KERANGKA KESELAMATAN INTERNET PELBAGAI BENDA (IPB) DALAM PERUSAHAAN KECIL DAN SEDERHANA

Siti Aisyah Anuar, Umi Asma' Mohktar

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia,
43600 Bangi, Selangor

P106812@siswa.ukm.edu.my, umiasmamokhtar@ukm.edu.my

ABSTRAK

Keselamatan Internet Pelbagai Benda (IPB) bukan satu isu baharu dalam implementasi teknologi IPB pada hari ini. Keselamatan IPB merupakan satu strategi dan mekanisme perlindungan terhadap serangan siber termasuk peranti, rangkaian dan aplikasi IPB. Tanpa strategi keselamatan yang betul, ketersambungan peranti IPB dengan rangkaian kepada aplikasi atau sistem akanterdedah kepada kerentanan, sekali gus mengundang penggodam untuk menyusup masuk ke dalam rangkaian, meletakkan perisian hasad dan mencuri data dan maklumat pengguna. Oleh itu, PKS memerlukan satu rangka kerja yangmenjadi panduan dalam memacu keselamatan ekosistem IPB. Objektif kajian ini dijalankan adalah untuk mengenal pasti ancaman keselamatan dan cabaran pelaksanaan IPB yang selamat dalam PKS. Kajian ini juga bertujuan mengenal pasti rangka kerja dari organisasi yang berkaitan dengan penubuhan rangka kerja keselamatan IPB dalam PKS. Kajian ini menggunakan kaedah persampelan bertujuan di 30 PKS di Malaysia yang menggunakan IPB melalui soal selidik dalam talian dan bersemuka. Analisis data menggunakan kaedah deskriptif secara frekuensi dan median serta kajian susastera lanjutan dilakukan. Kajian mendapati senario keselamatan IPB di PKS seperti ancaman keselamatan siber terhadap ekosistem IPB dan cabaran pelaksanaan IPB menjadi perkara yang perlu diberi perhatian untuk menjadikan IPB di PKS adalah selamat. Selain itu, sebuah kerangka keselamatan IPB dibina berdasarkan tiga komponen utama melindungi IPB di PKS iaitu melindungi peranti, rantaian dan aplikasi serta PKS secara keseluruhan. Tambahan pula, komponen pengetahuan turut ditambah dalam memastikan PKS dan personel mempunyai pengetahuan mengendalikan IPB yang selamat dalam PKS.

Kata Kunci: Internet Pelbagai Benda (IPB), Perusahaan Kecil dan Sederhana (PKS), Kerangka Keselamatan IPB

1.0 PENGENALAN

Set peranti fizikal, peranti, perisian, penderia dan sambungan rangkaian yang membolehkan elemen ini mengumpul dan berkongsi data dipanggil Internet Pelbagai Benda, IPB (Tiwary, Mahato, Chandrol, 2018). IPB bukan sekadar peranti seperti telefon yang disambungkan ke TV, tetapi kemungkinan IPB melampaui itu. Semakin banyak peranti dengan sambungan Internet sedang dibangunkan setiap hari, menjadikannya sebahagian daripada IPB. Kini segalanya boleh disambungkan dan dihubungkan ke Internet, jadi, komunikasi serta interaksi antara orang, proses dan perkara menjadi semakin lancar. Hal ini termasuklah dengan perniagaan, rutin dan sebagainya. Sambungan IPB adalah penting kepada perniagaan namun peranti yang tidak diselia dan tidak terjamin yang disambungkan ke rangkaian dan menimbulkan risiko keselamatan (Palo Alto, 2019). Popularity IPB semakin melonjak dan pembangunan langkah keselamatannya mesti bersaing dengan cepat. Keselamatan IPB boleh ditakrifkan sebagai strategi keselamatan dan mekanisme perlindungan yang pada asasnya melindungi peranti IPB pada rangkaian yang

sengaja dicipta untuk set ciri tertentu daripada serangan siber. Peranti IPB yang disambungkan yang tidak mempunyai keselamatan yang mencukupi terdedah kepada pencerobohan, kompromi dan kawalan oleh penyerang untuk mencuri data pengguna dan menurunkan taraf rangkaian. Lebih banyak peranti yang anda sambungkan ke IPB, lebih besar keperluan untuk melindungi peranti dalam rangkaian.

Kajian ini berlatarbelakangkan Perusahaan Kecil dan Sederhana (PKS) yang merangkumi sektor pembuatan, perkhidmatan dan lain-lain. Perusahaan kecil dan sederhana merujuk kepada syarikat yang dibina di atas perusahaan mikro, kecil dan sederhana. Definisi PKS secara umumnya ditentukan melalui dua kriteria iaitu daripada jumlah jualan tahunan atau jumlah pekerja sepenuh masa. Definisi terperinci mengikut kategori adalah seperti Rajah 1.1. Bagi sektor pembuatan, PKS didefinisi sebagai firma yang mempunyai jualan kurang dari RM50 juta atau kurang daripada 200 orang pekerja sepenuh masa. Manakala bagi sektor perkhidmatan dan lain-lain, PKS didefinisi sebagai firma yang mempunyai jualan kurang RM20 juta atau kurang daripada 75 orang pekerja sepenuh masa (SMECorp, 2021).

Organisasi khususnya PKS telah menerima pakai IPB dalam perniagaan. Menurut Vermanen, Rantanen, & Harkke, (2022), kejayaan organisasi besar mengimplementasi IPB memberi inspirasi kepada PKS agar menggunakan IPB bagi memudahkan urusan perniagaan harian. Peningkatan penggunaan IPB didorong oleh keperluan sesebuah perniagaan dalam membangunkan transformasi perniagaan digital (Gloukhovtsev, 2018). Oleh kerana PKS cuma menggunakan peranti IPB tanpa memikirkan ciri-ciri lain, tahap keselamatan teknologi IPB terhadap ancaman siber dalam perniagaan ini masih pada tahap rendah (Kuzminykh, Ghita, & Such, 2020).

2.0 KAJIAN LITERATUR

2.1 Internet Pelbagai Benda (IPB)

Istilah IPB ini sendiri tiada sebuah istilah yang tetap kerana teknologi ini sentiasa yang berkembang dan sentiasa relevan untuk dibincangkan (Patel & Patel, 2016). Istilah IPB mula diperkenalkan oleh Kevin Ashton pada tahun 1999 sebagai satu sistem yang menghubungkan Internet dengan objek fizikal dalam rangkaian yang membolehkan pertukaran maklumat berlaku (Norman, 2013). Badan organisasi ISO dan Suruhanjaya Elektroteknikal Antarabangsa (IEC) mendefinisi IPB secara rasmi sebagai sebuah infrastruktur menghubungkan entiti,orang, sistem

dan sumber maklumat dengan perkhidmatan yang memproses dan memberi respons kepada maklumat dari dunia fizikal dan dunia maya (ISO, 2018). Di samping itu, IPB didefinisikan oleh MIMOS (2015) sebagai interaktiviti pintar di antara individu dan objek untuk saling bertukar maklumat dan pengetahuan untuk mewujudkan nilai baharu (MIMOS, 2015). NIST sebaliknya membezakan penggunaan akronim IPB dan Rangkaian Pelbagai Benda. IPB mempunyai objek atau peranti fizikal yang bersambung kepada capaian Internet,menjadikan ia subset kepada RPB (Gloukhovtsev, 2018). Menurut TrendMicro (2019), IPB ditakrif sebagai perkembangan dan komunikasi rangkaian lain dengan sensor peranti fizikal yang berbeza. . IPB mewakili rangkaian objek, perkhidmatan, rangkaian dan konsep dan sambunganinfrastruktur. Teknologi baharu ini telah mengubah cara orang berinteraksi dengan objek (Eibo, Falana, Taiwo, Olumiawa, 2021). Namun, (Georgescu, 2021) berpendapat bahawa IPB merujuk kepada peranti fizikal yang berada dalam perisian, sensor dan teknologi lain yang membolehkan mereka menyambung ke Internet dan berkongsi data dengan peranti dan sistem lain.

