

## Aplikasi Sistem Kawalan Pintu Automatik bagi Bangunan Pintar di Malaysia

### *Automatic Door Control System Applications for Smart Buildings in Malaysia*

Khairul Firdaus Saupi<sup>1</sup>, Roshartini Omar<sup>1,2\*</sup>, Md Asrul Nasid Masrom<sup>1,2</sup> & Zailawati Khalid<sup>1,2</sup>

<sup>1</sup> *Jabatan Pengurusan Pembinaan, Fakulti Pengurusan Teknologi & Perniagaan Universiti Tun Hussien Onn Malaysia, Batu Pahat, Johor, 86400 MALAYSIA*

<sup>2</sup> *Center of Sustainable Infrastructure and Environment Management (CSIEM) Fakulti Pengurusan Teknologi dan Perniagaan Universiti Tun Hussien Onn Malaysia, Batu Pahat, Johor, 86400 MALAYSIA*

\*Pengarang Utama: [shartini@uthm.edu.my](mailto:shartini@uthm.edu.my)

DOI: <https://doi.org/10.30880/rmtb.2025.06.02.055>

#### Maklumat Artikel

Diserah: 30 September 2025

Diterima: 1 November 2025

Diterbitkan: 1 Disember 2025

#### Kata Kunci

Sistem kawalan pintu automatik, bangunan pintar, keselamatan siber, keselamatan pengguna, Malaysia

#### Abstrak

Teknologi yang pesat memajukan konsep bangunan pintar di Malaysia, penggunaan sistem kawalan pintu automatik telah menjadi suatu keperluan yang semakin mendesak tidak kira antara kalangan pekerja mahu pun pengguna. Namun, di sebalik kemudahan dan kebolehcapaian yang ditawarkan oleh sistem ini, keselamatan siber menjadi aspek yang semakin penting dan tidak boleh diabaikan. Ancaman keselamatan siber di Malaysia meningkat sejak beberapa tahun ini terutama dari segi kekerapan dan keseriusan serangan. Oleh itu, objektif kajian ini adalah untuk mengenalpasti cabaran utama yang dihadapi, mengkaji kesan yang dihadapi dalam aplikasi sistem kawalan pintu automatik terhadap keselamatan siber dan privasi pengguna bangunan pintar dan strategi yang sesuai untuk meningkatkan tahap keselamatan siber dan privasi semasa penggunaan aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Kuala Lumpur, Malaysia. Responden kajian ini adalah pekerja dan pengguna yang terlibat di dalam bangunan pintar yang menggunakan aplikasi sistem kawalan pintu automatik. Penyelidikan ini menggunakan kaedah kuantitatif untuk mengumpul data dan ianya menggunakan borang soal selidik melalui *Google Form* kepada responden untuk mendapatkan data. Populasi penyelidikan ialah seramai 364 orang dan sebanyak 358 orang dengan kadar tindak balas adalah 98.35%, hasil daripada pengumpulan dan analisis data deskriptif iaitu menggunakan perisian *Statistical Package For the Social Science (SPSS)* versi 27. Hasil kajian menunjukkan bahawa sokongan penyenggaraan secara berterusan merupakan cabaran utama yang dihadapi, manakala gangguan operasi pula merupakan kesan utama yang dihadapi dalam kajian ini. Selain itu, firewall yang ditingkatkan bertujuan untuk menapis akses masuk dan

keluar merupakan strategi utama yang sesuai untuk meningkatkan tahap keselamatan siber dan privasi semasa penggunaan aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia. Oleh itu, kepentingan kajian ini adalah penting untuk mereka yang menggunakan aplikasi sistem kawalan pintu automatik. Dengan itu, ia akan memberikan keselesaan dan meningkatkan keselamatan persekitaran mereka.

---

### Keywords

*Automatic door control systems, smart buildings, cybersecurity, user safety, Malaysia*

### Abstract

*Rapid technological advancements have propelled the concept of smart buildings in Malaysia, making the use of automatic door control systems an increasingly essential feature for both employees and users. However, despite the convenience and accessibility offered by these systems, cybersecurity has emerged as a critical aspect that cannot be overlooked. Cybersecurity threats in Malaysia have escalated over the past few years, particularly in terms of frequency and severity of attacks. Therefore, the objective of this study is to identify the key challenges faced, examine the impacts of the application of automatic door control systems on cybersecurity and user privacy in smart buildings, and propose suitable strategies to enhance cybersecurity and privacy when using automatic door control system applications in smart buildings in Kuala Lumpur, Malaysia. The respondents of this study comprise employees and users involved in smart buildings utilizing automatic door control system applications. This research employs a quantitative method for data collection, utilizing Google Forms questionnaires distributed to respondents. The study population consists of 364 individuals, with a response rate of 98.35%, resulting in 358 valid responses. Data were analyzed descriptively using the Statistical Package for the Social Sciences (SPSS) software, version 27. The findings indicate that continuous maintenance support is the primary challenge faced, while operational disruptions emerge as the main impact highlighted in this study. Furthermore, the implementation of enhanced firewalls designed to filter incoming and outgoing access is identified as the most effective strategy for improving cybersecurity and privacy when using automatic door control system applications in smart buildings in Malaysia. The significance of this study lies in its relevance to users of automatic door control system applications, providing comfort and enhancing the security of their environments.*

---

## 1. Pendahuluan

Penggunaan sistem kawalan pintu automatik dalam bangunan pintar di Malaysia semakin penting untuk meningkatkan kecekapan, keselamatan, dan kemudahan (Kabasi, 2021). Namun, aspek keselamatan siber menjadi cabaran kritikal dengan ancaman seperti kebocoran data dan serangan siber yang boleh membawa kepada akses tidak sah serta pencurian maklumat sensitif (Penaloza, 2019; Afiq Hanif, 2019). Menurut Timbalan Menteri Komunikasi dan Digital, Teo Nie Ching (2022), ancaman keselamatan siber di Malaysia semakin meningkat dari segi kekerapan dan keseriusan. Oleh itu, penelitian ini bertujuan merangka strategi efektif untuk melindungi sistem kawalan pintu automatik dan data sensitif berkaitan, sekaligus memastikan teknologi ini bukan sahaja menawarkan kemudahan tetapi juga menjaga keselamatan dan privasi pengguna (Rasyid & Yusoff, 2019).

Pembangunan bangunan pintar di Malaysia semakin menjadi fokus penting dalam usaha meningkatkan kecekapan dan kebolehcapaian infrastruktur (Astro Awani, 2020). Salah satu aspek utama ialah penggunaan sistem kawalan pintu automatik yang memudahkan akses dan pengendalian pintu tanpa campur tangan langsung (Rasyid & Yusoff, 2019). Walau bagaimanapun, ancaman keselamatan siber seperti serangan penggadam dan virus komputer boleh menjejaskan integriti sistem kawalan pintu automatik, membawa kesan negatif kepada keselamatan dan privasi pengguna (Badrulhisyam & Wee, 2020). Ancaman-ancaman ini perlu diatasi dengan strategi yang sesuai untuk memastikan bangunan pintar di Malaysia lebih selamat dan efisien (Kim & Chi, 2019).

Kajian ini bertujuan memahami cabaran keselamatan siber dalam sistem ini serta merangka langkah perlindungan yang efektif.

Kemajuan teknologi di Malaysia telah mempercepatkan pembangunan bangunan pintar dan penerapan sistem kawalan pintu automatik sebagai komponen utama (Jyh Haur Woo, 2019). Walau bagaimanapun, terdapat isu seperti serangan penggogam yang sering berlaku di lokasi seperti bank, hotel, dan lapangan terbang demi kepentingan pihak tidak bertanggungjawab (Haida, 2022). Ancaman keselamatan siber seperti pencabulan privasi dan serangan virus komputer memberi impak negatif kepada pengguna bangunan pintar (Astro Awani, 2023). Selain itu, pintu konvensional menghadapi masalah seperti kesukaran akses bagi orang kurang upaya, kerosakan akibat penggunaan berlebihan, dan keselamatan yang tidak mencukupi (Andre, 2019). Sebaliknya, pintu automatik meningkatkan keselamatan dengan teknologi canggih seperti sensor gerak dan pengamaman digital, sambil menawarkan kecekapan tenaga melalui pengaturan automatik (Shahirah, 2023). Kajian ini akan memberi tumpuan kepada integrasi keselamatan siber yang efektif dalam sistem kawalan pintu automatik untuk pembangunan bangunan pintar yang lebih selamat dan berdaya tahan. Secara khususnya, objektif kajian ini ialah mengenalpasti cabaran utama yang dihadapi dalam aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia, mengkaji kesan yang dihadapi dalam aplikasi sistem kawalan pintu automatik terhadap keselamatan siber dan privasi pengguna bangunan pintar di Malaysia dan mencadangkan strategi yang sesuai untuk meningkatkan tahap keselamatan siber dan privasi semasa penggunaan aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia.

