PELAN TINDAKAN KESELAMATAN
INTERNET OF THINGS (IoT)

MUHAMMAD SHAFIQ BIN AHMAD

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT MEMPEROLEH IJAZAH SARJANA SAINS KOMPUTER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2018

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

26 Disember 2017 MUHAMMAD SHAFIQ BIN AHMAD
GP04285

PENGHARGAAN

Syukur ke hadrat ilahi kerana dengan limpah dan kurnia-nya, akhirnya saya berjaya menyiapkan projek tahun akhir ini. Setinggi-tinggi penghargaan saya tujukan kepada Dr. Khairul Akram Zainol Ariffin selaku penyelia projek di atas bimbingan, pandangan dan nasihat beliau sepanjang saya membangunkan projek ini. Ucapan penghargaan ini turut ditujukan kepada para pensyarah di Fakulti Teknologi Dan Sains Maklumat atas segala didikan, nasihat dan ilmu yang dicurahkan sepanjang pengajian Sarjana saya di UKM. Selain itu, jutaan terima kasih saya rakamkan khas buat ahli keluarga yang banyak memberi sokongan dan dorongan yang tidak berbelah bahagi kepada saya. Tidak lupa juga kepada rakan-rakan seperjuangan yang turut memberi sokongan moral, motivasi dan bantuan sepanjang saya menyiapkan projek ini.
Sekian, terima kasih.

ABSTRAK

Kertas ini mencadangkan sebuah modul penyelesaian masalah keselamatan bagi teknologi rangkaian yang memfokuskan kepada penggunaan konsep *Internet of Things* (IoT). Motif kajian ini dilakukan adalah untuk memberi kesedaran terhadap risiko keselamatan penggunaan teknologi IoT, dan bagaimana risiko ini dapat ditangani melalui pelan tindakan keselamatan yang bersesuaian. Pelbagai modul pelan tindakan yang dicadangkan adalah berasaskan teori dan strategi keselamatan bagi memelihara tahap keselamatan rangkaian serta data pengguna. Namun, skema sedia ada tidak memfokuskan kepada aspek keselamatan pada rangka kerja Internet of Things secara menyeluruh. Skop pengajian yang dilakukan adalah berdasarkan beberapa elemen penting dalam struktur asas seni bina teknologi IoT, iaitu lapisan aplikasi, rangkaian, dan fizikal. Maklumat berkenaan risiko keselamatan dan pelan tindakan bagi menangani masalah tersebut akan disenaraikan mengikut lapisan seni bina teknologi IoT. Pelan tindakan yang dicadangkan akan memfokuskan kepada penambahbaikan terhadap piawaian ITU-T. Konsep pelan tindakan yang berasaskan lapisan seni bina IoT dapat memberi kemudahan kepada pengguna untuk lebih memahami teknik penyelesaian berdasarkan risiko yang dialami.

SECURITY ACTION PLAN FOR INTERNET OF THINGS

ABSTRACT

This paper proposes a modular security solution for network technology that focuses on the concept of the Internet of Things (IoT). The motive of this study is to provide awareness of the security risks of using IoT technology, and how these risks can be addressed through appropriate safety action plan. Various modules of the proposed action plan is based on theory and strategy for maintaining the security of network security and user data. The scope of study is based on several key elements of the basic structure of IoT technology architecture, the application layer, network, and physical. Information regarding a security risk and an action plan to address the issue will be listed according to the technology architecture of IoT. Draft action plan based layer IoT architecture can provide convenience to the user to better understand the technical solution based on the risks incurred.