2.2 Seni Bina IPB

Seni bina dalam konteks IPB merangkumi beberapa lapisan teknologi, yang mana bertujuan memberi gambaran bagaimana setiap teknologi yang berbeza ini disambungkan dan dihubungkan antara satu sama lain dalam satu rangkaian (Patel &Patel, 2016). Komponen ini menjadi tunggak utama dalam pengaplikasian sesebuah IPB (Assan, 2018). Seni bina IPB pada asasnya ialah satu set komponen yangterdiri daripada peranti, rangkaian dan aplikasi.

Rajah 2.1: Seni bina lapisan IoT

Seni bina IPB terdiri daripada tiga lapisan adalah yang asas (NASSCOM, 2021). Rajah 2.1 menerangkan model asas seni bina terdiri daripada tiga lapisan iaitu peranti, aplikasi, dan rangkaian seperti yang dicadangkan oleh (Khan, Khan, Zaheer, & Khan, 2012). Tiga lapisan IPB ini menjadi asas dan konsep IPB yang digunakan secara meluas (Reynolds, 2020).

Abdmezim (2015) bersetuju dengan tiga lapisan senibina IPB dan berpendapat tiga lapisan ini adalah cukup sebagai asas pembinaan IPB. Kajian Noor & Hassan (2018) berpendapat bahawa seni binaIPB adalah berdasarkan struktur tiga lapisan yang merangkumi lapisan peranti, lapisan rangkaian dan lapisan aplikasi berkaitan perisian yang membentuk sistem IPB.

Kajian ini memberi fokus kepada tiga lapisan senibina IPB yang menjadi asas kepada awal pembinaan senibina IPB. Tiga lapisan senibina tersebut adalah:

1. Lapisan Peranti: Lapisan Peranti merupakan lapisan yang menjadi asas atau tapak bermulanya ekosistem IoT. Lapisan ini meliputi peranti fizikal seperti penderia yang menerima maklumat daripada persekitaran (Burhan, 2018).
2. Lapisan Rangkaian: Lapisan Rangkaian menghubungkan peranti fizikal dengan aplikasi IPB dalam ekosistem IPB. Lapisan ini menghantar dan memproses maklumat yang diperoleh dari lapisan peranti untuk dibawa ke lapisan aplikasi melalui gerbang.
3. Lapisan Aplikasi: Lapisan Aplikasi menyampaikan perkhidmatan dan berinteraksi dengan pengguna IPB. Antara contoh aplikasi yang sering diganakan adalah ‘Pejabat Pintar’ dan sebagainya.

2.3 Keselamatan IPB

Menurut Fortinet (2019), keselamatan IPB ialah perlindungan peranti dan rangkaian Internet yang disambungkan kepadanya daripada ancaman dan pelanggaran dengan melindungi, mengenal pasti dan memantau ancaman, serta membantu menyelesaikan kelemahan dalam pelbagai peranti yang mungkin menimbulkan risiko keselamatan sesebuah perniagaan. Keselamatan mesti dibina ke dalam sistem IPB. Malangnya, peranti IPB dibina secara bebas daripada kelemahan keselamatan (El-Gendy & Azer, 2020). Hal ini menyebabkan peranti atau sistem IPB berpotensi besar untuk terdedah terhadap ancaman siber.

2.4 Kepentingan IPB yang selamat dalam PKS

Dengan kewujudan teknologi IPB, keadaan atau persekitaran sesebuah perniagaan menjadi agak berbeza. IPB memainkan peranan yang penting dalam memastikan operasi sesebuah perniagaan itu berjalan dengan lancar; seperti dalam hal ini, industri PKS mula menggunakan teknologi alaf baru ini dalam automasi pembuatan, contohnya proses pembuatan, pengurusan rantaian bekalan dan sebagainya. Kebanyakan perusahaan telah melaporkan

bahawa pencerobohan IPB ini mampu membawa kesan yang besar ke atas operasi sesebuah perniagaan (Hoppe, 2018). Memastikan IPB yang selamat merupakan satu langkah yang penting bagi pengusaha perniagaan demi memastikan kelansungannya pada masa akan datang. Hal ini kerana dalam industri pembuatan di PKS, contohnya, terdapat pelbagai peranti IPByang digunakan (Bhaskar, 2022). Namun, semakin banyak peranti disambungkan ke Internet, semakinbesar cabaran PKS untuk memastikan IPB ini berada di tahap yang selamat. Menurut kajian Atoui (2018), perkakasan, perisian dan rangkaian perlu dilindungi untuk meastikan IPB ini berada di tahap efisien dan efektif. Tanpa IPB yang selamat, penggodam mampu mengancam data-data dan privasi syarikat sesebuah perniagaan (Atoui, 2018). Menurut Duca (2020), jika keselamatan IPB contohnya peranti seperti sensor terancam, hal ini akan mengakibatkan reputasi sesebuah perniagaan itu tercalar, tambahan lagi dengan implikasi terhadap kewangan dan data-data penting sesebuah syarikat.

2.5 Cabaran Pelaksanaan IPB yang selamat

Cabaran pelaksanaan IPB yang selamat yang utama ialah kelemahan *firmware* dan perisian pada peranti dan sistem IPB (Feng et. al, 2023). Kemas kini perisian tegar dan pemasangan patch keselamatan pada peranti IPB mungkin mencabar. Kerentanan keselamatan baharu setiap hari diperkenalkan kepada Internet (Vignesh & Samydura, 2017). Selain itu, kelemahan mekanisma pengesahan turut menjadi cabaran dalam memastikan peranti IPB ini sentiasa dilindungi. Kerentanan keselamatan meningkat dengan penggunaan lalai kata laluan, ditetapkan oleh pengeluar tanpa mengubahnya juga dengan menggunakan kata laluan yang lemah pada mana-mana peranti. Tambahan pula, kekurangan dari segi kemahiran mengendalikan IPB dan keselamatan IPB turut menjadi cabaran utama. Pengguna tidak memahami sejauh mana keupayaan peranti IPB ini boleh bertindak atau menilai risiko keselamatan sekiranya peranti dan sistem diserang penggodam. Selanjutnya, jurang kepatuhan dan standard dalam pelaksanaan IPB yang selamat dalam PKS turut menjadi cabaran utama pada hari ini. Akhir sekali, implementasi IPB yang selamat dalam ekosistem PKS bukanlah percuma dan memerlukan kos. Oleh itu, sokongan dari segi kewangan dan sokongan pihak pengurusan merupakan satu cabaran yang perlu dilalui sekiranya pengusaha PKS inginmengaplikasikan IPB yang selamat dalam perniagaaan mereka.