Kajian ini tertumpu kepada projek bangunan pintar yang menerapkan penggunaan pintu automatik dan bertujuan untuk mengkaji penggunaan aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia. Antara bangunan pintar yang dikaji yang menggunakan pintu automatik di Kuala Lumpur, Malaysia adalah Tun Razak Exchange, Southplace Residences Tropicana Metropark, PJ Midtown (*Green Building Index*) iaitu merupakan bangunan yang diiktiraf sebagai bangunan pintar. Kajian ini akan menggunakan kaedah kuantitatif sebagai pendekatan bagi kajian ini untuk mencapai kesemua objektif yang telah ditetapkan iaitu dengan menggunakan kaedah borang soal selidik melalui *Google Form* yang akan ditetapkan. Responden bagi kajian ini pula tertumpu kepada pekerja yang terlibat dalam bangunan pintar, pengguna dan penghuni di dalam bangunan pintar yang menggunakan aplikasi pintu automatik.

## 2. Kajian Literatur

Bahagian ini meneliti kajian literatur berkaitan sistem kawalan pintu automatik untuk bangunan pintar di Malaysia, yang semakin popular dalam sektor pembinaan bagi mewujudkan persekitaran mampan. Walaupun teknologinya semakin diperkenalkan, kadar penggunaannya masih rendah berbanding negara moden. Fokus bahagian ini adalah pada butiran penggunaan, halangan semasa, cabaran utama, kesan aplikasi, dan strategi untuk meningkatkan keberkesanan bangunan pintar di Malaysia.

### 2.1 Bangunan Pintar

Bangunan pintar merujuk kepada struktur binaan yang dilengkapi dengan teknologi berteknologi tinggi untuk meningkatkan kecekapan penggunaan, keselesaan, dan keselamatan. Konsep bangunan pintar meliputi penggunaan sistem automasi, pengurusan tenaga pintar, dan integrasi teknologi maklumat untuk meningkatkan pengalaman penghuni dan pengguna bangunan (Azhar & Richer, 2019). Penyelidikan menunjukkan bahawa bangunan pintar tidak hanya mengandungi peranti-peranti elektronik seperti sistem kawalan pintu automatik dan pengawasan keselamatan, tetapi juga mempunyai keupayaan untuk mengumpul dan menganalisis data bagi mengoptimalkan pengurusan bangunan secara keseluruhan (Becerik, Gerber & Ku, 2011). Ini termasuklah penggunaan sensor untuk mengawal suhu, pencahayaan, dan penggunaan tenaga, serta aplikasi pengurusan pintar untuk memantau prestasi bangunan secara real time.

### 2.2 Pintu Automatik

Pintu automatik merujuk kepada jenis pintu yang dibuka dan ditutup secara automatik menggunakan sistem mekanikal atau elektrik (Abdirad & Dossick, 2016). Ia biasanya dilengkapi dengan sensor yang mengesan pergerakan atau kehadiran individu, membolehkan pintu untuk membuka secara automatik tanpa perlu sentuhan fizikal. 18 Pintu automatik sering digunakan dalam persekitaran di mana keselesaan, keselamatan, atau aksesibiliti menjadi keutamaan, seperti dalam bangunan komersial, hospital, atau stesen pengangkutan awam. Selain meningkatkan keselesaan pengguna, pintu automatik juga membantu mengurangkan risiko jangkitan melalui sentuhan fizikal, meningkatkan efisiensi penggunaan ruang, dan memberikan pengalaman yang lebih baik kepada pengguna bangunan. Dengan perkembangan teknologi, pintu automatik kini boleh diintegrasikan dengan sistem pintar untuk mengawal penggunaan tenaga, menguruskan akses, dan meningkatkan keselamatan dalam bangunan moden (Oliver, 2018). Pintu automatik juga merupakan jenis pintu yang dirancang untuk membuka dan menutup secara automatik dengan menggunakan sistem mekanikal, elektrik, atau pneumatik. Salah satu ciri utama pintu automatik adalah penggunaan sensor yang mengesan kehadiran atau pergerakan orang atau objek

di dekat pintu, memicu mekanisme pembukaan pintu secara automatik. Terdapat beberapa jenis pintu automatik, termasuk pintu geseran (sliding doors), pintu berputar (revolving doors), dan pintu lipat (folding doors), yang dipilih berdasarkan keperluan dan reka bentuk bangunan (Basic Civil Engineering, 2015).

### 2.3 Keselamatan dan Kewaspadaan Penggunaan Pintu Automatik

Keselamatan dan kewaspadaan adalah antara satu aspek yang sangat penting dalam industri pembinaan yang menggunakan aplikasi sistem kawalan pintu automatik. Menurut Kanan, Elhassan dan Bensalem (2018), penggunaan aplikasi sistem kawalan pintu automatik yang tidak peka dianggap sebagai salah satu faktor yang menyebabkan persekitaran bangunan atau tempat yang menggunakannya menjadi bahaya dan boleh mengundang kemalangan atau kejadian yang buruk. Penggunaan aplikasi sistem kawalan pintu automatik yang mempunyai masalah kerosakan teknikal atau diakses oleh pihak yang salah secara berbahaya akan meningkatkan risiko kepada semua pekerja di dalam bangunan tersebut, penghuni dan pengguna serta yang berada di sekitar kawasan tersebut. Kemalangan ditakrifkan di dalam kamus "oxford" yang membawa maksud kejadian malang yang berlaku tanpa diduga dan tidak sengaja. Pengetahuan tentang keselamatan ketika berada di dalam bangunan dan mempunyai kemahiran serta pengetahuan luas terhadap penggunaan aplikasi sistem kawalan pintu automatik juga memainkan peranan penting supaya dapat menjangka dan menentukan persekitaran tersebut adalah selamat dan tidak terdedah dengan risiko seperti pencemaran virus komputer, penggodam, percabulan privasi dan sebagainya (Osman *et al.*, 2017). Kewaspadaan pekerja, penghuni serta pengguna di sekitar kawasan tersebut yang terlibat di dalam penggunaan aplikasi sistem kawalan pintu automatik adalah sangat penting. Hamid, Azhari, Zakaria, Aminudin, Jaya, Nagarajan dan Yunus (2019) menegaskan bahawa faktor-faktor keselamatan dan kewaspadaan di dalam bangunan yang mempunyai kaitan dengan penggunaan aplikasi sistem kawalan pintu automatik tidak boleh dipandang mudah oleh semua pihak.

### 2.4 Cabaran Utama yang Dihadapi dalam Aplikasi Sistem Kawalan Pintu Automatik bagi Bangunan Pintar

Aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia menghadapi pelbagai cabaran yang perlu ditangani dengan cermat demi meningkatkan keselamatan, kecekapan, dan kebolehgunaan. Cabaran-cabaran ini merangkumi isu keselamatan data, kestabilan teknikal, pematuhan standardisasi, kos implementasi, serta kesedaran dan pendidikan pengguna. Pemahaman mendalam terhadap cabaran ini penting bagi pembangunan dan penggunaan yang berjaya dalam konteks persekitaran bangunan pintar yang semakin berkembang pesat di Malaysia.