KANDUNGAN

SENARAI JADUAL

SENARAI ILUSTRASI

SENARAI SIMBOL/SINGKATAN/TATANAMA/ISTILAH

No.	Istilah	Singkatan
1	*Internet of Things*	IoT
2	Sistem Antara Sambungan Terbuka / *Open Systems Interconnection*	OSI
3	*Transmission Control Protocol*	TCP
4	Protokol Internet / *Internet Protocol*	IP
5	*Denial of Service*	DoS
6	*Distributed Denial of Service*	DDoS
7	Pelayan Nama Domain / *Domain Name Servers*	DNS
8	Protokol Datagram Pengguna / *User Datagram Protokol*	UDP
9	*Radio Frequency Identification*	RFID
10	Mesin-ke-Mesin	M2M
11	Kesatuan Telekomunikasi Antarabangsa	ITU
12	Protokol Internet Versi 4 / *Internet Protocol Version 4*	IPv4
13	Protokol Internet Versi 6 / *Internet Protocol Version 6*	IPv6
14	Rangkaian Sensor Tanpa Wayar */ Wireless sensor networks*	WSN
15	Pengecam Unik Universal / *Universal Unique Identifiers*	UUID
16	Standard Enkripsi Maju / *Advanced Encryption Standard*	AES
17	Algoritma Enkripsi Data Antarabangsa / *International Data Encryption Algorithm*	IDEA
18	*Software Defined Networking*	SDN
19	Organization-based Access Control	OrBAC
20	Smart Organization-based Access Control	SmartOrBAC
21	Kesatuan Telekomunikasi Antarabangsa - Telekomunikasi	ITU-T
22	Pertubuhan Bangsa Bersatu	UN
23	Pertubuhan Standardisasi Antarabangsa	ISO
24	Suruhanjaya Elektroteknikal Antarabangsa	IEC
25	Teknologi Maklumat	IT
26	IoT-*Architecture*	IoT-A
27	Pasukan Petugas Kejuruteraan Internet	IETF
28	Lembaga Seni Bina Internet	IAB
29	IPv6 – Rangkaian Peribadi Tanpa Wayar Berkuasa Rendah	6LoWPAN
30	Protokol Aplikasi Terkekang / *Constrained Application Protocol*	CoAP
31	Institut Jurutera Elektrik dan Elektronik	IEEE
32	*Telecommunication Industry Association*	TIA
33	*Alliance for Telecommunications Industry Solutions*	ATIS
34	*Association of Radio Industry and Business*	ARIB
35	*Telecommunications Technology Committee*	TTC
36	Kumpulan Kerja / Working Group	WG
37	*Hypertext Transfer Protocol*	HTTP
38	*Message Queue Telemetry Transport*	MQTT
39	Institut Piawaian Telekomunikasi Eropah	ETSI
40	Spesifikasi Teknikal	TS
41	Asas Pengurusan Maklumat */ Management Information Base*	MIB
42	*Time-Slotted Channel Hopping*	TSCH
43	*Resource Location and Discovery*	RELOAD
44	*Open Mobile Alliance Device Management*	OMADM
45	*Light-Weight Machine to Machine*	LWM2M
46	*Open Interconnect Consortium*	OIC
47	*Open Connectivity Foundation*	OCF
48	*Routing Protocol for Low-Power and Lossy Networks*	RPL