2.6 Ancaman Siber terhadap IPB dalam PKS

Peranti wujud dalam lapisan IPB sebagai salah satu lapisan permulaan yang penting kerana ia

maklumat dikumpulkan melalui peranti-peranti IPB contohnya sensor atau penderia. Malahan, dalam kajian yang dibuat oleh (Alaba, Othman, Hashem, & Alotaibi, 2017) menyatakan serangan jamming merupakan salah satu serangan yang paling kerap berlaku pada lapisan ini. Jamming merupakan gangguan dalam komunikasi tanpa wayar dengan pengurangan nisbah *'signal-to-noise'* pada bahagian penerima melalui transmisi wayarles yang terganggu. Di samping itu, (Ingham, Marchang, & Bowmik, 2019) menggariskan potensi penggunaan peranti IPB mampu tercemar sekiranya IPB ini tidak dilengkapi dengan ciri keselamatan yang boleh mengundang kepada isu kecurian data dan sebagainya (Ingham, Marchang, & Bowmik, 2019).

Seterusnya, ialah lapisan peranti yang juga terdedah kepada serangan kerana ia menghubungkan peranti antara satu sama lain dalam rangkaian (Ceron et al, 2019). Antara ancaman siber yang boleh wujud pada lapisan ini ialah Serangan Penafian Perkhidmatan (DoS). Serangan DoS terjadi untuk melarang pengguna daripada mengakses peranti atau lain-lain sumber rangkaian. Selain itu, pada lapisan aplikasi, lapisan ini merupakan lapisan yang bertanggungjawab ke atas operasi setiap aplikasi (Yildirim, Senol, & Demiroglu, 2021). Sun & Ansari (2017) menambah lapisan ini turut menambah perkhidmataan kepada aplikasi. Skrip Silang Tapak di penyerang membuat skrip laman web dipercayai yang dilawati oleh pengguna lain. Disini, penyerang boleh mengubah suai maklumat dan merosakkan system. Seterusnya merupakan serangan Kod Hasad, ia adalah kod yang merosakkan system terletak di mana-mana dalam perisian.

2.7 Pembinaan Kerangka Konseptual

Berdasarkan 14 sorotan literatur yang dibuat dalam kajian ini, sebuah kerangka konseptual dibina berdasarkan tiga komponen yang wajar di ambil kira dalam membina satu ekosistem IPB yang selamat. Rajah 2.13 menunjukkan kerangka konseptual yang dibina.

Rajah 2.2: Kerangka Konseptual

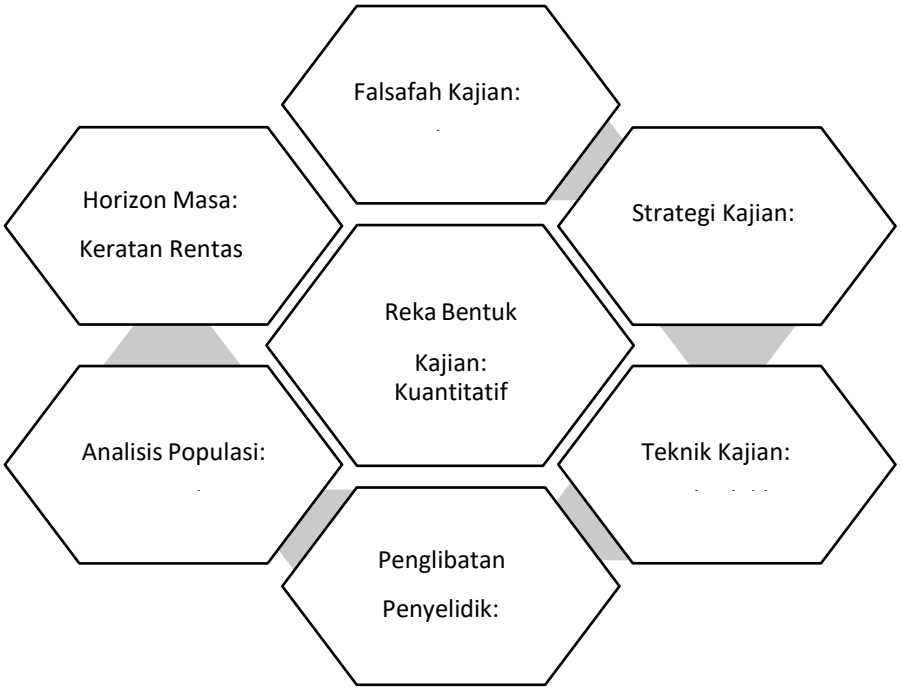
2.8 Ringkasan Kerangka Keselamatan IPB yang sedia ada

Literatur	Organisasi	Jenis Kerangka	Dapatan
Guidelines for Secure InternetPelbagai Benda (IPB) (Cybersecurity Malaysia, 2020)	Cybersecurity Malaysia	Garis Panduan	Kawalan keselamatan yang disenaraikan pada Senarai Semak Keselamatan Siber IPB diperoleh daripada garis panduan ini. Senarai semak ini boleh digunakan oleh pemain utama sebagai panduan semasa pembangunan, pemasangan atau pelaksanaan IPB sistem.
Information Security Guidelines for Small & Medium Entreprises (SMEs) (Cybersecurity Malaysia, 2011)	Cybersecurity Malaysia	Garis Panduan	Garis Panduan ini menyediakan senarai semak sebagai panduan dalam melindungi keselamatan informasi, namunbukan IPB.
Internet of Things (IPB) Security Best Practices (Corser, et.al, 2017)	IEEE Internet Technology Policy Community White Paper	Amalan pematuhan terbaik	Tujuan dokumen ini adalah untuk membentangkan satu set Internet yang diselidiki dengan baik Garis panduan yang memberi fokus kepada peranti fizikal IPB.
SME Guide for the Implementation of ISO/IEC27001 on InformationSecurity Management (SBS, 2018)	European Digital SME Alliance	Garis Panduan	Berdasarkan kandungan ISO/IEC 27001, Panduan ini menerangkan satu siri praktikal aktiviti yang boleh membantu dengan ketara dalam mewujudkan atau meningkatkan keselamatan maklumat peringkat dalam PKS.
SME Guide for Industrial Internet of Things (IIoT): Special Focus on Security (SBS, 2020)	European Digital SME Alliance	Garis Panduan	Isu panduan akan ditumpukan terutamanya pada aspek keselamatan yang palingpenting dalam persekitaran IIPB.Panduan ini terbahagi kepada dua; organisasi dan operasi. Setiap pembahagian ini meliputi aspek yang berbeza namun menyeluruh.
Polisi 4IR Kebangsaan (Unit Perancang Ekonomi, 2020)	Unit Perancang Ekonomi,Jabatan Perdana Menteri	Polisi	Polisi ini bertindak sebagai garispanduan untuk menilai dan mengurus risiko
IoT SecurityAssurance Framework Release 3.0 (IotSF, 2021)	*Internet Security Foundation*	Kerangka	Rangka Kerja ini bertujuan membantu semua syarikat membuat pilihan keselamatan termaklum berkualiti tinggi dengan membimbing mereka melalui senarai semak keperluan yang komprehensif dan proses pengumpulan bukti.
Hala Tuju IPB Strategik Kebangsaan (MIMOS, 2014)	MIMOS Berhad	Hala tuju	Hala Tuju ini berhasrat menjadikan Malaysia sebagai hub IPB,mencipta satu ekosistem dan menguatkan teknousahawan. Namun, dokumen ini tidak mengandungi keselamatan IPB.