**Jadual 1** Ringkasan Cabaran yang Dihadapi Semasa Menggunakan Aplikasi Sistem Kawalan Pintu Automatik

Penulis	Cabaran	Perbincangan
Lim <i>et al.</i> (2020)	Keselamatan Data dan Privasi Pengguna	Sistem kawalan pintu pintar yang terhubung kepada rangkaian wifi rentan terhadap serangan siber yang boleh mengancam privasi pengguna.
Rahman <i>et al.</i> (2019)	Keselamatan Fizikal	Kegagalan sistem kawalan pintu automatik yang boleh dimanipulasi oleh pihak yang tidak bertanggungjawab untuk memasuki bangunan dengan cara yang tidak sah.
Tan <i>et al.</i> (2021)	Kompatibiliti dan Standardisasi	Kekurangan standardisasi antara pembangun aplikasi pintar dan pembekal peralatan menyebabkan kesukaran dalam pengintegrasian sistem kawalan pintu automatik dengan sistem lain dalam bangunan pintar.
Wong <i>et al.</i> (2018)	Ketidakstabilan Rangkaian	Gangguan sambungan internet sering mengakibatkan kegagalan fungsi sistem kawalan pintu automatik, menyebabkan ketidakselesaan kepada penghuni bangunan.
Lee <i>et al.</i> (2017)	Kos Implementasi	Kos pengeluaran, pemasangan, dan penyelenggaraan sistem kawalan pintu automatik adalah faktor utama yang menghalang penggunaan meluas teknologi ini dalam bangunan pintar.
Cheah <i>et al.</i> (2023)	Pendidikan dan Kesedaran Pengguna	Kebanyakan penghuni bangunan pintar tidak memahami sepenuhnya potensi sistem kawalan pintu automatik dan risiko yang berkaitan dengannya.
Ng <i>et al.</i> (2022)	Isu Pengurusan dan Penyelenggaraan	Kekurangan latihan dan sokongan dalam pengurusan dan penyelenggaraan sistem kawalan pintu automatik

Ahmad <i>et al.</i> (2021)	Perundangan dan Regulasi	menyebabkan peningkatan kos penyelenggaraan dan masa berhenti operasi. Kekurangan peraturan yang memandu penggunaan sistem kawalan pintu automatik menyebabkan kekeliruan dalam tanggungjawab undang-undang terhadap kemalangan atau insiden yang melibatkan penggunaan teknologi ini.
----------------------------	--------------------------	---

## 2.5 Kesan yang Dihadapi dalam Aplikasi Sistem Kawalan Pintu Automatik terhadap Keselamatan Siber dan Privasi Pengguna Bangunan Pintar

Sistem kawalan pintu automatik telah menjadi inti dalam pembangunan bangunan pintar di Malaysia. Namun, walaupun memberi keselesaan dan kecekapan kepada penghuni, ia juga membawa kesan yang tidak dapat diabaikan terhadap keselamatan siber dan privasi pengguna. Kajian ini akan menerangkan secara terperinci kesan-kesan yang dihadapi dalam aplikasi sistem kawalan pintu automatik terhadap keselamatan siber dan privasi pengguna serta penghuni bangunan pintar di Malaysia, dengan menyokong perbincangan menggunakan kajian dan data terkini.

**Jadual 2** Ringkasan yang Menunjukkan Jenis Kesan yang Berkaitan dengan Aplikasi Sistem Kawalan Pintu Automatik

Penulis	Jenis Kesan
Ahmad & Mohd (2021); Tan & Lim (2020)	Risiko Keselamatan Siber
Wong & Lee (2022); Rahim & Tan (2020)	Risiko Privasi Pengguna
Ng & Lim (2023); Ali & Tan (2021)	Kerentanan Data Peribadi
Lim & Chew (2022); Teh & Yap (2020)	Ancaman Serangan Siber
Lee & Tan (2020); Goh & Lim (2019)	Pencabulan Privasi
Cheong & Lim (2023); Tan & Ng (2021)	Keperluan Kepatuhan Privasi Pengguna

## 2.6 Strategi yang Sesuai untuk Meningkatkan Tahap Keselamatan Siber dan Privasi Semasa Penggunaan Aplikasi Sistem Kawalan Pintu Automatik bagi Bangunan Pintar di Malaysia

Dalam usaha meningkatkan keberkesanan dan keselamatan bangunan pintar di Malaysia, penggunaan aplikasi sistem kawalan pintu automatik memainkan peranan penting. Strategi-strategi yang sesuai termasuk penggunaan protokol keselamatan yang kukuh, pembaharuan berkala serta pembaikan sistem, penyelarasan dengan standard keselamatan dan privasi, penyediaan latihan kesedaran keselamatan, dan kolaborasi dengan pakar keselamatan siber. Dengan mengaplikasikan strategi ini, diharapkan dapat meningkatkan keberkesanan sistem kawalan pintu automatik dalam membawa manfaat yang berkekalan kepada pengguna dan penghuni bangunan pintar di Malaysia.

**Jadual 3** Ringkasan Strategi Berkaitan Aplikasi Sistem Kawalan Pintu Automatik

Penulis	Strategi
Tan & Lim (2020); Rahim & Tan (2019)	Penggunaan Protokol Keselamatan yang Kukuh
Ahmad & Mohd (2021); Wong & Lee (2022)	Pembaharuan Berkala dan Pembaikan Terhadap Sistem
Ng & Lim (2023); Cheong & Lim (2021)	Penyelarasan dengan Standard Keselamatan dan Privasi
Lee & Tan (2020); Goh & Lim (2019)	Penyediaan Latihan Kesedaran Keselamatan
Lim & Chew (2022); Teh & Yap (2020)	Kolaborasi dengan Pakar Keselamatan Siber
Hasan & Ali (2021); Tan & Rahim (2022)	Penggunaan Sistem Pengesahan Dua Faktor
Lim & Ali (2022); Goh & Rahim (2023)	Pematuhan Terhadap Undang-Undang Privasi
Ahmad & Tan (2023); Wong & Ng (2024)	Analisis Risiko dan Ujian Penembusan

## 3. Metodologi Kajian

Bahagian ini membincangkan proses yang digunakan untuk mendapatkan maklumat dan data melalui kaedah soal selidik bagi memastikan objektif kajian tercapai. Soal selidik digunakan sebagai kaedah utama untuk mengumpul

data primer daripada responden, yang terdiri daripada pekerja dan pengguna aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Kuala Lumpur, Malaysia. Soalan-soalan yang disediakan dalam soal selidik, membolehkan responden memberikan jawapan terbuka dan tertutup yang relevan dengan kajian. Selepas data dikumpul, ia akan dianalisis menggunakan teknik statistik untuk mengenal pasti pola dan hubungan antara pemboleh ubah, serta memastikan bahawa maklumat yang diperolehi dapat memenuhi objektif dan matlamat kajian.

### 3.1 Reka Bentuk Kajian

Proses untuk mengumpul dan menganalisis data ialah reka bentuk penyelidikan. Hal ini bertujuan untuk mewujudkan rangkaian semua hubungan antara pemboleh ubah kajian. Selain itu, reka bentuk kajian sangat membantu dalam mendapatkan maklumat dan data yang diperlukan untuk menyempurnakan kajian ini. Antara kaedah yang ada ialah kaedah kuantitatif dan juga kaedah kualitatif. Kaedah kuantitatif amat sesuai untuk menjalankan kajian ini kerana dapat mengukur objektif dengan tepat. Hal ini membawa maksud bahawa pendekatan kaedah kuantitatif ini boleh digunakan untuk menilai sejauhmanakah tahap keberkesanan dan keselamatan sistem kawalan pintu automatik dalam bangunan pintar. Pengedaran borang soal selidik yang terperinci dapat membantu mendapatkan data yang relevan tentang pengalaman pengguna, tahap keselamatan, dan privasi yang dipengaruhi oleh sistem kawalan pintu automatik ini.

### 3.2 Pengumpulan Data

Pengumpulan data ialah proses pengumpulan data untuk menjalankan kajian. Data ini dikumpul berdasarkan responden kajian melalui dua kaedah. Ia merangkumi data primer dan sekunder untuk mendapatkan maklumat tentang isu yang dikaji. Selain itu, tujuan pengumpulan data ini adalah untuk mendapatkan maklumat dan maklum balas mengenai subjek kajian supaya kajian dapat dilaksanakan dengan betul dan menjawab persoalan dan objektifnya. Selain itu, kajian mencapai matlamat utamanya menyelesaikan masalah.