GLOSARI

Bahasa Inggeris	Bahasa Melayu	Penerangan
Algorithm	Algoritma	Set langkah bagi kod komputer untuk menyelesaikan sesuatu tugasan.
Application	Aplikasi	Barisan kod komputer yang direka untuk menjalankan tugasan spesifik.
Architechture	Seni Bina	Model seni bina dan reka bentuk sesebuah sistem.
Attacker Node	Nod Penyerang	Nod yang mewakili penyerang sistem
Authentication	Pengesahan	Proses pengesahan bagi memastikan pengguna yang mendapat akses ke sistem, merupakan pengguna sah dan berdaftar.
Authentication Certificates	Sijil Autentikasi	Sejenis pasport elektronik yang membenarkan pengguna, peranti, atau komputer untuk mengesahkan diri mereka kepada sistem.
Backdoors	Pintu Belakang	Cubaan akses ke dalam sistem komputer tanpa melalui mekanisma keselamatan.
Bluetooth	Bluetooth	Sambungan rangkaian tanpa wayar yang membolehkan peranti untuk berhubung antara satu sama lain.
Comparative	Komparatif	Berdasarkan perbandingan
Computer Worms	Cacing Komputer	Virus yang berupaya untuk mereplikasi diri dan berfungsi mengurangkan jumlah memori aktif pada sistem komputer.
Conotation	Konotasi	Idea yang dimaksudkan oleh sesuatu perkataan atau ungkapan.
Constrained	Dikekang	Disekat atau tidak mempunyai akses penuh
Constrained Application Protocol (CoAP)	Protokol Aplikasi Terkekang	Sebuah protokol penghantaran yang digunakan bersama nod dikekang dan rangkaian dikekang pada teknologi IoT.
Cryptography	Kriptografi	Sebuah cara penyimpanan dan penghantaran data pada sesuatu format di mana hanya pengguna yang mempunyai kunci kepada data tersebut boleh mendapat akses.
Data	Data	Sebarang maklumat yang disimpan di dalam komputer.
Data Mining	Perlombongan Data	Proses penyusunan maklumat dan data besar bagi mengenal pasti bentuk atau pola tertentu bertujuan bagi meramal sesuatu trend.
De Facto	Dengan Fakta	Pada hakikatnya yang berlandaskan fakta
De Jure	Dengan Hak	Menurut Undang-undang
Decryption	Dekripsi	Proses menukar data yang disimpan dalam format ciphertext kepada data umum.
Encryption	Enkripsi	Proses menukar data umum kepada format ciphertext.
Ethernet	Ethernet	Sejenis teknologi rangkaian yang mempunyai kelajuan transmisi menghala ke julat gigabit.
Exploit	Eksploit	Serangan terhadap sistem komputer yang mengambil kesempatan terhadap sebarang kelemahan pada reka bentuk sistem tersebut.

Firmware	Firmware	Pengaturcaraan yang terletak di memori storan tidak menentu pada peranti teknologi.
Gateway	Gerbang	Sebuah pintu masuk yang membenarkan transmisi antara sistem berlaku.
Node	Nod	Unit atau peranti elektronik yang mempunyai sambungan kepada rangkaian.
Open Systems Interconnection Model (OSI)	Sistem Antara Sambungan Terbuka	Model konsep yang menerangkan fungsi komunikasi di antara sistem komputer dan lapisan struktur dalaman teknologi tersebut.
Original User Node	Nod Pengguna Asli	Nod yang mewakili pengguna asal
Protocol	Protokol	Sebuah persetujuan yang memantau sebarang prosedur yang digunakan dalam proses pertukaran maklumat yang melibatkan beberapa entiti.
Real-time	Kadar Semasa	Pemprosesan transaksi maklumat yang dilakukan secara serentak mengikut lingkungan masa.
RFID Tag	Label RFID	Sistem pengesahan yang menggunakan peranti berteknologi radio berfrekuensi rendah bagi proses pengesahan dan menjejak.
Spoofing	Spoofing	Teknik pemalsuan data atau maklumat komputer bagi menggambarkan mesej tersebut datangnya dari pengguna asal.
Wireless Technology	Teknologi Wayarles	Teknologi yang menghubungkan peranti dan rangkaian komputer tanpa menggunakan sambungan fizikal atau wayar.
Working Group (WG)	Kumpulan Kerja	Kumpulan individu yang mempunyai peranan tersendiri dalam pelaksanaan tugas.
Working Node	Nod Bekerja	Nod yang mewakili proses yang berlaku di dalam sistem rangkaian IoT.

