction

The introduction of the internet of Things (IoT) concept can be viewed as an expansion of the interaction between humans and software (Omolara *et al.*, 2022; Aldowah *et al.*, 2018). For the deployment of a secured IoT system, it has been determined that identity and authentication, access control and privacy are significant concerns. In addition, the IoT will significantly

Frontiers in Engineering and Built Environment
Vol. 4 No. 1, 2024
pp. 1-14
Emerald Publishing Limited
e-ISSN: 2634-2502
p-ISSN: 2634-2499
DOI 10.1108/FEBE-01-2023-0006

influence the educational experience, particularly in the higher education system. As such, integration of physical security, namely access control, into any institution's system or platform is vital to ensure property safety, people protection and the preservation of the institution's integrity (Aldowah *et al.*, 2018).

Access control is a crucial aspect of security (Chinnasamy and Deepalakshmi, 2022; Karp *et al.*, 2010). Security is an important management issue for all higher education institutions for the safety and security of students, staff and visitors. Also, the potential damages to the institutions can affect their reputation because of the incidents related to crimes. The risk analysis of physical, information technology (IT) and communications security management in member educational institutions establishes higher security measures to be adopted for all legal objectives, assets and values. It is transposed into the security plan and alarm system design. Despite measures put in place to provide everyone the right to be free from all forms of violence, in recent years, universities have been plagued with increasing levels of violence with minimal response from university authorities (Dlamini and Olanrewaju, 2021).

University and college campuses are similar to urban centers in that they have people interacting within physical environments. However, just like cities, crime and the fear of crime is of concern on campuses (Iloma *et al.*, 2022; Mrozla, 2022; Jennings *et al.*, 2007). This suggests a real need to address campus safety better. Campus surveillance is paramount in every university institution, and it is a design concept that facilitates the rightful owners of space to observe people that appear to be suspicious. A result is that potential offenders will avoid these spaces because they sense a potential risk of being noticed (Iloma *et al.*, 2022; Crowe, 2000). Crime and fear of crime affect the quality of life of those that call campuses "home" (Mrozla, 2022; Jennings *et al.*, 2007). Should institutional leaders choose not to address the issue of personal safety on campus, users may begin to avoid certain areas within the campus's physical environment out of fear for their safety. In some cases, they may choose to avoid the campus completely. However, numerous studies and theories suggest that effective planning and design practices can increase personal safety and improve the quality of life and experience of places.

With the Ghanaian government's introduction of the double-track education system, the number of prospective students expected in various universities is bound to increase. This suggests that safety and security on the various campuses will be affected negatively due to the explosive increase in population. Many university campuses in Ghana have started deploying access control devices at several facilities to help mitigate the menace associated with the increased intake of students and external intruders. These controls will assist in improving the security of life and property on the campuses. Notwithstanding, there are questions that ought to be asked. Are the university communities aware of any importance associated with deploying these devices? Do the university communities encounter any vulnerabilities with the deployment of these devices? The answers to these questions are sought after by using a typical Ghanaian university as a case study. The study investigates the importance and vulnerabilities of deploying physical access control (PAC) systems on university campuses. The study is structured into five major sections. The first section introduces the study. The second section reviews literature pertinent to the theme under investigation. The third section presents the methodology. The fourth section presents and discusses the results. The final section concludes the study.

2. Literature review

2.1 Access control systems

Access is the selective restriction of entry to a property, a building or a room to authorized persons by which the act of accessing may mean entering or using (Azimi and O'Brien, 2022; Bowers, 2013). The term access control describes the procedures and safeguards to restrict and monitor who has access to sensitive data or places (Hu *et al.*, 2019). Access control allows or prevents persons from entering or leaving an area. Access control systems rely on a person or asset being recognized and authenticated, usually utilizing a credential (Laan, 2021). A credential refers to the authorization a person holds, which can be in the form of a key, ID card, PIN or password which is intrinsic to them. It can also be biometric data such as iris recognition or fingerprints (Hu *et al.*, 2019). Access control is not meant to restrict access but control it.

Access control systems can be categorized into two broad classes: geographical and physical. Personnel such as border guards and ticket collectors are examples of geographical access control systems regulating who can enter a restricted area. Furthermore, PAC determines who is allowed to enter or exit, where they are allowed to enter or exit, and when they are allowed to enter or exit (Hutter, 2016). For example, parking access control systems allow parking and garage owners to regulate, restrict access and generate a profit. Parking software manages and authorizes access to parking systems. Mantrap and other electronic access control systems are examples of technological solutions to the problem of ensuring that only authorized individuals have access to a building or other restricted areas.

A complete access control system performs three functions: authentication, authorization, and accountability (Ouaddah *et al.*, 2017). Authentication verifies a person, process or device's identity before granting access to system resources. Authorization grants or denies a user, program or process access permissions. Accountability is the independent inspection of records and operations to guarantee compliance with established controls, policies and operational processes (Floridi *et al.*, 2022; Hu *et al.*, 2006).