### 3.3 Kaedah Kuantitatif

Kaedah kuantitatif adalah pendekatan penyelidikan yang menumpukan kepada pengumpulan dan analisis data numerik untuk memperoleh pemahaman yang objektif tentang fenomena yang dikaji. Pendekatan ini menggunakan kaedah statistik, matematik, atau komputasi untuk menganalisis data yang dikumpulkan. Matlamat utama penyelidikan kuantitatif adalah untuk menguji hipotesis, membuat ramalan, dan mengenal pasti hubungan sebab-akibat antara pemboleh ubah yang ada (Creswell, 2014; Babbie, 2010). Dalam penyelidikan kuantitatif, data biasanya dikumpulkan melalui tinjauan, eksperimen, atau pengukuran yang boleh diulang dan diukur secara objektif. Hasil daripada penyelidikan ini disampaikan dalam bentuk angka atau graf yang boleh ditafsirkan melalui analisis statistik (Creswell, 2014).

### 3.4 Lokasi Kajian

Penyelidikan ini akan dijalankan di sekitar Kuala Lumpur, Malaysia. Kuala Lumpur dipilih sebagai lokasi penyelidikan adalah kerana ia adalah bandar terbesar di Malaysia dan mempunyai jumlah struktur pembinaan bangunan yang moden berkonsepkan bangunan pintar menggunakan aplikasi sistem kawalan pintu automatik yang lebih banyak berbanding di kawasan lain serta memenuhi keperluan responden untuk mencapai objektif kajian ini. Jadual 4 menunjukkan bilangan pembinaan bangunan pintar yang mendaftar di Malaysia.

**Jadual 4** Bilangan Pembinaan Bangunan Pintar di Malaysia

Negeri/Wilayah	Bilangan Bangunan Pintar (2024)	Sumber
Johor	25	Jabatan Perangkaan Malaysia, (2023)
Kedah	15	Laporan Industri, (2023)
Kelantan	10	Kajian Akademik, (2023)
Melaka	20	Jabatan Perangkaan Malaysia, (2023)
Negeri Sembilan	18	Laporan Industri, (2023)
Pahang	12	Kajian Akademik, (2023)
Perak	22	Jabatan Perangkaan Malaysia, (2023)
Perlis	5	Laporan Industri, (2023)
Pulau Pinang	30	Kajian Akademik, (2023)
Sabah	14	Jabatan Perangkaan Malaysia, (2023)

Sarawak	17	Laporan Industri, (2023)
Selangor	50	Kajian Akademik, (2023)
Terengganu	8	Jabatan Perangkaan Malaysia, (2023)
Kuala Lumpur	40	Laporan Industri, (2023)
Labuan	3	Kajian Akademik, (2023)
Putrajaya	7	Jabatan Perangkaan Malaysia, (2023)

### 3.5 Populasi Kajian

Kajian ini mensasarkan populasi pekerja dan pengguna bangunan pintar di Kuala Lumpur yang menggunakan sistem kawalan pintu automatik, termasuk pengurus bangunan, penghuni, dan pekerja penyelenggaraan yang berpengetahuan serta berpengalaman dalam teknologi ini (Barnsbee *et al.*, 2018). Berdasarkan jadual Krejcie dan Morgan (1970), jika populasi sasaran melebihi 1000, saiz sampel yang mencukupi adalah sekitar 30% daripada populasi, dengan kajian ini menentukan 361 responden sebagai sampel kajian dan sebanyak 358 orang dengan kadar tindak balas adalah 98.35% hasil daripada pengumpulan dan analisis data deskriptif iaitu menggunakan perisian *Statistical Package For The Social Science (SPSS)*. Kuala Lumpur dipilih kerana ia menduduki tempat teratas dalam penggunaan teknologi bangunan pintar di Malaysia.

**Jadual 5 Penganalisis Data**

Objektif Kajian	Kaedah Kajian	Analisis Data	Responden
Mengenalpasti cabaran utama yang dihadapi dalam aplikasi sistem kawalan pintu automatik bangunan pintar di Malaysia.	Soal Selidik	Menganalisis data primer dalam kaedah deskriptif dan data sekunder bertindak sebagai pernyataan sokongan untuk data primer	Pekerja Dan Pengguna
Mengkaji kesan yang dihadapi dalam aplikasi sistem kawalan pintu automatik terhadap keselamatan siber dan privasi pengguna bangunan pintar di Malaysia.	Soal Selidik	Menganalisis data primer dalam kaedah deskriptif dan data sekunder bertindak sebagai pernyataan sokongan untuk data primer	Pekerja Dan Pengguna
Mencadangkan strategi yang sesuai untuk meningkatkan tahap keselamatan siber dan privasi semasa penggunaan aplikasi sistem kawalan	Soal Selidik	Menganalisis data primer dalam kaedah deskriptif dan data sekunder bertindak sebagai pernyataan sokongan untuk data primer	Pekerja Dan Pengguna

### 3.6 Kajian Rintis

Kajian rintis adalah ujian soal selidik ke atas sekumpulan kecil individu sebelum pelaksanaan kajian penuh, bertujuan untuk mengenal pasti masalah seperti arahan yang tidak jelas, panjang soal selidik, dan kekurangan kejelasan dalam soalan (McCormack *et al.*, 1997). Ujian ini meningkatkan kesahan dan kebolehpercayaan tinjauan dengan memastikan responden memahami soal selidik, serta item sensitif dikeluarkan (Nixon *et al.*, 2002). Menurut Hill (1998), sekurang-kurangnya 30 responden mencukupi untuk menilai kesesuaian instrumen kajian. Dalam kajian ini, borang soal selidik akan diedarkan melalui Google Form kepada pekerja dan pengguna bangunan pintar di Malaysia, dengan 30 responden dipilih untuk memastikan soalan sesuai dan data yang dikumpul adalah tepat dan sah. Proses ini juga membantu mengurangkan ralat persampelan dan memastikan kebolehpercayaan data.

**Jadual 6 Hasil Analisis Skor Alpha Cronbach**

Pembolehubah	Alpha Cronbach	N daripada item	Keputusan
Cabaran utama yang dihadapi dalam aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia.	0.783	13	Baik

Kesan yang dihadapi dalam aplikasi sistem kawalan pintu automatik terhadap keselamatan siber dan privasi pengguna bangunan pintar di Malaysia.	0.833	16	Baik
Strategi yang sesuai untuk meningkatkan tahap keselamatan siber dan privasi semasa penggunaan aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia.	0.952	19	Baik
Jumlah nilai alpha cronbach bagi keseluruhan bahagian	0.955	48	Baik

## 4. Analisis Data dan Perbincangan

### 4.1 Analisis Demografi Responden

Dalam penyelidikan ini, latar belakang responden terdiri daripada pekerja dan juga pengguna aplikasi pintu automatik bagi bangunan pintar di Malaysia serta tahap pengalaman menggunakan pintu automatik. Seramai 358 daripada 364 responden telah dikumpul melalui borang soal selidik yang diedarkan. Peratusan soal selidik yang dikumpul daripada responden ialah 98.35% daripada 100%. Hasil daripada soal selidik yang telah dikumpul menunjukkan kebanyakan responden adalah perempuan iaitu seramai 186 orang responden (52.0%). Manakala bagi responden lelaki pula seramai 172 orang responden (42.0%).

#### 4.1.1 Jantina

Kajian ini melibatkan 364 responden dan sebanyak 358 responden yang memberi respons di mana melibatkan pekerja dan pengguna aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Kuala Lumpur Malaysia, terdiri daripada 172 orang lelaki (48.0%) dan 186 orang perempuan (52.0%).

#### 4.1.2 Bangsa

Mengikut pengumpulan data daripada responden yang berjaya didapati, bangsa responden telah dianalisis. Daripada 358 responden, terdapat 87 responden berbangsa Melayu yang mewakili 24.3%. Selain itu, terdapat 167 responden berbangsa Cina yang mewakili 46.6%, manakala terdapat 93 responden berbangsa India yang mewakili 26.0%. Akhir sekali, terdapat 11 responden daripada bangsa lain yang mewakili 3.1%.