BAB 1

PENGENALAN

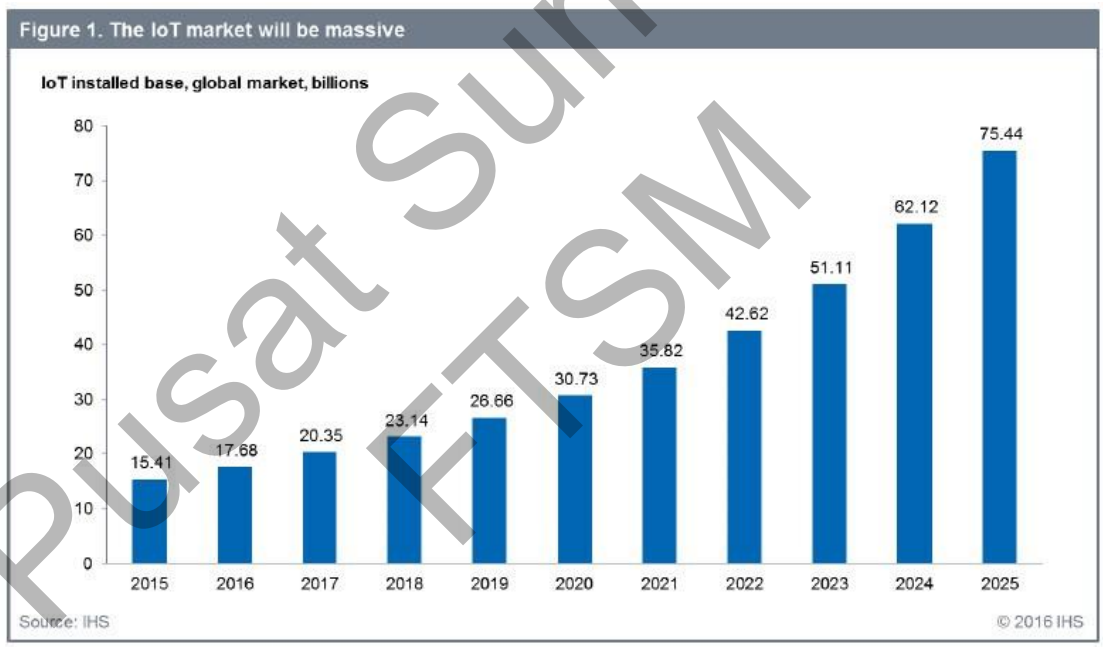
1.1 PENDAHULUAN

Di alaf teknologi maklumat ini, penggunaan Internet telah menjadi unsur yang penting dalam pelbagai bidang contohnya perindustrian, pembelajaran, perubatan, dan automotif. Perkembangan ini selaras dengan hasrat kerajaan untuk menjadikan Malaysia sebuah negara celik teknologi supaya sejajar dengan visi menjelang tahun 2020. Sehubungan itu, hampir kebanyakan barangan serta peralatan teknologi yang digunakan oleh manusia pada waktu ini disambungkan secara terus ke Internet melalui konsep teknologi "Internet of Things (IoT)".

Konsep IoT yang diperkenalkan oleh Kevin Ashton pada tahun 1998 membawa satu visi di mana setiap barangan serta peranti dapat berhubung antara satu sama lain melalui pemasangan *transceiver* mudah alih-jarak dekat, sekaligus membentuk satu dimensi komunikasi antara manusia dan peralatan teknologi (Santucci 2009). Selain itu, teknologi IoT mampu mengaktifkan peranti elektronik melalui fungsi perkongsian maklumat di antara peranti-peranti di dalam rangkaian tanpa memerlukan interaksi dari pengguna (Singh 2014).

Kelebihan IoT dalam membantu mengurangkan jurang antara pengguna dan teknologi dapat dilihat dalam pelbagai konteks, antaranya adalah menerusi industri pembuatan, industri automotif, pendidikan, dan kesihatan. Menurut agensi IHS, aplikasi yang dibangunkan melalui teknologi IoT merangkumi sistem pengawalan kualiti di kilang pembuatan dan teknologi kereta pintar pada industri automotif.

Menurut kajian yang dijalankan oleh agensi IHS pada 2016, mereka meramalkan bahawa penggunaan teknologi IoT bakal meningkat dan menjelang tahun 2025, diramalkan jumlah pasaran global IoT bakal berjumlah sebanyak 75.44 Bilion. Rajah di bawah memaparkan hasil kajian berkenaan pasaran global IoT dari agensi tersebut.