Accelerating the Impact of Industrial IoT inSmall and Medium Sized Enterprises: A Protocol for Action (World EconomicForum, 2020)	Forum Ekonomi Dunia	Protokol	Protokol Dasar yang disertakan dalam dokumen ini menyediakan asas fakta untuk dipelajari oleh pembuat dasar daripada menyesuaikan dan menggunakan dalam bidang kuasa mereka sendiri. Dokumen ini turut menyenaraikan cabaran pelaksaan IPB dalam industri
Rangka KerjaKeselamatan Siber Sektor Awam (RAKKSA)(NACSA, 2016)	National Cybersecurity Agency Malaysia (NACSA)	Kerangka	Rangka kerja ini dibangunkan berdasarkan rangka kerja keselamatan sebelumnya. Aspekrangka kerja adalah untuk memenuhi prinsip keselamatan berdasarkan kepada penilaian risiko.
Malaysia Digital Economic Blueprint (Unit Perancangan Ekonomi, 2020)	Unit Perancang Ekonomi, Jabatan Perdana Menteri	Pelan Tindakan	Pelan Tindakan ini melahirkan program MyDigital yang menjana pertumbuhan perniagaan digital di Malaysia khususnya PKS. Pelan ini melihat kepada keselamatan siber secara menyeluruh untuk sistem IPB
Secure Design Best Practice Guides Release 2 (IoTSF, 2019)	*IoT Security Foundation*	Garis Panduan	Panduan ini memberikan nasihat penting yang ringkas tentang 'perkara yang perlu dilakukan' untuk membantu menjamin produk dan sistem IPB. Namun, ianya agak umum untuk peranti IPB sahaja.
Industrial Internet of Things (IIPB) Volume G4: Security Framework (IIC, 2016)	*Industrial Internet Consostium*	Kerangka	Dokumen ini menggariskan amalan terbaik dan pertimbangan yang diperlukan untuk menangani risiko keselamatan dikaitkan dengan IIPB Bahan dalam dokumen ini harus membolehkan pembangun dalam pelbagai jenis sektor, termasuk tenaga, pembuatan penjagaan kesihatan, pengangkutan dan sektor awam
Industry 4WRD:National Policy on Industry 4.0 (MITI, 2018)	Kementerian Perdagangan Antarabangsa dan Industri	Polisi	Polisi ini menjadi satu pendekatan implementasi untuk memajukan teknologi IR4.0.

3.0 METODOLOGI KAJIAN

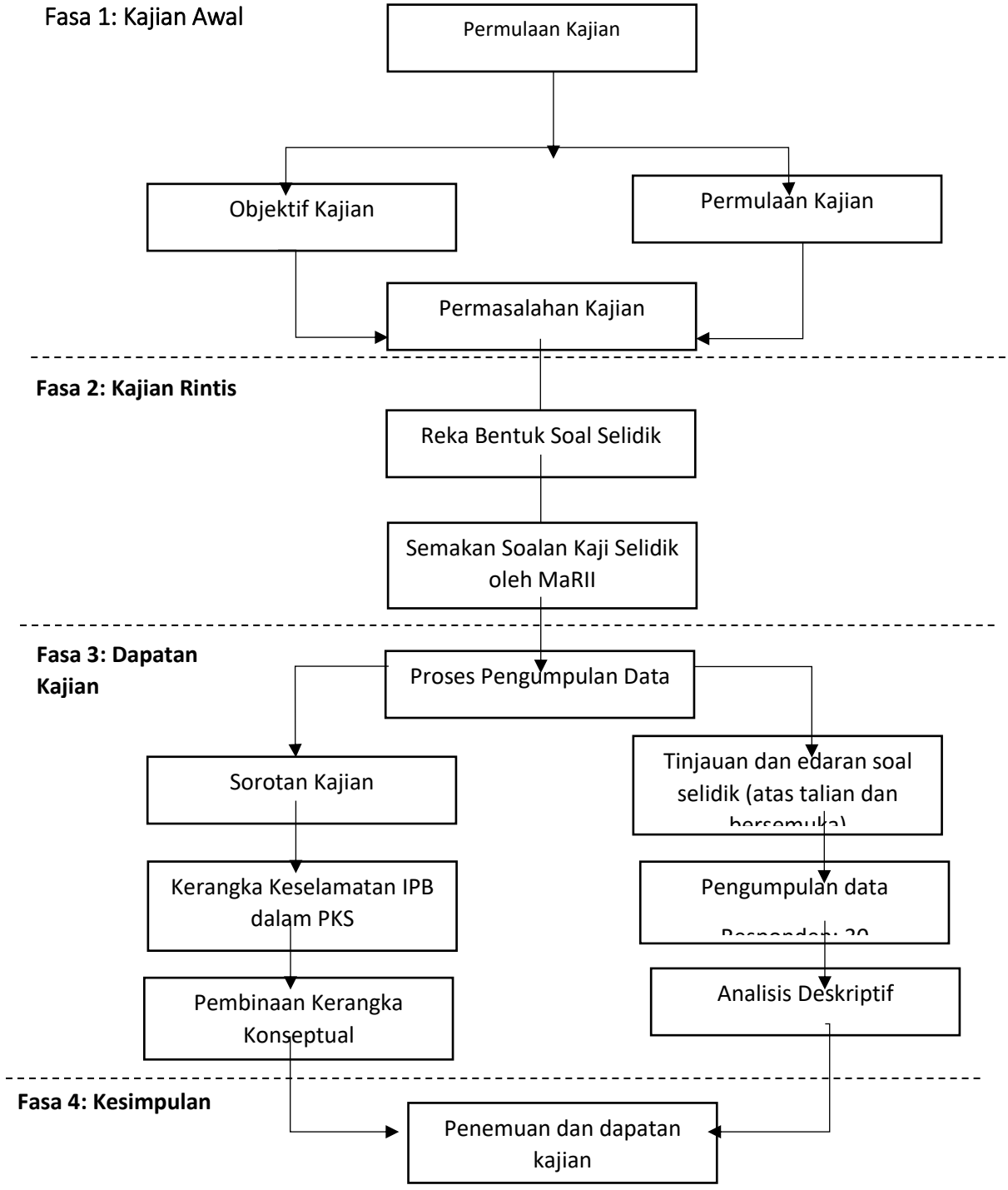
Sekaran dan Bougie (2016) menyatakan reka bentuk kajian merupakan pelan tindakanatau pelan untuk mengumpul , mengukur dan menganalisis data yang dibuat untuk menjawab persoalan kajian yang telah diutarakan (Sekaran & Bougie, 2016). Proses untuk mereka bentuk sesebuah kajian ini bermula daripada pengenalpastian masalah,pengumpulan data awalan, pembangunan kerangka teori, pembangunan persoalan kajian, pembangunan reka bentuk kajian, pengumpulan data dan analisis dan diakhiri dengan penutup.



Rajah 3.1: Rekat Bentuk Kajian

Sementelahan, berdasarkan Rajah 3.2, bab ini turut menerangkan proses kajian yang dilakukan bermula dari awal kajian hingga ke dapatan akhir. Penyelidik membahagikan proses kajian ini kepada empat fasa, bermula Fasa Kajian Awal, Fasa Kajian Rintis, Fasa Dapatan Kajian dan akhir sekali Kesimpulan (Cresswell, 2009). Menurut Hanacek (2016), fasa-fasa dalam proses kajian adalah sebagai satu prosedur sistematik untuk menjana pengetahuan dan memberi fokus kepada skop utama penyelidikan (Hanacek, 2016). Bagi kajian ini, penyelidik telah memilih untuk melakukan pensampelan bukan kebarangkalian untuk mengetahui senario keselamatan IPB dalam PKS oleh individu yang berpengalaman mengendalikan IPB. Seramai 30 orang individu telah ditemui oleh penyelidik untuk memahami situasi penggunaan IPB yang selamat dalam perniagaan. Penyelidik menggunakan persampelan bertujuan di mana persampelan ini mengandaikan bahawa setiap responden mempunyai kriteria yang sama (Nikolopoulou, 2022), iaitu seperti dalam kajian ini adalah PKS yang menggunakan IPB dalam

perusahaan mereka. Penyelidik mengedarkan borang soal selidik secara atas talian (Google Form) dan luar talian.