2.2 Physical access control

Prevention of unlawful entry, property damage and data interference is the goal of PAC deployment (Masoumzadeh *et al.*, 2022; Holstein *et al.*, 2022; Sodiya *et al.*, 2010). Physical security, in architecture, deals with controlling entry into a building and protecting assets or properties from theft. Physical security involves using multiple layers of interdependent systems, including CCTV surveillance, security guards, protective barriers, locks, access control protocols and many other methods to deter security vulnerabilities and threats (Nelson, 2020). This is achieved through adequate site planning, extensive burglar proofing, and the creation of buffer zones that increase the time it takes to access critical spaces, thereby effectively controlling and managing access (Nelson, 2020; Ebregt and Greve, 2000). PAC can efficiently monitor resource access and prevent the transmission of unauthorized entry. In addition, physical access systems have evolved from traditional padlocks and keys to barriers such as speed gates and turnstiles, as well as advanced electronic and logic-based access control technologies such as smart cards and biometrics (Masoumzadeh *et al.*, 2022). According to Rouhani *et al.* (2018), access control comprises essential components: user credentials, a reader/scanner and access control software. The user credential allows entry into an area, and the reader/scanner allows the credential to be read for authorization to take place. In addition, the software manages the access control functions to allow smooth operation.

In recent years, it is noticed that many buildings do not need full-time security guards since it is possible to regulate who can enter and exit at specific points. Physical security barriers, including doors, locks, network video systems, alarms and electronic access control, can be used where stationing an officer is impractical (Best and Nelson, 2020). As a preventive measure against the devastating effects of vandalism, theft and terrorism, PACs limit who can access available resources and enter protected places (Masoumzadeh *et al.*, 2022). In higher education, PAC is essential for entry into the library, residential halls, lecture theaters and network access (Velasco, 2022; Cheng *et al.*, 2020; Bigelow Stephen, 2008). However, these systems continue to depend significantly on user authentication. To increase the efficiency of the security systems, combinations of the various systems are used (Qiu *et al.*, 2020; Yaacoub *et al.*, 2020; Oriyano, 2014).

An example is a smart card with a retina scanner so that whenever the card goes missing or is stolen, there is no immediate threat of accessing the place of interest with the retina scanner. In addition, improving safety for higher institution students, teachers and administration is a top priority. As a result, the institution's regular educational operations can proceed without fear of disruption due to acts of violence, and protection from potential intruders makes PAC a need (Adu *et al.*, 2022).

3. Research method

3.1 Research approach/strategy

This research followed a qualitative approach, as it systematically worked to solve the research problem and achieve the aim of the study. The study sought to explore the importance and vulnerabilities of deploying PAC systems in a typical Ghanaian university setting. This study settled on this approach because, after the literature review, there needed to be more information concerning the theme under investigation, regionally and globally. With this insufficiency in information, it became necessary for the study to focus on the actual views of respondents concerning the subject under study. Figure 1 is a flow chart that shows the steps followed in the methodology.

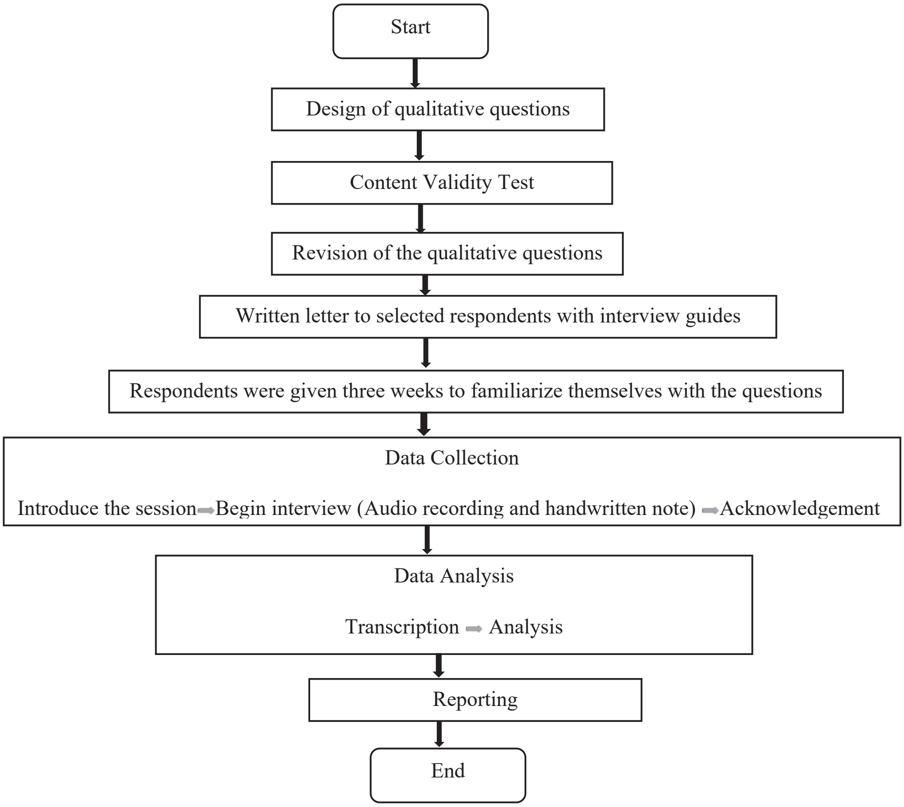
Start
Design of qualitative questions
Content Validity Test
Revision of the qualitative questions
Written letter to selected respondents with interview guides
Respondents were given three weeks to familiarize themselves with the questions
Data Collection
Introduce the session
Begin interview (Audio recording and handwritten note)
Acknowledgement
Data Analysis
Transcription
Analysis
Reporting
End