Rajah 1.1: Ramalan Pasaran Global IoT
(Sumber: https://www.ihs.com/Info/0416/internet-of-things.html)

Namun begitu, penggunaan teknologi IoT yang meluas dapat memberi kesan negatif terhadap pengguna terutamanya faktor keselamatan rangkaian, dan kebocoran maklumat peribadi serta privasi mereka (Gupta 2016). Di samping itu, alatan peranti IoT yang mempunyai sambungan rangkaian Internet lebih terdedah kepada risiko untuk digodam serta serangan siber (Andrea 2015).

Projek ini bertujuan untuk mencari kesan negatif penggunaan teknologi "Internet of Things (IoT)" terhadap aspek keselamatan pengguna dan mencadangkan jalan penyelesaian dalam menambah-baik faktor keselamatan.

Kertas kajian ini akan membincangkan tahap keselamatan rangkaian dalam penggunaan teknologi IoT, serta menerangkan keperluan bagi membincangkan aspek keselamatan penggunaan dimensi IoT yang kian meluas. Ini amat penting kerana sebarang teknologi yang asing atau baru memerlukan sebuah modul langkah keselamatan bagi memelihara taraf integriti teknologi tersebut.

Pemfokusan terhadap penambahbaikan tahap integriti pada teknologi IoT ditekankan di dalam projek ini kerana majoriti peranti dan aplikasi IoT tidak direka untuk menangani serangan terhadap faktor rangkaian IoT seperti; kerahsiaan maklumat, proses autentikasi pengguna, integriti terhadap data maklumat, dan kawalan akses pada peranti IoT.

1.2 PENYATAAN MASALAH

Setelah membuat pemerhatian dan kajian kertas ilmiah, dapat dirumuskan bahawa penggunaan dan pemahaman konsep teknologi IoT masih di peringkat awal dan masih terdapat banyak risiko serta kes-kes berkaitan faktor keselamatan rangkaian yang boleh memberi impak negatif terhadap pengguna. Masalah yang dihadapi sehingga mencetuskan idea penghasilan modul keselamatan IoT adalah berkenaan:-

a) Kurangnya pemahaman terhadap konsep dan penerapan aspek keselamatan dalam penggunaan teknologi rangkaian IoT.

b) Modul keselamatan IoT sedia ada yang kurang menitik beratkan integrasi keselamatan infrastruktur IoT bermula dari lapisan rangkaian hingga ke lapisan aplikasi pengguna.

Menurut kajian yang dijalankan oleh agensi Gartner pada 2016, mereka meramalkan bahawa jumlah perbelanjaan khusus bagi sektor keselamatan IoT bakal meningkat sehingga mencecah 547.20 juta Dollar US menjelang tahun 2018. Rajah di bawah memaparkan hasil kajian tersebut:

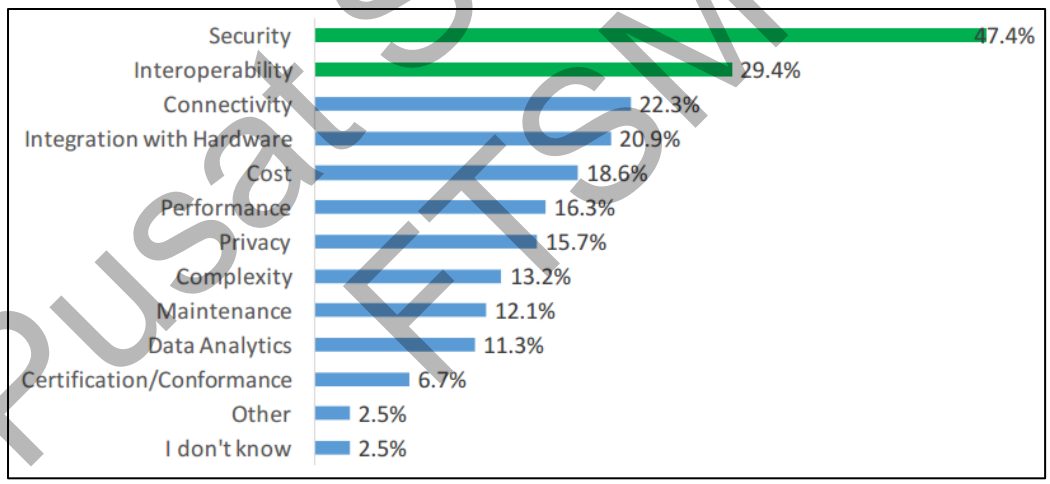
Worldwide IoT Security Spending Forecast (Millions of Dollars)