Rajah 3.2: Proses Kajian

4.0 KEPUTUSAN KAJIAN DAN PERBINCANGAN

Untuk kajian ini, penyelidik telah membahagikan pecahan soalan dan hasil kajian kepada 5 seksyen; profil perniagaan, profil personel, ekosistem IPB, senario keselamatan IPB dan strategi memastikan IPB yang selamat dalam perniagaan.

4.2 Analisis Seksyen A (Profil Perniagaan)

Saiz Perniagaan	**%**	**Lokasi Perniagaan**	**%**	**Sektor Perniagaan**	**%**	**Tempoh Pengoperasian**	**%**
Mikro	10	Lembah Klang	60	Pembuatan	46.7	Kurang 1 tahun	3.3
Kecil	60	Sabah Sarawak	3.3	Perkhidmatan dan lain-lain	53.3	1 – 5 tahun	43.3
Sederhana	30	Utara Malaysia	13.3			6 – 10 tahun	46.7
		Selatan Malaysia	23.3			Lebih 10 tahun	6.7
Jumlah	100	Jumlah	100	Jumlah	100	Jumlah	100

Jadual 4.1 merupakan kekerapan jawapan yang diperoleh daripada responden untuk Soal Selidik Seksyen A. Analisis seksyen ini adalah untuk mengetahui latar belakang perniagaan yang merangkumi saiz, lokasi, sektor dan tempoh pengoperasi perniagaan. Penyelidik menggambarkan maklumat yang diperoleh dalam bentuk jadual yang menggabungkan kesemua soalan bersama peratusan.

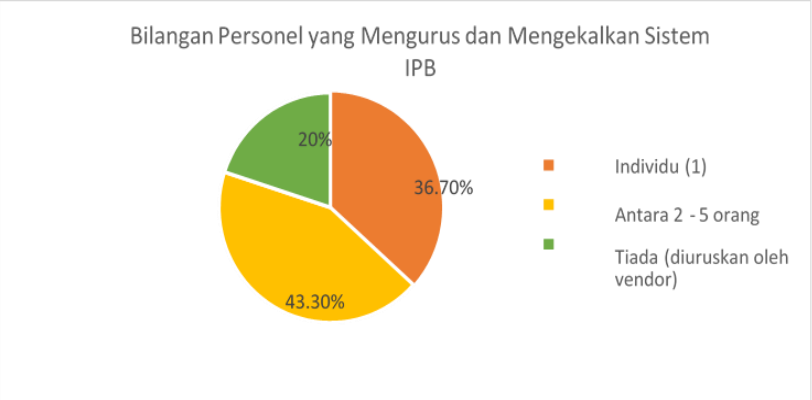
4.3 Analisis Seksyen B (Profil Personel)

Tempoh	**Tempoh Bekerja (Peratus %)**	**Tempoh Pengalaman Teknikal (Peratus %)**	**Tempoh Terlibat dengan IPB (Peratus %)**	**Keterlibatan dengan IPB (Peratus%)**
Kurang 1 tahun	13.3	13.3	23.3	-
1 – 5 tahun	76.7	60	73.3	-
6 – 10 tahun	10	23.3	3.3	-
Lebih 10 tahun	0	3.3	0	-
Pemula	-	-	-	56.7
Pertengahan	-	-	-	40.0
Mahir	-	-	-	3.3%
Jumlah	100	100	100	100

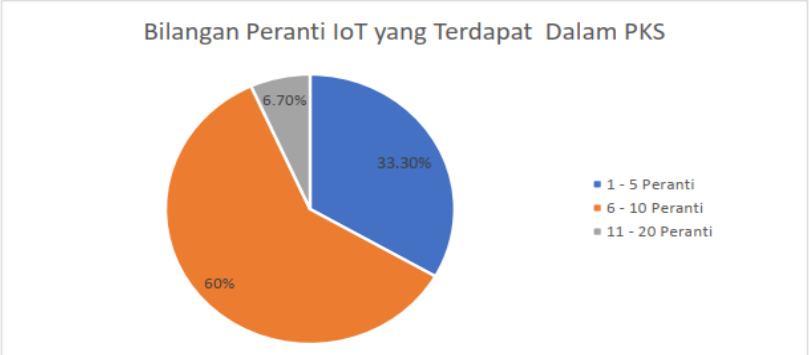
Jadual 4.2 di atas menggambarkan tempoh pengalaman personel dari segi pekerjaan, teknikal serta tempoh dan tahap penglibatan dengan IPB. , penyelidik mendapati bahawa majoriti

responden iaitu sebanyak 56.7% daripada responden mempunyai tahap pengetahuan keselamatan siber di tahappemula. Hasil tinjauan penyelidik mendapati bahawa hal ini berlaku kerana respondendi tahap ini menyatakan mereka mempunyai asas keselamatan siber di mana mereka mempunyai pengetahuan asas mengenai perlindungan ke atas endpoint seperti antivirus atau perlindungan rangkaian seperti dinding api.

4.4 Analisis Seksyen C (Ekosistem IPB)

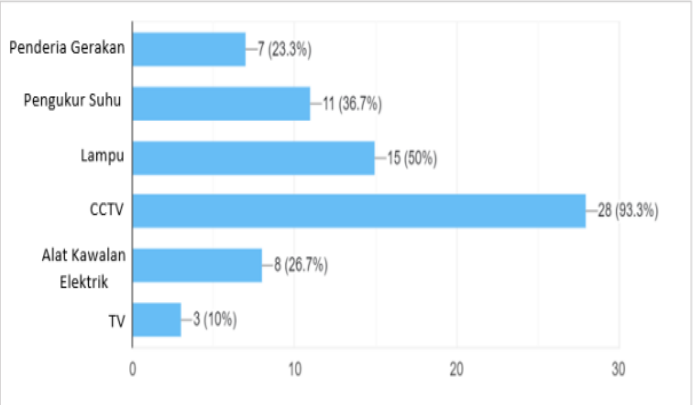


Tinjauan penyelidik mendapati sebanyak 43.3% daripada responden mempunyai antara 2 – 5 personel yang membangun dan mengekalkan sistem IPB. Hasil tinjauan penyelidik mendapati tiada lebih dari seorang individu yang menguruskan sistem IPB kerana responden berpendapat PKS hanya syarikat kecil dan hanya memerlukan asas keselamatan IT, oleh itu pelaburan untuk tenaga kerja manusia tidak banyak. Di samping itu, penyelidik mendapati 20% daripada PKS tiada individuyang menguruskan sistem IPB dalam premis kerana mereka menyerahkan tugasan tersebut kepada vendor sebagai salah satu cara '*outsourcing'* dan penjimatan kos.