Figure 1.
Flow chart for adopted methodology

Source(s): Authors (2023)

3.2 Design of interview guide

To achieve the research aim, a literature review on the theme under consideration was carried out to gain insight into existing information. Because the study was qualitative, an interview guide was employed. The interview guide was structured into two sections. The first section gathered some background information about the respondents. The second section sought the respondents' views on the importance and vulnerabilities of deploying PAC systems on the university campus under investigation. A two-step approach was followed to assess the appropriateness and rationality of the interview guide. A content validity test was first conducted by referring to five researchers with in-depth knowledge of PAC. The researchers' comments helped to revise the unclear and obscured questions by rewording them. Also, non-functioning and ineffective questions were discarded. The second step ensured the modification of the interview guide using the comments and suggestions from these researchers. Finally, the interview guide was given to the various interviewees, with an accompanying letter detailing the purpose of the study. The interview guide was distributed three weeks before the planned interview schedule to offer the interviewees quality time to prepare and provide salient responses.

3.3 Conducting interview

The population for the study comprises both students and staff who have lived on the university campus under consideration for more than one academic year. Face-to-face and telephone interviews were used. The interview duration ranged from 20 to 40 min, allowing interviewees to express their thoughts and ideas in detail freely. The criteria used to select the interviewees are as follows.

(1) The interviewee must be a student, teaching staff, or non-teaching staff of the university.

(2) The interviewee must possess knowledge of PAC devices.

(3) The interviewee must have lived, schooled or worked on the university campus for more than one academic year.

(4) The interviewee must be willing to partake in the research.

Following the above criteria, purposive sampling was used to select 20 students, three teaching staff, and two non-teaching staff on the university campus. Variabilities in the sample size were due to the level of usage of the PAC devices by the participants of the study. Because the population of students at the university was respectively higher than the teaching and non-teaching staff, and also, because the students use the PAC devices deployed on the university campus more often compared to other study participants, the study targeted more students. According to Agyekum *et al.* (2021) and Yin (2014), using between 5 and 50 participants for a qualitative study is adequate. Furthermore, Pillay *et al.* (2022), Agyekum *et al.* (2021), and Parse (1990) stated that for a qualitative study, obtaining data from 2 to 10 participants was sufficient. Hence, the 25 respondents in this study phase adequately provided the information needed.

3.4 Data analysis

Data obtained were thematically analyzed. According to Castleberry and Nolen (2018), thematic analysis is a qualitative approach that examines research data to understand and represent the experiences of people as they encounter, engage with, and live those experiences. It is used to identify, analyze and report patterns or themes within data. Kiger and Varpio (2020) provided procedural guidelines for conducting thematic analysis. Lester *et al.* (2020) and Charmaz (2006) postulated that the phases of thematic analysis are like the data analysis process for the development of grounded theory. It was further indicated that it involves familiarizing oneself with the data; generating initial codes; searching for themes; reviewing the themes, and defining and naming them. In analyzing the data from the interviewees, the responses were coded using Nvivo 11 Pro analysis application software. The coding involved the examination of interviewees' responses, intending to group and tag the responses with codes to facilitate later retrieval. The responses were coded in nodes (themes) by identifying patterns. Node allowed the researchers to gather related material in one place to look for emerging patterns and ideas. From the interviews, the importance of PAC systems identified was the following: (1) prevent unwanted premise access or intrusions, (2) prevent disruptions to university/staff operations on campus, (3) protect students and staff from outside intruders, (4) limit movements during and after business hours and (5) protect inventory and equipment from theft or misuse (decrease liability and risk associated with stolen or misused equipment). The vulnerabilities identified were the following: (1) tailgating, (2) delay in emergent cases, (3) a power outage may affect its usage, (4) security men having to monitor its usage, (5) human trafficking, (6) students/staff giving their cards out/misplacing ID cards and (7) malfunctioning of most of the PAC devices. This importance and vulnerabilities are discussed and supported by verbatim (unedited) extracts from the data to highlight important issues. The interviewees were recorded using an audio recorder, and the data obtained were transcribed using MS Word 2016.