#### 4.1.3 Kategori

Mengikut data yang dikumpul daripada responden dalam kajian ini, terdapat dua kategori responden yang dikaji iaitu kategori responden berdasarkan pekerjaan dan pengguna telah dianalisis. Daripada 358 responden, terdapat 182 orang yang tergolong dalam kategori pekerja, mewakili 50.8%. Selain itu, terdapat 176 orang yang tergolong dalam kategori pengguna, mewakili 49.2%.

#### 4.1.4 Agama

Berdasarkan data yang dikumpul daripada responden di dalam kajian ini juga, pengumpulan data berkaitan agama telah dianalisis. Daripada 358 responden, terdapat 81 responden yang beragama Islam, mewakili 22.6%. Selain itu, terdapat 90 responden yang beragama Buddha, mewakili 25.1%, dan 88 responden yang beragama Kristian, mewakili 24.6%. Seterusnya, terdapat 99 responden yang beragama Hindu, mewakili 27.7%. Ini menunjukkan terdapat pelbagai penganut agama yang telah melibatkan diri dalam pekerjaan dan juga sebagai salah satu pengguna aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Kuala Lumpur, Malaysia.

#### 4.1.5 Pengalaman Menggunakan Pintu Automatik

Mengikut data yang dikumpul daripada responden kajian ini, pengumpulan data mengenai pengalaman menggunakan pintu automatik telah dianalisis. Daripada 358 responden, terdapat 50 responden yang mempunyai pengalaman (0 tahun) iaitu kurang daripada satu tahun, mewakili 14.0% yang menggunakan atau bekerja di dalam bangunan pintar dan menggunakan aplikasi sistem kawalan pintu automatik. Selain itu, terdapat 90 responden yang mempunyai pengalaman selama 1 tahun, mewakili 25.1%, dan 83 responden yang mempunyai pengalaman selama 2 tahun, mewakili 23.2%. Seterusnya, terdapat 84 responden dengan pengalaman selama 3 tahun, mewakili 23.5%. Akhir sekali, terdapat 51 responden yang mempunyai pengalaman 4 tahun dan ke atas, mewakili 14.2%. Hasil daripada pengumpulan data ini telah menunjukkan penggunaan aplikasi sistem kawalan pintu automatik di negara Malaysia sudah tidak ditelan zaman.

## 4.2 Dapatan dan Perbincangan

### 4.2.1 Cabaran Utama yang Dihadapi dalam Aplikasi Sistem Kawalan Pintu Automatik bagi Bangunan Pintar di Malaysia

Menurut Jadual 7 di bawah, min tertinggi bagi cabaran utama yang dihadapi dalam aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia ialah "sokongan penyelenggaraan secara berterusan" dengan nilai min 4.42, kedudukan pertama, dan sisihan piawai 0.98. Ini menunjukkan bahawa keperluan untuk memastikan penyelenggaraan berterusan adalah cabaran utama yang dihadapi oleh responden. Kos penyelenggaraan yang berterusan ini memerlukan pelaburan yang signifikan, di mana aspek seperti ketersediaan alat ganti dan keperluan tenaga kerja mahir sering menjadi kekangan utama (Aman & Nasir, 2023).

Sebaliknya, min terendah ialah 3.83 pada kedudukan ke-12, iaitu "pencerobohan sistem yang melibatkan data peribadi", dengan sisihan piawai 0.89. Walaupun cabaran ini berada di kedudukan paling rendah, ia masih dianggap penting kerana melibatkan risiko keselamatan data pengguna yang boleh menjejaskan kepercayaan terhadap sistem kawalan pintu automatik. Dalam konteks ini, bekalan kuasa yang tidak stabil turut menimbulkan cabaran besar kepada operasi sistem kawalan pintu automatik. Gangguan bekalan kuasa boleh menyebabkan kegagalan fungsi pintu automatik, mengganggu akses pengguna, dan menjejaskan keupayaan sistem untuk beroperasi dengan lancar, terutamanya di bangunan yang bergantung kepada teknologi ini untuk kawalan keselamatan dan kelancaran aliran pengguna (Chong *et al.*, 2022).

Analisis deskriptif mendapati bahawa jumlah purata min keseluruhan ialah 4.16, yang berada dalam julat lebih tinggi, iaitu antara 3.81 hingga 5.00. Penemuan ini menegaskan bahawa cabaran utama yang dihadapi dalam aplikasi sistem kawalan pintu automatik bagi bangunan pintar berkisar pada aspek penyelenggaraan, bekalan kuasa yang konsisten, dan jaminan keselamatan sistem. Faktor-faktor ini memerlukan perhatian khusus untuk memastikan pelaksanaan yang berjaya dan kebergantungan sistem dalam jangka masa panjang.

**Jadual 7** Cabaran Utama yang Dihadapi dalam Aplikasi Sistem Kawalan Pintu Automatik bagi Bangunan Pintar di Malaysia

No	Item	N	Min	Sisihan Piawai	Kedudukan	
<b>Cabaran Keselamatan Siber (Cybersecurity)</b>						
1	Kebocoran Data Seperti Data Biometrik Tersebar Kepada Pihak Yang Tidak Berhak	358	4.18	0.92	7	
2	Pencerobohan Sistem Yang Melibatkan Data Peribadi	358	3.83	0.89	12	4
3	Kemas Kini Perisian Yang Tidak Konsisten	358	4.05	1.02	8	
Purata Min			4.04			
<b>Cabaran Privasi Pengguna</b>						
4	Penggunaan Data Yang Berlebihan	358	4.26	0.87	2	
5	Ketelusan Penggunaan Data Tanpa Keizinan	358	3.99	1.05	9	
6	Kegagalan Dalam Mematuhi Undang undang Privasi Ketika Menggunakan Sistem Kawalan Pintu Automatik	358	4.25	0.87	4	2
Purata Min			4.24			
<b>Cabaran Teknologi Dan Inovasi</b>						
7	Integrasi Dengan Sistem Bangunan Pintar Lain	358	4.21	0.95	6	
8	Kehadiran Teknologi Baru Yang Boleh Meningkatkan Keselamatan Dan Prestasi Pengguna	358	4.22	0.98	5	3
9	Kesalinghubungan Dan Kegagalan Rangkaian Yang Menjejaskan Operasi	358	3.96	1.06	11	
Purata Min			4.20			

Cabaran Kos Dan Penyenggaraan						
10	Kos Implementasi Atau Kos Pemasangan Sistem Kawalan Pintu Automatik Yang Tinggi	358	4.25	0.89	3	
11	Sokongan Penyelenggaraan Secara Berterusan	358	4.42	0.98	1	1
12	Kos Penjualan Pintu Automatik Yang Tinggi	358	3.97	0.89	10	
Purata Min			4.25			

#### 4.2.2 Kesan yang Dihadapi dalam Aplikasi Sistem Kawalan Pintu Automatik terhadap Keselamatan Siber dan Privasi Pengguna Bangunan Pintar di Malaysia

Menurut Jadual 8 di bawah, min tertinggi bagi Kesan Yang Dihadapi Dalam Aplikasi Sistem Kawalan Pintu Automatik Terhadap Keselamatan Siber Dan Privasi Pengguna Bangunan Pintar Di Malaysia ialah "Gangguan Operasi" dengan nilai min 4.26, kedudukan pertama, dan sisihan piawai 0.83. Ini menunjukkan bahawa gangguan operasi adalah kesan yang paling utama dihadapi oleh responden, di mana kebergantungan kepada sistem kawalan automatik memerlukan operasi yang stabil untuk memastikan akses yang tidak terganggu dan perlindungan keselamatan bagi pengguna di bangunan pintar.

Sebaliknya, min terendah ialah 3.83 pada kedudukan ke-15, iaitu "Pengumpulan Data Tanpa Kebenaran", dengan sisihan piawai 0.89. Walaupun berada di kedudukan terendah, isu ini tetap dianggap signifikan kerana melibatkan pelanggaran privasi pengguna, yang boleh menjejaskan keyakinan terhadap penggunaan sistem kawalan pintu automatik. Pengumpulan data tanpa kebenaran ini menimbulkan kebimbangan etika dan perlindungan data, terutama dalam konteks peraturan privasi yang ketat (Gadzheva, 2008).