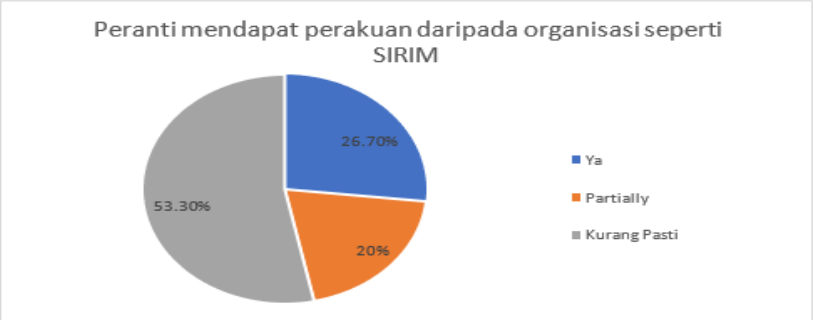


Hasil kajian mendapati peratusan bilangan IPB yang terbanyak dalam PKS adalah sebanyak 60% daripada responden iaitu 6 – 10 peranti. Penyelidik mendapati PKS ini menggunakan sistematau peranti IPB yang boleh membantu melancarkan proses perniagaan

seharian seperti automasi bil contohnya dalam servis kurier. Namun begitu, penyelidik berpendapat, besar atau kecil bilangan peranti IPB, perlindungan daripada terdedah dari kelemahan adalah satu perkara yang penting untuk dipraktikkan.



Penyelidik mendapati kebanyakan PKS mempunyai Kamera Litar Tertutup (CCTV) iaitu sebanyak 93.3% daripada responden. Menurut pandangan responden, CCTV yang digunakan mempunyai fungsi asas IPB yang menghubungkan kamera tersebut dengan aplikasi di telefon bimbit yang membolehkanmereka memantau keadaan premis perniagaan melalui telefon bimbit sahaja.

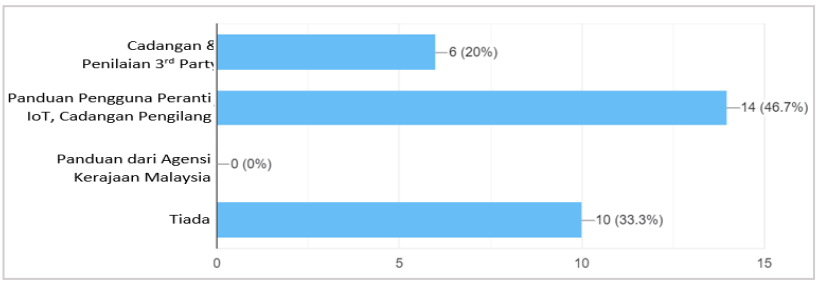


Hasil kajian mendapati sebanyak 53.3% daripada responden menyatakan mereka kurang pasti jika peranti yang digunakan telah diperakukan oleh SIRIM atau tidak. Hal ini kerana responden mengakui mereka tidak menyedari yang peranti IPB turut perlu diberikan perhatian dari segi perakuan badan- badan yang diiktiraf untuk mengelakkan berlaku serangan sekiranya peranti diletakkandalam rangkaian seperti *botnet* atau malware.

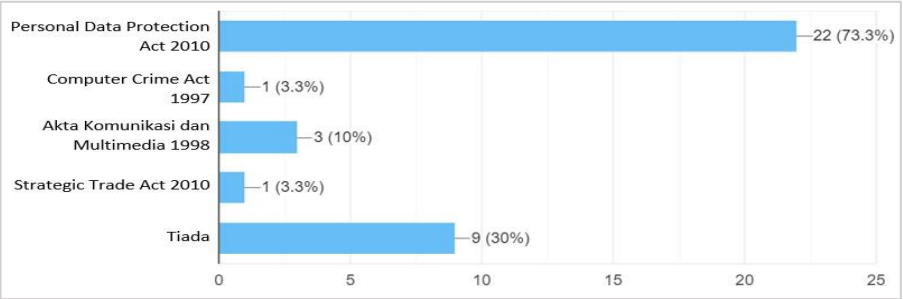
4.4 Analisis Seksyen D (Senario Keselamatan IPB)

Isu keselamatan IPB dalam premis perniagaan	**Median**	**Tahap**
Kerahsian	4.00	Tinggi
Integriti	4.00	Tinggi
Ketersediaan	4.00	Tinggi
Pengesahan	4.00	Tinggi
Kawalan Akses	4.00	Tinggi
Privasi	4.00	Tinggi
Kebolehpercayaan	4.00	Tinggi
Penguatkuasaan dasar	3.00	Sederhana

Kerahsiaan berada di tahap kebimbangan yang tinggi kerana responden sedar mengenai isu kerahsiaan data dan perlindungan terhadap data. Integriti berada di tahap yang tinggi kerana responden mengetahui bahawa data dan maklumat dalam sistem perlu dikekalkan dan mengelakkan daripada akses yang tidak dibenarkan. Namun, penguatkuasaan polisi hanya berada di tahap yang sederhana. Tinjauan penyelidik mendapati tidak semua PKS mengaplikasikan polisi keselamatan maklumat dan beranggapan bahawa asas keselamatan rangkaian sudah mencukupi.

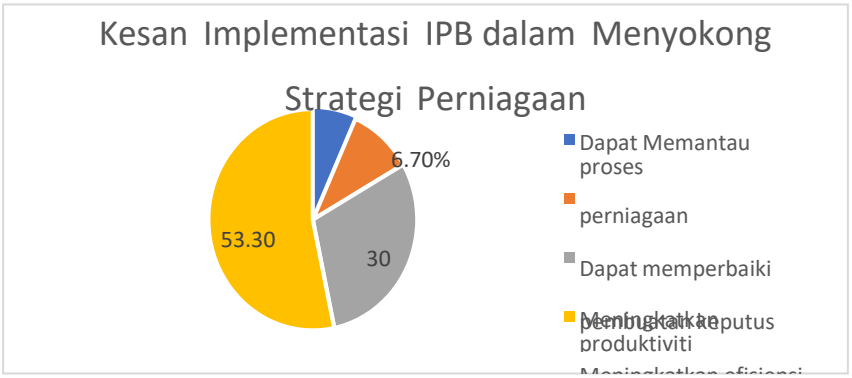


46.7% daripada responden memilih dan menyatakan mereka merujuk kepada panduan Pengguna peranti IPB dan Cadangan pengilang ketika melakukan pemasangan peranti IPB. Hal ini disebabkan panduan tersebut merupakan manual untuk memasang peranti yang sudah sedia ada pada peranti tersebut, jadi responden tidak perlu bersusah payah mencari dan merujuk panduan lain.

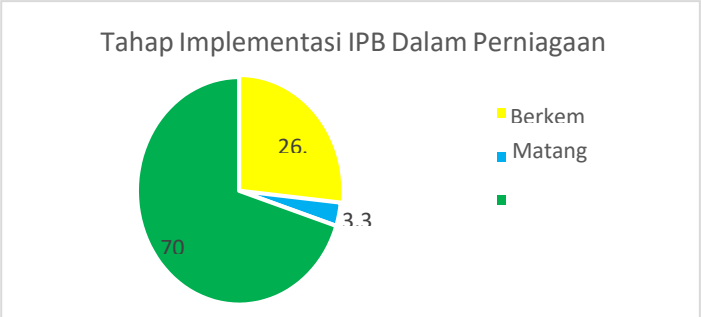


73.3% daripada responden menyatakan bahawa mereka tahu akan kewujudan Akta Perlindungan Data Peribadi 2010 (PDPA) kerana akta ini merupakan akta yang bukan asing lagi di Malaysia. Namun, 30% daripada responden tidak mengetahui akta atau undang-undang keselamatan informasi ini. Hal ini mungkin kerana mereka tidak didedahkan dengan pengetahuan mengenai akta tersebut. Akhir sekali, *Computer Crime Act 1997* dan *Strategic Trade Act 2010*, masing-masing mencatatkan 3.3% daripada responden kerana kebanyakan responden tidak ada pengetahuan tentang akta berkenaan kerana penggunaannya yang kurang meluas.