4. Results and discussion

4.1 Respondents' demography

Respondents' positions in the tertiary institution, years of stay on campus, and the interview mode are presented in Table 1. For ease of interpretation, the 25 interviewees were given

Table 1. Demographic Information of interviewees

No.	Position in KNUST	Code	Years spent on KNUST campus	Mode of interview
1	Student	ST 1	5	Face-to-face
2	Student	ST 2	4	Face-to-face
3	Student	ST 3	2	Face-to-face
4	Student	ST 4	3	Phone call
5	Student	ST 5	4	Phone call
6	Teaching staff	TS 1	15	Face-to-face
7	Teaching staff	TS 2	25	Face-to-face
8	Student	ST 6	3	Face-to-face
9	Student	ST 7	4	Phone call
10	Student	ST 8	3	Phone call
11	Student	ST 9	6	Phone call
12	Student	ST 10	4	Face-to-face
13	Non-teaching staff	NTS 1	10	Face-to-face
14	Non-teaching staff	NTS 2	14	Face-to-face
15	Student	ST 11	5	Phone call
16	Student	ST 12	2	Phone call
17	Student	ST 13	4	Phone call
18	Student	ST 14	4	Phone call
19	Student	ST 15	3	Phone call
20	Teaching staff	TS 3	23	Face-to-face
21	Student	ST 16	4	Face-to-face
22	Student	ST 17	4	Face-to-face
23	Student	ST 18	3	Face-to-face
24	Student	ST 19	3	Face-to-face
25	Student	ST 20	4	Face-to-face

Source(s): Authors (2023)

unique codes to represent the individual participants of the study. Participants within the student category were coded from ST1 to ST20, participants within the non-teaching staff category were coded from NTS1 to NTS2, and participants within the teaching staff category were coded from TS1 to TS3. Table 1 shows that the minimum number of years spent on campus by the interviewee was two years, and the maximum is 25 years indicating that the interviewees are in an excellent position to give adequate information on the subject matter. Fifteen out of the twenty-five interviewees were interviewed face-to-face, while the remaining ten were interviewed on the telephone after the samples of the interview guides had been sent to them. Thematic content analysis was used in the analysis of the data to identify the recurring materials.

4.2 Physical access control deployed by the tertiary institution under study

Through exploration and interviews, the conclusion was that the various security systems work alongside the access control systems to strengthen the efficiency of the overall security model used on campus. This included using security cameras and security personnel who help enhance the surveillance levels and monitoring of spaces coupled with the circulation control of the access control systems to enhance security. However, the inability of the portable key access control system to identify the user of any credential at the moment of granting access leaves room for intrusions into secure places on campus. The interviewees postulated that:

> All the halls of residences and the hostels on campus have turnstiles to ensure authorized entry. This has helped to curb crime and theft issues on campus over the past three years (NTS2).

> The various faculties have also mounted vehicle access control systems (auto-boom barriers) to ensure authorized entry into the faculties. The university's main library also has a turnstile, security guards, security cameras, and biometric scanners that help to ensure proper surveillance of students, staff, and their properties whiles using the library. In addition, students are mandated to use their ID cards to access the library, which makes it difficult for intruders to enter the library (NTS1).

All the interviewees revealed that they consider the campus safe due to the deployment of physical control devices in areas they perceived to be a threat.

4.3 Importance of physical access control deployment on campus

The study investigated the importance of PAC deployed on the university campus under investigation. The results indicated that the university premise felt safe and secure, except for a few places without physical security and access control devices. This reveals the importance of PAC systems in ensuring safety and security on the university campus for students, staff and visitors. As indicated earlier, the five themes that were generated include: "Prevent unwanted premise access or intrusions," "Prevent disruptions to university/staff operations on campus," "Protect students and staff from outside intruders," "Limit movements during and after business hours" and "Protect inventory and equipment from theft or misuse (Decrease liability and risk associated with stolen or misused equipment)." Sub-sections 4.3.1 to 4.3.5 further elaborate on these themes.

4.3.1 Prevent unwanted premise access or intrusions. The interviewees believed that the gates, turnstiles, auto-boom barriers and other PAC devices deployed by the university have helped to avoid unauthorized access/intrusion into the university premises. This conforms to the assertion by Masoumzadeh *et al.* (2022) and Holstein *et al.* (2022), who posited that PAC deployment aims to prevent unauthorized access, property damage and data disturbance. PAC can efficiently monitor resource access and prevent the transmission of unauthorized entry. With the primary goal of prohibiting unlawful entry into a facility, physical access systems have gone from traditional padlocks and keys to barriers like speed gates and turnstiles, as well as cutting-edge electronic and logic-based access control technologies like smart cards and biometrics (Masoumzadeh *et al.*, 2022; Lebea, 2020). Some of the comments received from the interviewees include the following:

> The turnstiles at the various residence halls prevent unauthorized people from accessing the halls, which provide some form of privacy (ST 3).

> "It will be difficult for any 'outsider' to access the hall facilities if they do not get assistance from the students or the security officers at the halls. This has helped to prevent unwanted entry into the university campus and the various halls and hostels on campus" (ST 5).

4.3.2 Prevent disruptions to university/staff operations on campus. Respondents also highlighted that the deployment of PAC systems in the university would help to prevent the disruption of operations/activities that the staff/university carries out. According to Rouhani *et al.* (2018), user credentials, a reader/scanner and access control software comprise essential access control elements. For example, the reader/scanner can read the credential so that entrance can be authorized. Additionally, the program controls the access control features to ensure they run smoothly without interference from unauthorized users or third parties (Rouhani *et al.*, 2018; Blackler, 2022). This was evident in some of the comments from the interviewees, such as:

> There is limited disruption of activities carried out in the university because the university does not accommodate unauthorized access or intruders (ST 7).