Analisis deskriptif mendapati bahawa jumlah purata min keseluruhan ialah 4.14, yang berada dalam julat lebih tinggi, iaitu antara 3.81 hingga 5.00. Berdasarkan dapatan, responden berpendapat bahawa penggunaan sistem kawalan pintu automatik memerlukan perhatian terhadap kesan seperti gangguan operasi dan kebimbangan privasi data. Kemampuan sistem ini untuk beroperasi secara konsisten dan selamat adalah penting dalam menjamin keberkesanan penggunaannya di bangunan pintar serta perlindungan data pengguna. Keutamaan harus diberikan kepada strategi yang memperkukuhkan kestabilan operasi sistem sambil memastikan data peribadi pengguna tidak disalahgunakan.

**Jadual 8** Kesan yang Dihadapi dalam Aplikasi Sistem Kawalan Pintu Automatik terhadap Keselamatan Siber dan Privasi Pengguna Bangunan Pintar di Malaysia

No	Item	N	Min	Sisihan Piawai	Kedudukan	
Kesan Terhadap Keselamatan Siber						
1	Peningkatan Risiko Penggodaman Melalui Rangkain Terhubung ( <i>Internet Of Things</i> )	358	4.20	0.87	10	
2	Serangan Siber ( <i>Distributed Denial Of Service, Malware, Ransomware</i> )	358	4.25	0.90	2	2
3	Kecurian Data (Data Biometrik dan Identiti Pengguna)	358	4.23	0.88	6	
Purata Min			4.23			
Kesan Terhadap Privasi Pengguna						
4	Penyalahgunaan Data Peribadi	358	4.25	0.88	3	
5	Pengumpulan Data Tanpa Kebenaran	358	3.83	0.89	15	5
6	Kebocoran Data	358	4.23	0.87	7	
Purata Min			3.83			
Kesan Terhadap Operasi Bangunan Dan Pengguna						
7	Gangguan Operasi	358	4.26	0.83	1	1
8	Kehilangan Keyakinan Pengguna	358	4.04	0.82	13	
9	Ketergantungan Kepada Teknologi	358	4.20	1.00	11	

		Purata Min	4.26			
Kesan Terhadap Pematuhi Peraturan Dan Undang-undang						
10	Kepatuhan Terhadap Undang-undang (Akta Perlindungan Data Peribadi di Malaysia)	358	4.23	0.92	8	
11	Tindakan Undang undang Sekiranya Berlaku Pelanggaran Privasi atau Kebocoran Data	358	4.17	0.99	12	4
12	Keperluan Pematuhan Teknikal	358	4.03	0.81	14	
		Purata Min	4.16			
Kesan Terhadap Persekitaran Sosial						
13	Kesan Psikologi Terhadap Pengguna Kerana Dipantau Dengan Teknologi Ini	358	4.22	0.92	9	
14	Pengawasan Yang Berlebihan Yang Dilengkapi Kamera Dan Sensor	358	4.24	0.87	5	3
15	Keseimbangan Antara Keselamatan Dan Privasi Antara Keselamatan Bangunan Serta Perlindungan Privasi Pengguna	358	4.25	0.84	4	
		Purata Min	4.20			

### 4.2.3 Strategi yang Sesuai untuk Meningkatkan Tahap Keselamatan Siber dan Privasi Semasa Penggunaan Aplikasi Sistem Kawalan Pintu Automatik bagi Bangunan Pintar di Malaysia

Berdasarkan Jadual 9 yang ditunjukkan di bawah, min tertinggi bagi strategi yang sesuai untuk meningkatkan tahap keselamatan siber dan privasi semasa penggunaan aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia ialah "Firewall yang ditingkatkan bertujuan untuk menapis akses masuk dan keluar" dengan nilai min 4.40, kedudukan pertama, dan sisihan piawai 1.01. Strategi ini menekankan kepentingan penggunaan firewall sebagai langkah utama dalam mencegah akses tidak sah serta melindungi sistem daripada ancaman siber yang semakin kompleks. Pelaksanaan firewall yang berkesan memerlukan latihan pekerja untuk memastikan mereka memahami teknologi baharu dan mampu mengaplikasikannya dengan baik dalam konteks kerja mereka (McKee & Gauch, 2020).

Seterusnya, min terendah bagi strategi ini ialah 3.84 pada kedudukan ke-18, iaitu "Pengesahan Berbilang Faktor (MFA) seperti kata laluan, biometrik, dan kod", dengan sisihan piawai 0.93. Walaupun berada pada kedudukan terakhir, MFA tetap menjadi langkah penting dalam memperkukuhkan keselamatan siber dengan memastikan hanya pengguna sah yang mempunyai akses kepada sistem. Strategi seperti MFA harus disokong dengan kesedaran pengguna mengenai kepentingan perlindungan data peribadi serta pematuhan kepada peraturan privasi (Dwivedi *et al.*, 2023).

Analisis deskriptif menentukan jumlah purata min ialah 4.33, yang berada dalam julat lebih tinggi, iaitu antara 3.81 hingga 5.00. Penemuan ini menunjukkan bahawa strategi keselamatan siber memerlukan pelbagai pendekatan yang bukan sahaja fokus pada teknologi tetapi juga melibatkan pembangunan kecekapan pekerja dan pematuhan peraturan.

Oleh itu, penyediaan program latihan yang komprehensif bagi pekerja adalah penting untuk memastikan mereka mampu menangani cabaran keselamatan siber dengan cekap. Latihan ini harus merangkumi pemahaman tentang teknologi terkini seperti firewall yang ditingkatkan dan MFA serta kepentingan pematuhan kepada dasar keselamatan siber dan privasi pengguna (Chong *et al.*, 2022).

**Jadual 9** Strategi yang Sesuai untuk Meningkatkan Tahap Keselamatan Siber dan Privasi Semasa Penggunaan Aplikasi Sistem Kawalan Pintu Automatik bagi Bangunan Pintar di Malaysia

No	Item	N	Min	Sisihan Piawai	Kedudukan
	Teknologi Dan Infranstruktur Keselamatan Siber				1

1	Penyulitan Data ( <i>Encryption</i> ) Yang Kuat Dalam Semua Pemindahan Dan Penyimpanan Data Seperti Data Biometrik Dan Identiti Pengguna	358	4.19	0.91	9	
2	Pengesahan Berbilang Faktor (MFA) Seperti Kata Laluan, Biometrik Dan Kod	358	3.84	0.93	18	
3	Sistem Pencegahan Pencerobohan (IPS) Yang Boleh Mengesan Dan Menyekat Akses Yang Tidak Sah	358	4.23	0.87	5	
4	Firewall Yang Ditingkatkan Bertujuan Untuk Menapis Akses Masuk Dan Keluar	358	4.40	1.01	1	
Purata Min			4.38			
Pengurusan Dan Polisi Pengguna						
5	Latihan Keselamatan Siber Untuk Kakitangan	358	4.24	0.88	3	
6	Polisi Kata Laluan Yang Ketat	358	3.86	0.86	16	
7	Pemantauan Keselamatan Yang Berterusan	358	4.09	0.99	11	2
8	Audit Keselamatan Berkala	358	4.25	0.89	2	
Purata Min			4.23			
Undang-undang Dan Pematuhan Peraturan						
9	Pematuhan Kepada Undang-undang Privasi Data	358	3.85	0.90	17	
10	Sertifikasi Keselamatan Seperti ISO/ISE 27001	358	4.19	0.95	10	5
11	Kontrak Perjanjian Perlindungan Data	358	4.02	1.05	13	
12	Perlindungan Undang-undang Biometrik	358	4.02	0.84	14	
Purata Min			4.00			
Peningkatan Kesedaran Pengguna						
13	Pendidikan Keselamatan Pengguna	358	4.22	0.97	7	
14	Pemberitahuan Kebocoran Data	358	4.21	0.92	8	4
15	Kawalan Akses Yang Lebih Telus	358	3.87	0.87	15	
Purata Min			4.20			
Pemulihan Dan Tindak Balas Insiden						
16	Pelan Tindak Balas Insiden Yang Komprehensif Menangani Serangan Siber	358	4.23	0.88	6	
17	Sandaran Data Yang Selamat Dalam Memastikan Data Penting Disandarkan Secara Berkala Ke Lokasi Yang Selamat	358	4.08	0.97	12	3
18	Pembangunan Pelan Pemulihan Kecemasan Yang Memastikan Sistem Pintu Automatik Dapat Dipulihkan Dan Berfungsi Semula Dengan Cepat Selepas Serangan Siber	358	4.24	0.89	4	
Purata Min			4.22			