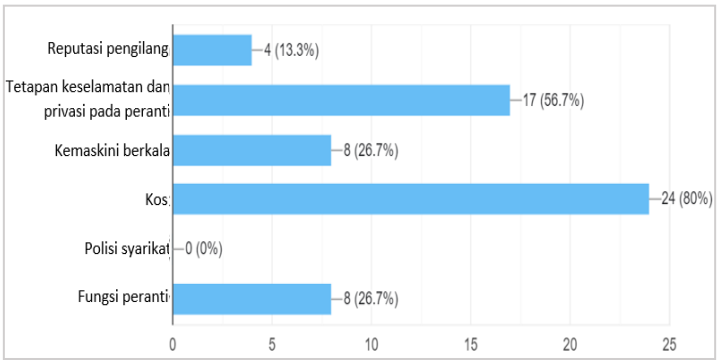
4.5 Analisis Seksyen E (IPB dan Strategi Perniagaan)



Sebahagian besar responden iaitu sebanyak 53.3% merekodkan implementasi teknologi IPB dapat meningkatkan produktiviti. Penyelidik mendapati penggunaan sistem IPB dapat menambahbaik pengurusan inventori dan penjejakan asset. Dalam sektor pembuatan, ia juga dapat menambahbaik perolehan seperti perolehan bahan mentah dan penggunaan IPB boleh memberi notifikasi sekiranya bekalan bahan mentah di bawah tahap rendah.



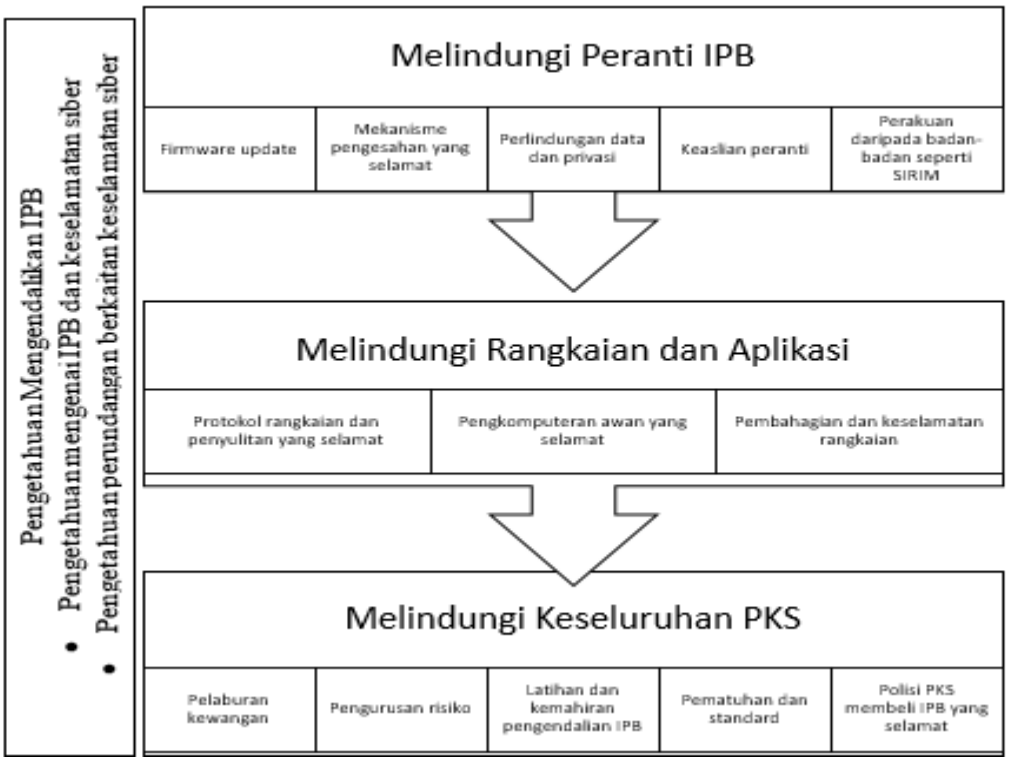
Berdasarkan Rajah 4.19, penyelidik mendapati bahawa sebilangan besar iaitu seramai 70% daripada responden yang terlibat dalam kajian ini menyatakan impelementasi IPB dalam perniagaan mereka berada di tahap pengenalan. Hasil tinjauan penyelidik mendapati PKS di tahap ini hanya menggunakan peranti yang asas, tanpa kawalan keselamatan seperti pengimbas suhu.



Majoriti responden iaitu sebanyak 80% daripada responden memilih kos peranti sebagai kriteria utama dalam pembelian peranti IPB. Menurut tinjauan penyelidik bersama responden, kos menjadi factor utama kerana polisi syarikat dan pengurusan yang tidak mahu memberi peruntukan lebih untuk membeli peranti IPB yang lebih selamat dan bagus. Responden juga mengakui mereka cenderung untuk membeli dari hub-hub penjualan atas talian seperti Shopee dan Lazada kerana kos efektif. Responden percaya kos yang tinggi boleh mempengaruhi kualiti sesebuah peranti.

4.6 Kerangka Keselamatan IPB di PKS

Berdasarkan analisis deskriptif dan kerangka konseptual yang di bina pada awal kajian, dalam bahagian ini, penyelidik telah membangunkan sebuah kerangka keselamatan IPB dalam PKS dengan menyediakan beberapa komponen yang dipadankan dengan dari kerangka konseptual dengan hasil kajian daripada analisis deskriptif. Rajah 4.21 merujuk kepada kerangka IPB yang dibangunkan.



Rajah 4: Kerangka Konseptual Keselamatan IPB dalam PKS

Penyelidik mencadangkan untuk menambah komponen pengetahuan. Kajian ini mencadangkan pengetahuan PKS mengenai IPB dan keselamatan siber serta pengetahuan PKS mengenai perundangan yang melibatkan keselamatan siber seperti Akta Perlindungan Data dan Privasi 1987. Penyelidik berpendapat bahawa komponen pengetahuan ini penting bagi PKS dan personel yang menguruskan PKS bagi melindungi ekosistem IPB khususnya. Tanpa pengetahuan, ekosistem IPB boleh terdedah kepada ancaman siber.

5.0 KESIMPULAN DAN CADANGAN

5.1 Pencapaian Objektif dan Sumbangan Kajian

a. Mengenalpasti senario keselamatan IPB dalam PKS

Melalui sorotan kajian susastera yang dijalankan, penyelidik telah menganalpasti ancaman siber terhadap IPB dalam perniagaan iaitu ancaman Penafian Perkhidmatan, serangan *jamming*, kecurian data, perisian tebusan dan sebagainya. Antara faktor penyumbang kepada berlakunya ancaman siber seperti yang disebutkan adalah keranabeberapa faktor. Antaranya, kelemahan kata kunci keselamatan, penyimpanan data yang tidak selamat dan kelemehan melindungi peranti secara fizikal.