> The deployment of the physical access control system in KNUST, especially the vehicle access control system and car park access control system (auto-boom barrier), has helped to promote serenity in the various faculties. However, it has also created larger parking spaces for staff at the various faculties. Only staff with authorized ID cards can access the car parks at the various faculties (TS1).

4.3.3 Protect students and staff from outside intruders. Iloma *et al.* (2022) and Crowe (2000) postulated that every university institution prioritizes campus surveillance. This design idea enables the authorized occupants of a location to watch persons who seem suspects. As a result, potential perpetrators will steer clear of these areas because they fear being seen. Mrozla (2022) and Jennings *et al.* (2007) added that intruders in a university community might put fear in the lives of those who call camps "home," thereby affecting the quality of life on campus. Campus users may start to avoid specific areas of the campus' physical environment out of concern for their own lives if institutional authorities decide not to address the issue of personal safety and intruders on campus (Jennings *et al.*, 2007). Some interviewees deduced that:

> Most intruders in the surrounding communities come into the university campus for their personal agenda' (ST8).

> Most theft cases and misuse of the university facilities are recorded to be carried out by outsiders. However, the deployment of physical access control devices such as the turnstile, vehicle access control system, and car park access control system has helped to bring the situation down to its minimum best (TS 2 and NTS 1).

4.3.4 Limit movements during and after business hours. Interviewees indicated that the PAC systems in the university would limit the movement of students, staff, and visitors, which will go a long way toward ensuring productivity and confidence. This was evident in some interviewees' comments, as indicated below:

> Students are limited on spaces or areas they can be at certain times. Most places require staff IDs to access them, ensuring less academic and administrative work disruption. This will also go a long way to improve productivity and put confidence in students when moving around the university

> campus. Auto-boom barriers also ensure that only authorized vehicles get access to the various colleges and administrative spaces on campus (TS1).

> Movement is limited during lecture hours compared to the pre-deployment of physical control systems on campus because people just move into the faculties at any time (TS1).

4.3.5 Protect inventory and equipment from theft or misuse (decrease liability and risk associated with stolen or misused equipment). Interviewees clearly indicated that many spaces on the university campus are restricted from unauthorized access due to misuse of the space and theft issues experienced over the past few years. Some of the interviewees expressed their views as follows:

> Aside from giving confidence to students when using the university facilities, physical access control systems reduce crime actions and unforeseen robberies (ST13)

> Most physical access control devices are accompanied by security personnel or security access to track who uses the devices such as security cameras. This helps to detect crime and its associated risks (NTS 2).

All the security officers and lecturers who were interviewed indicated a reduction in the overall crime rate/cases on the university campus under study, suggesting that access control is necessary to curb crime in university campus settings.

4.4 Vulnerabilities for the deployment of physical access control system on campus

Seven themes were also generated from the analysis as vulnerabilities to the deployment of physical control access systems. These themes are: “Tailgating,” “Delay in emergent cases’,” “Power outage may affect its usage,” “Security men have to monitor its usage,” “Human trafficking,” “Students/staff give their cards out/Misplacing ID cards” and “Malfunctioning of most of the physical access control devices.”

4.4.1 Tailgating. Hutter (2016) indicated that attackers can enter secured areas through tailgating or hacking into access control smart cards or breaking in through doors. This means that under no circumstances can any security system be considered invulnerable. Tailgating is when an unauthorized person waits for a legal user to pass a PAC system and follows them in before the system closes (Reddy *et al.*, 2018). Also, a person can approach a security officer with a plausible story and be permitted in, notwithstanding the organization’s security rules (Salahdine and Kaabouch, 2019). The most common form of vulnerability for electronic systems is the “piggyback” intrusion. After a token is used to access a portal, an intruder follows right behind the authorized personnel. Some of the interviewees expressed their views as follows:

> There have been several instances where you will see people following you to access the faculty, but because they do not have an ID card, they will try and follow you closely before the system/machine closes (TS1).

> The security officers at the entrance of the halls and hostels normally have their ID cards with them to open for people who need access due to maybe misplacement of ID cards. Students sometimes lure them to let them get access to the halls to visit friends amongst others (ST 4)

4.4.2 Delay in emergent cases. The double-track system implemented in Ghanaian senior high schools will inevitably increase the number of students enrolling in the country’s colleges and tertiary institutions (Duflo *et al.*, 2019). This increase suggests that integrating and updating student information into the security database will take time. The time will create a lapse where security is at its weakest due to deactivating the security systems until all student data have been updated. This will occur during the first few months of the new academic year, putting students and properties at risk of being harmed or stolen. It was clear from the interviewees that:

> The turnstiles are left open in the first three months when new students arrive every academic year because their information needs to be captured in the system. They must also get their ID cards before accessing the halls, which normally takes about three months. This makes it impossible to use the turnstiles during this period (NTS 2)

> You may be late sometimes to class, and you happen to forget your ID card, but you have to go back and get it if nobody is around to assist you with his/hers (ST 5 – ST 8).

> There is always a queue at the entrance of the halls and hostels with the introduction of turnstiles in all the halls. This makes it difficult to access or exit the hall early in emergent situations (ST 11).