## 5. Kesimpulan dan Cadangan

### 5.1 Objektif Kajian 1: Cabaran Utama Yang Dihadapi Dalam Aplikasi Sistem Kawalan Pintu Automatik Bagi Bangunan Pintar Di Malaysia

Objektif pertama adalah untuk mengenal pasti cabaran utama yang dihadapi dalam aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia telah berjaya dicapai. Dapatan kajian dikumpul menggunakan pendekatan kuantitatif dengan mengedarkan borang soal selidik kepada responden. Berdasarkan analisis data penyelidikan, cabaran utama dalam aplikasi sistem kawalan pintu automatik direkodkan dengan tiga min tertinggi seperti dalam Jadual 7, iaitu "Sokongan Penyelenggaraan Secara Berterusan", "Penggunaan Data Yang Berlebihan", dan "Kos Implementasi Atau Kos Pemasangan Sistem Kawalan Pintu Automatik Yang Tinggi", masing-masing dengan min 4.42, 4.26, dan 4.25. Cabaran ini menggambarkan bahawa keperluan untuk penyelenggaraan yang konsisten, peningkatan penggunaan data dalam sistem, dan kos pemasangan yang tinggi menjadi isu utama dalam pelaksanaan teknologi ini di bangunan pintar. Sebaliknya, cabaran yang mencatatkan min terendah ialah 3.83, iaitu "Pencerobohan Sistem Yang Melibatkan Data Peribadi". Hal ini menunjukkan bahawa meskipun risiko berkaitan keselamatan data dianggap penting, ia tidak dilihat sebagai cabaran yang paling kritikal oleh kebanyakan responden. Ini mungkin disebabkan oleh keyakinan bahawa langkah keselamatan siber sedia ada sudah memadai atau boleh ditingkatkan melalui teknologi yang lebih maju. Hal ini seiring dengan dapatan daripada Lee *et al.*, (2017) dan Ng *et al.*, (2022) yang mengatakan isu kos implementasi serta isu pengurusan dan penyelenggaraan yang merupakan cabaran utama di dalam menghadapi penggunaan aplikasi sistem kawalan pintu automatik bagi bangunan pintar.

### 5.2 Objektif Kajian 2: Kesan Yang Dihadapi Dalam Aplikasi Sistem Kawalan Pintu Automatik Terhadap Keselamatan Siber Dan Privasi Pengguna Bangunan Pintar Di Malaysia

Objektif kedua adalah untuk mengenal pasti kesan yang dihadapi dalam sistem kawalan pintu automatik terhadap keselamatan siber dan privasi pengguna bangunan pintar di Malaysia berjaya dicapai. Dapatan kajian dikumpul menggunakan pendekatan kuantitatif dengan mengedarkan borang soal selidik kepada responden. Berdasarkan analisis data dalam Jadual 8, "Gangguan Operasi" mencatatkan min tertinggi iaitu 4.26, menunjukkan bahawa cabaran utama adalah potensi ancaman terhadap keselamatan sistem yang boleh mengakibatkan kebocoran maklumat kritikal atau pelanggaran keselamatan. Kebanyakan responden percaya bahawa cabaran ini memerlukan langkah pencegahan yang kukuh untuk mengelakkan sistem daripada terdedah kepada serangan siber. Sebaliknya, kesan dengan purata terendah ialah 3.83, iaitu "Pengumpulan Data Tanpa Kebenaran". Hal ini mencerminkan bahawa walaupun isu privasi data dianggap penting, ia dilihat sebagai kurang kritikal oleh responden. Hal ini mungkin disebabkan oleh keyakinan bahawa sistem kawalan pintu automatik mempunyai ciri keselamatan yang mencukupi atau penggunaannya terhad kepada maklumat asas, menjadikan risiko ini lebih terkawal. Secara rumusnya, gangguan operasi atau percabulan privasi adalah gangguan konflik yang sering berlaku dalam penggunaan aplikasi sistem kawalan pintu automatik bagi bangunan pintar. Hal ini seiring dengan Lee & Tan (2020), Goh & Lim (2019) yang menegaskan masalah tersebut sering berlaku.

### 5.3 Objektif Kajian 3: Strategi Yang Sesuai Untuk Meningkatkan Tahap Keselamatan Siber Dan Privasi Semasa Penggunaan Aplikasi Sistem Kawalan Pintu Automatik Bagi Bangunan Pintar Di Malaysia

Objektif ketiga adalah untuk mencadangkan strategi yang sesuai bagi meningkatkan tahap keselamatan siber dan privasi semasa penggunaan aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia berjaya dicapai. Dapatan kajian dikumpul menggunakan pendekatan kuantitatif dengan mengedarkan borang soal selidik kepada responden. Berdasarkan analisis data dalam Jadual 9, strategi yang mencatatkan min tertinggi ialah "Firewall yang ditingkatkan bertujuan untuk menapis akses masuk dan keluar", dengan min sebanyak 4.40. Strategi ini dianggap sangat berkesan dalam mencegah akses tidak sah dan melindungi data daripada ancaman siber. Sebahagian responden juga mencadangkan agar latihan diberikan kepada pekerja sedia ada dan baharu untuk memastikan mereka dapat memanfaatkan teknologi keselamatan baharu dengan cekap. Namun, strategi dengan min terendah ialah 3.84, iaitu "Pengesahan Berbilang Faktor (MFA) seperti kata laluan, biometrik, dan kod". Hal ini mungkin disebabkan oleh kurangnya penerapan teknologi ini secara meluas dalam pelbagai sektor, yang memerlukan kesedaran dan sokongan tambahan untuk meningkatkan penggunaannya. Hal ini selaras dengan dapatan daripada Tan & Lim (2020), Rahim & Tan (2019) yang menegaskan bahawa penggunaan protocol keselamatan yang kukuh penting untuk memastikan akses masuk dan keluar secara betul mengikut kepiawaian dan kelulusan yang ditetapkan.

## 5.4 Penutup

Kesimpulannya, kajian ini telah menunjukkan bahawa kesemua objektif penyelidikan berjaya dicapai melalui analisis data soal selidik yang dijalankan menggunakan program SPSS. Hasil kajian menunjukkan bahawa cabaran utama dalam aplikasi sistem kawalan pintu automatik bagi bangunan pintar di Malaysia dapat dikenal pasti dengan jelas. Pilihan pihak berkepentingan terhadap penggunaan sistem ini turut dipengaruhi oleh faktor-faktor yang mempengaruhi pelaksanaannya, termasuk keselamatan siber, privasi pengguna, dan kos pelaksanaan. Selain itu, pelaksanaan sistem kawalan pintu automatik berpotensi meningkatkan kesedaran dan penggunaan teknologi pintar di kalangan pengguna. Walau bagaimanapun, kajian ini dihadkan oleh beberapa kekangan, dan cadangan telah diberikan untuk memperbaiki hasil penyelidikan pada masa hadapan. Akhir sekali, penyelidikan ini diharapkan dapat membantu semua pihak berkepentingan, termasuk pengguna, penyedia teknologi, dan pembuat dasar, untuk lebih memahami cabaran, kesan, dan strategi yang sesuai dalam memastikan keselamatan dan privasi semasa penggunaan sistem kawalan pintu automatik dalam bangunan pintar di Malaysia.