Tidak dinafikan dalam mengendalikan sesebuah IPB ekosistem yang selamat, terdapatpelbagai cabaran yang perlu diambil kira sebelum pelaksanaan. Cabaran pelaksanaan IPB yang selamat yang dihasilkan dalam kajian ini boleh dibahagikan kepada tiga komponen utama mengikut senibina IPB iaitu, cabaran dari segi peranti IPB, rangkaian dan aplikasi IPB serta melindungi PKS secara keseluruhan.

b. Membina kerangka keselamatan IPB

Melalui hasil kajian daripada penelitian dari literatur, penyelidik dapat mengenalpastirangka kerja yang boleh diaplikasi oleh PKS dalam melaksanakan IPB yang selamat. Terdapat empat kategori pembahagian mengikut kegunaan IPB dalam PKS iaitu; merujuk rangka kerja IPB sebagai rangka kerja yang matang, dijelaskan dengan baik dan khusus, sebagai keselamatan tambahan dalam peranti dan proses perniagaan, sebagai senarai semak untuk menambahbaik keselamatan IPB dan rangka kerja yang kurang formal namun memerlukan rekomendasi yang baik. Daripada sorotan kajian susatera yang dibuat, penyelidik mengeluarkan faktor-faktor kritikal yang boleh diaplikasikan dalam keselamatan IPB dan pemetaan dibuat kepada komponen yang penting untuk melindungi IPB. Oleh itu, satu kerangka konseptual yang menggabungkan komponen senibina IPB yang selamat iaitu cabaran melindungi peranti, rangkaian dan aplikasi serta PKS secara keseluruhan telah dibina dengan faktor-faktor kritikal yang perlu di ambil kira dalam membina satu ekosistem IPB yang selamat dalam PKS. Tambahan, komponen pengetahuan turut ditambah sebagai satu komponen penting dalam kerangka mewujudkan sebuah IPB yang selamat.

5.2 Batasan Kajian

Ketika kajian dijalankan, terdapat beberapa kekangan yang dihadapi penyelidik. Penyelidik menggunakan kaedah dokumentasi dari rangka kerja, prosedur atau garis panduan yang telah sedia ada dan menganalisis dapatan kajian iaitu rekomendasi dan jurang dokumen-dokumen tersebut. Kajian dijalankan juga terhad kepada penggunaan IPB yang selamat dalam industri PKS sahaja. Penyelidik mendapati tidak banyak kajian yang pernah dijalankan dalam konteks Keselamatan IPB dalam PKS, khususnya dari segi rekomendasi dan analisis jurang dari kajian yang sedia ada.

Rujukan

Alaba, F., Othman, M., Hashem, I., & Alotaibi, F. (2017). Internet Pelbagai Benda security: A survey. *Journal of Network and Computer Applications*, 10-28.

Albăstroiu, I. (2021). Challenges of IPB Technologies for Businesses and Consumers. *Amfiteatru Economic*, 321-323.

AlFuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet Pelbagai Benda: Survey on Enabling Technologies, Protocols and Applications. *IEEE Communication Surveys and Tutorials*, 2347-2370.

Andreica, G., Bozga, L., Zinca, D., & Dobrota, V. (2020). Denial of service and man-in- the-middle attacks against IPB devices in a GPS-based monitoring software for intelligent transportation systems. *RoEduNet Conference: Networking in Education and Research (RoEduNet).*

Assan, L. (2018). *POTENSI INTERNET SALING BERHUBUNG (INTERNET PELBAGAI BENDA) DALAM INDUSTRI PEMBINAAN DI MALAYSIA.* Johor Bahru: Universiti Teknologi Malaysia .

Assan, L. (2018). Potensi Internet Saling Berhubung (Ionternet of Things) dalam Industri Pembinaan di Malaysia. 22-24.

Atoui, R. (25 April, 2018). *The Importance of Security by Design for IPB*. Retrieved fromIIPB World: https://www.iIPB-world.com/ics-security/cybersecurity/the-importance-of-security-by-design-for-IPB-devices/#:~:text=Hardware%2C%20software%20and%20connectivity%20will,steal%20the%20user's%20digital%20data.

AWS. (2023). *IPB Lens: AWS Well-Architected Framework.* Retrieved from Amazon Web Services: https://docs.aws.amazon.com/wellarchitected/latest/IPB-lens/firmware- updates.html

Bahadur, P. (12 June, 2014). *Difference Between Guideline, Procedure, Standard and Policy*. Retrieved from LinkedIn: https://www.linkedin.com/pulse/20140611162901-223517409-difference-between- guideline-procedure-standard-and-policy/

Balbix. (2022). *IPB Security Challenges and Problems*. Retrieved from Balbix: https://www.balbix.com/insights/addressing-IPB-security-challenges/

Bangsgaard, M. (28 April, 2020). *Harnessing Technology to Accelerate Digitalisation.* Retrieved from SME Corp: https://www.smecorp.gov.my/index.php/en/resources/2015-12-21-10-55- 22/news/4141-harnessing-technology-to-accelerate-digitalisation

Bhandhari, P. (14 May, 2020). *Population vs Samples: Definitions, Definitions and Examples*. Retrieved from Scribbr:

Cresswell, J. W. (2009). *Research Design: Qualitative, Quantitative and Mixed Method Approach.* Thousand Oaks, California: SAGE.

Crotty, M. (1998). *The foundation of social research: meaning and perspective in the research process.* Thousand Oaks, California: SAGE .

Cybersecurity Malaysia. (2011). *Information Security Guidelines for Small and Medium Enterprises (SMEs).* Kuala Lumpur: Cybersecurity Malaysia.

Cybersecurity Malaysia. (5 May , 2020). *Guidelines for Secure Internet Pelbagai Benda.* Retrieved from Cybersecurity Malaysia: https://www.cybersecurity.my/data/content_files/56/2074.pdf

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet Pelbagai Benda Architecture, Possible Applications and Key Challenges. *Conference Paper*. doi:DOI: 10.1109/FIT.2012.53

Kocakulak, M., & Ismail, B. (2017). An Overview of Wireless Sensor Networks towards Internet Pelbagai Benda. *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 504-509). IEEE.

Palo Alto. (2023). *What is IPB Security?* Retrieved from Palo Alto Networks: https://www.paloaltonetworks.com/cybersecurity#:~:text=IPB%20security%20can%20be%20understood,are%20connected%20to%20the%20network.

Patel, K. K.,& Patel, S. M. (2016). Internet Pelbagai Benda -(IPB): Definition, Characteristics, Architecture, Enabling Technologies, Applications and Future Challenges. *International Journal of Engineering Science and Computing*, 6122-6123.

Preedy, V.R., Watson, R.R. (eds) (2010). 5-Point Likert Scale. *Handbook of Disease Burdens and Quality of Life Measures*. Springer, New York, NY. https://doi.org/10.1007/978-0-387-78665-0_6363

Weinberg, A. (5 October, 2021). *Top 5 Enterprise IPB Security Challenges*. Retrieved fromFirst Point: https://www.firstpoint-mg.com/blog/top-5-enterprise-IPB-security- challenges/

World Economic Forum. (2020). *Accelerating the Impact of Industrial IPB in Small and Medium Sized Enterprises: A Protocol for Action.* Geneva: World Economic Forum.

Yaung, D., & Merritt, J. (2020). *IPB Can Help Small and Medium Business Implemen t Sustainability Measure*.

Retrieved from World Economic Forum: https://www.weforum.org/agenda/2022/07/IPB-small-medium-businesses- profitable-sustainable/

Yildirim, M., Senol, B., & Demiroglu, U. (2021). An in-depth exam of IPB, IPB Core Components, IPB Layers, and Attack Types. *European Journal of Science and Technology*, 665-669.