4.4.3 Power outage may affect its usage. In most tertiary institutions, PAC is crucial for entry into residential halls/hostels, lecture theaters, libraries and network access (Velasco, 2022; Cheng *et al.*, 2020; Bigelow Stephen, 2008). Nonetheless, user authentication and the use of electricity continue to be heavily reliant on these systems. Some of the challenges that are presented by power fluctuation on the university campus were indicated by one of the interviewees:

> Most systems driven by electricity without backup power sources tend to be disabled during blackouts. The turnstiles go off automatically when there is no electrical power. This makes the security personnel on duty open them for all users (ST 9).

4.4.4 Security men have to monitor its usage. Some interviewees pinpointed that the deployment of PAC devices, especially the turnstile, has no use because it requires security officers to monitor its usage and ensure users do not jump it. Some of the comments received include the following:

> The deployment of the turnstile has no use if security men would still have to be there to monitor how it is being used. Students can jump the machine or use someone's ID card to access it. There should be a means of ensuring that only one user can access it with his/her credentials. This can be done by making the machines biometric (ST 12).

> There are so many instances where students jump the machine or open it for friends to access it in the absence of a security officer monitoring it (ST 20).

4.4.5 Human trafficking/overcrowding. Interviewees indicated that the PAC system deployment had caused much traffic at the various halls and hostels in the morning since most students have lectures in the morning. In addition, the auto-boom barrier also creates traffic at the faculties in the morning when staff has to report to their various offices. They expressed their views as follows:

> Introducing physical access control creates congestion at the faculty during exams week. This is because almost all the students have to access one physical access control device or the other (ST18).

> The entrance of the halls is normally overcrowded in the morning or during major activities in the halls because there is only one turnstile each for entry and exit (ST 15 and ST 16).

4.4.6 Students/staff give their cards out/misplace their ID cards. From the results gathered, many respondents admitted to not carrying their ID cards wherever they went. Results also showed that it is common for individuals to share their credentials when accessing a space. This, therefore, leaves the system vulnerable to entry by criminals since the system only detects the credential of the certified individual and not the individual that enters using sharing other ID cards. They expressed their views as follows:

> I sometimes forget my ID card in the room, so I ask anyone at the entrance to place his ID on the turnstile for it to open for me. I do same for anyone I know (ST1 -ST8, ST12 – ST13, ST17).

> People normally ask you to open it for them, and you have no option. Sometimes, the machine is left open, especially when the lights are off and the plant has not been turned on. Anyone at all can access the hall/hostel in such a situation (ST11-15, ST20).

4.4.7 Malfunctioning of most of the physical access control devices. Respondents also highlighted that some turnstiles and CCTV cameras in the halls must be fixed due to the students' demonstration exercise in 2020. Some of the interviewees indicated that:

> Some of the turnstiles at the hostels on campus are not functioning due to an extensive student demonstration in 2020. Management has not fixed these turnstiles and CCTV cameras, so the hostels are easily accessed by people who do not reside in the hostels without any permission or invitation. Also, some of the auto-boom barriers at some faculties are out of function, so security officers monitor access to these faculties. The university lacks maintenance culture, and this needs to be improved in order to improve upon the benefits that come with the usage of the physical access control systems (TS 3).

> Potentially, the access control systems are a major crime deterrence, but the associated vulnerabilities indicate that over time, the system will not be as effective as it was in the inception phase (NTS1 and NTS 2).

According to Masoumzadeh *et al.* (2022), PAC may be exposed to the devastating effects of vandalism, theft and terrorism. This means adequate surveillance should exist in all areas where PAC devices are employed.

This study has revealed that PAC devices are essential in preventing unauthorized access to the university community. Gates, turnstiles, auto-boom barriers and other PAC devices deployed by the university have helped to avoid unauthorized access/intrusion into the university premises, thereby avoiding unlawful entry, damage to property and interference with the university data/facilities. This has also helped reduce crime and theft cases on the university campus. Moreover, disruption in university activities is limited since there is the need to access a PAC device before entering the university's critical places. University equipment and properties are protected from unauthorized uses, limiting the risks associated with stolen or misused university properties. The deployment of PAC devices by university communities must be considered due to the benefits of ensuring safety and security for students, staff and visitors on the university campus. However, deploying these devices comes with several vulnerabilities. Unauthorized persons wait for legal users to pass a system and then follow them in before the system closes, which makes the deployment of these systems susceptible to unauthorized users. The deployment also creates higher traffic on the university campuses, especially during peak times such as exams, orientations, graduations, etc. Power outages and the fact that security personnel must monitor the usage of the devices make its deployment inefficient. Efficient surveillance could be employed to this effect, such as fixing CCTV cameras near each PAC device. Lastly, students or staff giving their ID cards to colleagues to access the systems and Ghanaians' lack of maintenance culture make deploying these devices vulnerable.