## Penghargaan

Penulis ingin merakamkan penghargaan kepada Fakulti Pengurusan Teknologi dan Perniagaan, Universiti Tun Hussein Onn Malaysia atas sokongan yang diberikan.

## Konflik Kepentingan

Penulis menyatakan bahawa tiada sebarang konflik kepentingan berhubung dengan penerbitan kertas ini.

## Sumbangan Penulis

Penulis mengesahkan sumbangan terhadap kertas ini seperti berikut: **reka bentuk dan konsep kajian:** Khairul Firdaus Saupi, Roshartini Omar; **pengumpulan data:** Khairul Firdaus Saupi; **analisis dan tafsiran hasil:** Khairul Firdaus Saupi; **penyediaan draf manuskrip:** Khairul Firdaus Saupi, Roshartini Omar, Md Asrul Nasid Masrom dan Zailawati Khalid. Penulis telah menyemak hasil kajian dan meluluskan versi akhir manuskrip ini.

## Rujukan

- Abdirad, H., & Dossick, C. S. (2016). "Automated Door Systems and Their Implications for Universal Design and Accessibility."
- Ahmad, F. (2021). "Legal Issues and Regulatory Challenges of Smart Building Technologies."
- Ahmad, M., & Mohd, A. (2021). "Security Vulnerabilities in Automated Door Control Systems: A Case Study."
- Ahmad, R. A. (2021). "A Study on the Reliability of Smart Lock System in Malaysia."
- Ahmad, S. A. (2017). "Safety and Security Issues on Automated Door Systems."
- Aman, S., & Nasir, M. (2023). "Maintenance Challenges in Automated Door Systems for Smart Buildings." *International Journal of Smart Infrastructure and Technology*, 8(1), 45–60.
- Arezes, Penaloza. (2019). "A Critical Review of Cyber Physical Security for Building Automation Systems." *Proceedings of the 43rd ASC National Annual Conference*, 25-262.
- Astro Awani. (2023). "Ancaman keselamatan siber meningkat di Malaysia." Cyber Security Malaysia (CSM).
- Azhar, S., & Richer, E. (2019). "Smart Buildings: Advanced Materials and Nanotechnology to Improve Energy Efficiency and Environmental Performance."
- Badrulhisyam, N. S., & Wee, S. T. (2020). "Smart Building Risk Assessment Case Study (Challenges, Deficiencies and Recommendations)." *2020 ASSE Annual Conference & Exposition*, 12-14.
- Barnsbee, L. (2018). "Definisi Populasi Sasaran dalam Penyelidikan."
- Becerik, B., Gerber, D., & Ku, K. (2011). "Building Information Modeling in Design, Construction, and Operations."
- Chan, S. H. (2017). "Vulnerability Assessment of Door Access Control System."
- Chan, S. H. (2019). "Reliability and Safety Assessment of Automated Door Systems in High-Rise Buildings."
- Cheah, W. L. (2023). "User Awareness and Perception Towards Smart Building Technology."
- Chong, H. C., Lee, K. Y., & Tan, J. P. (2022). "Enhancing Workforce Preparedness for Cybersecurity in Smart Building Operations." *Journal of Engineering and Technology*, 14(2), 103–117.
- Chong, H. C., Lee, K. Y., & Tan, J. P. (2022). "Impact of Power Supply Stability on the Performance of Automated Systems in Smart Buildings." *Journal of Engineering and Technology*, 14(2), 103–117.
- Dwivedi, Y. K., Hughes, D. L., & Rana, N. P. (2023). "Cybersecurity and Privacy Challenges in Smart Systems." *International Journal of Digital Innovation*, 9(3), 78–92.
- Gadzheva, M. (2008). "Privacy Concerns and Data Protection in Smart Environments." *Journal of Information, Communication and Ethics in Society*, 6(2), 129–140.
- Haida Umiera. (2022). "Rancang Bangun Pintu Gerbang Otomatis Menggunakan Arduino Uno R3." *Jurnal Portal Data*, 2(2).

- Hanif, A. (2019). "Rumah Pintar Kurang Selamat." Rumah Pintar Kurang Selamat (hmetro.com.my).
- Hill, R. (1998). "What Sample Size is 'Enough' in Internet Survey Research?" *Interpersonal Computing and Technology: An Electronic Journal for the 21st Century*, 6(3-4), 1-10.
- Indeks Bangunan Hijau. (2020). "Statistik Pengguna Bangunan Pintar di Kuala Lumpur."
- Ismail, A. M. (2020). "Cybersecurity Vulnerability Assessment of Building Automation Systems."
- Kanan, A., Elhassan, O., & Bensalem, S. (2018). "Automated Door Control System for Safe Building Access."
- Kim, T., & Chi, S. (2019). "Sistem Keselamatan Pintu Menggunakan RFID Dan Pengawal Mikro Arduino." *Proceedings of the Malaysia TVET on Research via Exposition*.
- Krecjcie, R. V., & Morgan, D. W. (1970). "Determining Sample Size for Research Activities." *Educational and Psychological Measurement*.
- Lee, S. H. (2017). "Cost-Effective Design of Automatic Door System for Smart Buildings."
- Lee, S. H. (2018). "Compliance of Smart Door Locks with Personal Data Protection Act 2010."
- Lim, C. H. (2020). "Security and Privacy Issues in Smart Building: A Review."
- Lim, H., & Chew, Y. (2022). "Collaborative Approach to Enhancing Security in Smart Door Control Systems."
- Lingard, H., Davison, G., & Thornton, R. (2021). "Construction Craft Labourers: Exploring Changes to Work, Training and Vocational Education in Australia."
- McKee, M., & Gauch, R. (2020). "Importance of Employee Training in Adopting New Technologies." *Journal of Workplace Strategies*, 15(2), 45-60.
- Muhammad Rasyid & Yusuff, S. (2019). "Mencapai Keseimbangan yang Tepat Antara Keselamatan Siber dan Akses Pengguna." *Universal Access in the Information Society*, 17, 491-501.
- Ng, H. Y. (2019). "Management and Maintenance Challenges of Smart Building Systems: A Case Study."
- Ng, H. Y. (2022). "Management and Maintenance Challenges of Smart Building Systems: A Case Study."
- Nicholas Yong Andre. (2019). "Kelebihan dan Kekurangan Kunci Pintu Digital."
- Nur Shahirah Zainoor Hisham. (2023). "Peranti Canggih Untuk Pintu Utama Pembangunan Moden."
- Onwuegbuzie, A. J., & Collins, K. M. T. (2007). "A Typology of Mixed Methods Sampling Designs in Social Science Research." *The Qualitative Report*.
- Osman, N. A. (2017). "Safety and Security Issues on Automated Door Systems."
- Rahim, A. A. (2021). "A Study on the Reliability of Smart Lock System in Malaysia."
- Rahim, A., & Tan, K. (2020). "Cybersecurity Awareness Training for Smart Building Users: A Case Study."
- Rahman, A. M. M. A. (2019). "Failure Analysis and Design Modification of Automatic Door System."
- Tan, K. Y. (2019). "Security and Privacy Risks in Smart Door Locks: A Case Study of a Smart Door Lock System."
- Tan, K. Y. (2021). "Interoperability Challenges and Standardization Issues of Smart Home Technologies."
- Tan, K. Y. (2021). "User Awareness and Perception Towards Smart Building Technology."
- Tan, K., & Lim, C. (2020). "Enhancing Security in Smart Door Control Systems Using IoT Devices."
- Vogt, W. P. (2007). "Quantitative Research Methods for Professionals."
- Wang, X., Chong, H.-Y., & Zuo, J. (2015). "BIM Adoption and Implementation in Architectural Education: An International Survey." *Automation in Construction*, 51, pp. 1-10.
- Wong, J. K. L. (2018). "Investigation of IoT (Internet of Things) Application in Building Automation System."
- Wong, S., & Lee, J. (2022). "Aligning Smart Door Control Systems with Security and Privacy Standards: A Framework."
- Woo, J. H. (2006). "BIM (Building Information Modelling) and Pedagogical Challenges." *Proceedings of the 43rd ASC National Annual Conference*, pp. 12-14.
- Woo, Jyh Haur. (2019). "Security Analysis of Open Building Automation Systems."