5. Conclusion and recommendations

This study investigated the importance and vulnerabilities of deploying PAC systems in a typical university setting in Ghana. Face-to-face and telephone interviews organized around a semi-structured interview guide among students and staff of the institution were adopted. Data collected were thematically analyzed, and the findings revealed five importance of PAC deployment in the institution. The importance identified include "*prevent unwanted premise access or intrusions,*" "*prevent disruptions to university/staff operations on campus,*" "*protect students and staffs from outside intruders,*" "*limit movements during and after business hours*" and "*protect inventory and equipment from theft or misuse (decrease liability and risk associated with stolen or misused equipment).*" The study further revealed seven vulnerabilities in deploying PAC in the institution. The vulnerabilities identified are "*tailgating,*" "*delay in emergent cases,*" "*a power outage may affect its usage,*" "*security men* *have to monitor its usage," "human trafficking," "students/staff give their cards out/misplacing ID cards" and "malfunctioning of most of the physical access control devices."* The study offers both theoretical and practical implications. For theory, the study provides a novel contribution to deploying PAC systems in university settings in Ghana. The study provides relevant findings helpful to policymakers, stakeholders and practitioners to formulate planning and design recommendations for university settings. From the study's practical outlook, the outcome provides a valuable and readily available reference for university campus stakeholders, in this case, including the Campus Planning Office, Physical Plant, the Security Services Department, Central Administration – and the planners and urban designers. This gives policymakers a benchmark in PAC in university campus settings. The study also informs university stakeholders about improving the university campus in several other ways. From the findings of the study, it is recommended that the PAC systems should be provided with features that allow entry only via biometrics. Measures should also be implemented to ensure that entry through an access control barrier can be made only once within a time frame. Secondary systems must be put in place to ensure that scanners can passively regulate and observe all individuals that use the system. Lastly, updates and maintenance must be performed on the systems to ensure that they remain invulnerable and impenetrable. Though this study was conducted within Ghana, the findings and implications of this study can be helpful to policymakers, stakeholders and practitioners in other developing countries worldwide. This study has focused on the importance and vulnerabilities in deploying the PAC system in the university setting. However, strategies to improve upon the deployment of PACs were not explored. Further studies should explore the strategies for making the deployment of PAC efficient. Further research into the causes and effects of crime in university settings should also be conducted to understand a safe environment fully. Other areas for research include the social aspects of making the university community a better place for all stakeholders.

References

Adu, V., Adane, M.D. and Lartey, Y.N. (2022), *Ensuring Effective Secure Learning Environment Using Authentication System in Terms of Cost and Time at Kumasi*, Technical University, Ghana.

Agyekum, K., Kukah, A.S. and Amudjie, J. (2021), "The impact of COVID-19 on the construction industry in Ghana: the case of some selected firms", *Journal of Engineering, Design and Technology*, Vol. 20 No. 1, pp. 222-244.

Aldowah, H., Ul Rehman, S. and Umar, I. (2018), "Security in internet of things: issues, challenges and solutions", *International conference of reliable information and communication technology*, Springer, Cham, pp. 396-405.

Azimi, S. and O'Brien, W. (2022), "Fit-for-purpose: Measuring occupancy to support commercial building operations: a review", *Building and Environment*, Vol. 215 No. 3, 108767.

Best, C. and Nelson, J. (2020), "Access control", *The Professional Protection Officer*, Butterworth-Heinemann, Oxford, pp. 165-173.

Bigelow Stephen, J. (2008), "Implement access control systems successfully in your organization", (accessed on November, 2022).

Blackler, E. (2022), How does access controls for schools work? (Simple Guide), available at: https://blog.nortechcontrol.com/access-control-for-schools (accessed November 2022).

Bowers, D.M. (2013), *Access Control and Personal Identification Systems*, Butterworth-Heinemann, Oxford.

Castleberry, A. and Nolen, A. (2018), "Thematic analysis of qualitative research data: is it as easy as it sounds?", *Currents in Pharmacy Teaching and Learning*, Vol. 10 No. 6, pp. 807-815.

Charmaz, K. (2006), *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*, Sage, Los Angeles.

Cheng, S.Y., Wang, C.J., Shen, A.C.T. and Chang, S.C. (2020), "How to safely reopen colleges and universities during COVID-19: experiences from Taiwan", *Annals of Internal Medicine*, Vol. 173 No. 8, pp. 638-641.

Chinnasamy, P. and Deepalakshmi, P. (2022), "HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 13, pp. 1001-1019.

Crowe, T. (2000), *Crime Prevention through Environmental Design*, Butterworth-Heinemann, Oxford.

Dlamini, N. and Olanrewaju, O.A. (2021), "An investigation into campus safety and security", *11th Annual International Conference on Industrial Engineering and Operations Management Singapore.*

Duflo, E., Dupas, P. and Kremer, M. (2019), "The impact of free secondary education: experimental evidence from Ghana".

Ebregt, A. and Greve, P.D. (2000), *Buffer Zones and Their Management: Policy and Best Practices for Terrestrial Ecosystems in Developing Countries*, Theme Studies Series, Netherlands).

Floridi, L., Holweg, M., Taddeo, M., Amaya Silva, J., Mökander, J. and Wen, Y. (2022), "CapAI-A procedure for conducting Conformity Assessment of AI systems in line with the EU Artificial Intelligence act", available at: SSRN 4064091.

Holstein, D., Adamiak, M. and Falk, H. (2022), "Cybersecurity integration with IEC 61850 systems", *IEC 61850 Principles and Applications to Electric Power Systems*, Springer International Publishing, Cham, pp. 131-165.

Hu, V.C., Ferraiolo, D. and Kuhn, D.R. (2006), *Assessment of Access Control Systems*, US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD.

Hu, V.C., Ferraiolo, D.F. and Kuhn, D.R. (2019), *Attribute Considerations for Access Control Systems*, NIST Special Publication, Gaithersburg, Vol. 800, p. 205.

Hutter, D. (2016), *Physical Security and Why it Is Important*, SANS Institute Information Security Reading Room, pp.1-31.

Iloma, D.O., Nnam, M.U., Effiong, J.E., Eteng, M.J., Okechukwu, G.P. and Ajah, B.O. (2022), "Exploring socio-demographic factors, avoiding being a victim and fear of crime in a Nigerian university", *Security Journal*, Vol. 36 No. 1, pp. 1-20.

Jennings, W.G., Gover, A.R. and Pudrzynska, D. (2007), "Are institutions of higher learning safe? A descriptive study of campus safety issues and self-reported campus victimization among male and female college students", *Journal of Criminal Justice Education*, Vol. 18 No. 2, pp. 191-208.

Karp, A.H., Haury, H. and Davis, M.H. (2010), "From ABAC to ZBAC: the evolution of access control models", *Journal of Information Warfare*, Vol. 9 No. 2, pp. 38-46.

Kiger, M.E. and Varpio, L. (2020), "Thematic analysis of qualitative data: AMEE Guide No. 131", *Medical Teacher*, Vol. 42 No. 8, pp. 846-854.

Laan, J.H. (2021), *Incremental verification of physical access control systems", Master's thesis*, University of Twente, Enschede.

Lebea, K. (2020), *Context-driven Authentication in Physical Access Control Environments*, Doctoral dissertation, University of Johannesburg, Johannesburg.

Lester, J.N., Cho, Y. and Lochmiller, C.R. (2020), "Learning to do qualitative data analysis: a starting point", *Human Resource Development Review*, Vol. 19 No. 1, pp. 94-106.

Masoumzadeh, A., van der Laan, H. and Dercksen, A. (2022), "BlueSky: physical access control: Characteristics, challenges, and research Opportunities", *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*, pp. 163-172.

Mrozla, T. (2022), "On and off campus: examining fear of crime in a rural college town", *Journal of Criminal Justice Education*, Vol. 33 No. 1, pp. 23-40.

Nelson, J. (2020), "Access control and biometrics", *Handbook of Loss Prevention and Crime Prevention*, Butterworth-Heinemann, Oxford, pp. 239-249.

Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A. and Arshad, H. (2022), "The internet of things security: a survey encompassing unexplored areas and new insights", *Computers and Security*, Vol. 112, 102494.

Oriyano, S. (2014), "Physical security", *Cehv8: Certified Ethical Hacker Version 8 Study Guide*, Wiley, Indianapolis, IN USA, pp. 393-409.

Ouaddah, A., Elkalam, A.A. and Ouahman, A.A. (2017), "Towards a novel privacy-preserving access control model based on blockchain technology in IoT", *Europe and MENA Cooperation Advances in Information and Communication Technologies*, Springer, Cham, pp. 523-533.

Parse, R.R. (1990), "Parse's research methodology with an illustration of the lived experience of hope", *Nursing Science Quarterly*, Vol. 3 No. 1, pp. 9-17.

Pillay, H.L., Singh, J.S.K. and Chan, B. (2022), "Innovative activity in SMEs: critical success factors to achieve sustainable business growth", *Marketing I Menedžment Innovacij*, No. 2, pp. 31-42.

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S. and Fang, B. (2020), "A survey on access control in the age of the internet of things", *IEEE Internet of Things Journal*, Vol. 7 No. 6, pp. 4682-4696.

Reddy, D.N., Mahadev, B., Achyuth, K.V. and Nageswaran, S. (2018), "Development of security system to prevent tail-gating", *2018 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, pp. 0966-0969.

Rouhani, S., Pourheidari, V. and Deters, R. (2018), "Physical access control management system based on permissioned blockchain", *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, pp. 1078-1083.

Salahdine, F. and Kaabouch, N. (2019), "Social engineering attacks: a survey", *Future Internet*, Vol. 11 No. 4, p. 89.

Sodiya, A.S., Onashoga, S.A., Rosanwo, O.D. and Lawal, B.H. (2010), "MANAGING ICT INFRASTRUCTURE IN HIGHER EDUCATIONAL INSTITUTIONS", *College of Natural Sciences Proceedings*, pp. 60-67.

Velasco, T. (2022), *The Effects of College Desegregation on Academic Achievement and Students' Social Interactions: Evidence from Turnstile Data*, Columbia University Job Market Paper, New York.

Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A. and Malli, M. (2020), "Cyber-physical systems security: limitations, issues and future trends", *Microprocessors and Microsystems*, Vol. 77, 103201.

Yin, R.K. (2014), *Case Study Research: Design and Methods*, 5th ed., Sage, Thousand Oaks, CA.

Corresponding author
Kofi Agyekum can be contacted at: agyekum.kofi1@gmail.com, kagyekum.cap@knust.edu.gh