2014	2015	2016	2017	2018
231.86	281.54	348.32	433.95	547.20

Rajah 1.2 Ramalan Perbelanjaan Keselamatan IoT
(Sumber: http://www.gartner.com/newsroom/id/3291817)

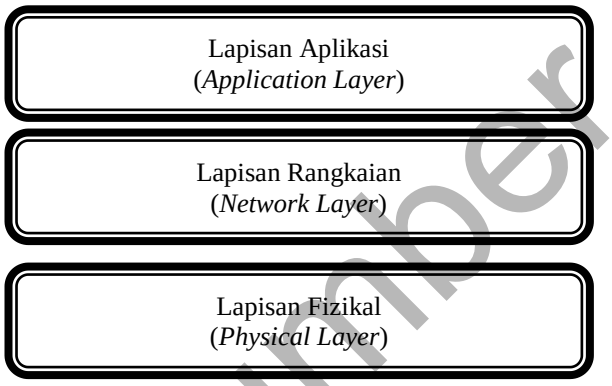
Selain itu, menurut kajian yang dijalankan oleh Farooq pada tahun 2015, beliau mendapati bahawa piawaian keselamatan sedia ada tidak merangkumi keseluruhan faktor keselamatan IoT iaitu, faktor keselamatan Fizikal, Rangkaian, Aplikasi, dan Enkripsi data pengguna serta peranti IoT. Sehubungan itu, perbandingan berkenaan kelebihan dan kekurangan di antara piawaian keselamatan perlu dilakukan bagi menghasilkan sebuah modul piawaian yang memfokuskan terhadap kesemua faktor keselamatan IoT.

Permasalahan tersebut juga disokong oleh kajian yang dijalankan oleh Institut Jurutera Elektrik dan Elektronik (IEEE) bertajuk "*IoT Developer Survey"* pada tahun 2016, mereka telah merumuskan bahawa isu keselamatan merupakan faktor tertinggi yang patut diberi fokus dalam pembangunan solusi IoT. Rajah 1.3 menunjukkan hasil kajian yang dijalankan oleh pihak IEEE berkenaan isu-isu penting berkenaan teknologi IoT.



Rajah 1.3 Isu-Isu Penting Berkaitan IoT
(Sumber: http://iot.ieee.org/images/files/pdf/iot-developer-survey-2016-report-final.pdf)

Bagi menjamin aspek keselamatan rangkaian dalam keadaan terbaik, konsep asas IoT yang membabitkan implementasi dan integrasi antara teknologi rangkaian serta infrastruktur rangkaian perlu difahami secara mendalam (Andrea 2015). Rajah 1.3 memaparkan struktur asas seni bina teknologi IoT yang terdiri daripada 3 lapisan iaitu: Aplikasi, Rangkaian, dan Fizikal (Song 2013).



Rajah 1.4 Seni Bina Teknologi Internet of Things (IoT)

Masalah keselamatan rangkaian dapat didapati pada setiap lapisan struktur senibina IoT, contohnya (Suo 2012):-

1.2.1 Lapisan Aplikasi *(Application Layer)*

Lapisan aplikasi adalah salah satu contoh lapisan di dalam model Sistem Antara Sambungan Terbuka (OSI), dan di dalam suit *Transmission Control Protocol/Internet Protocol* (TCP/IP). Ia terdiri daripada protokol yang memberi tumpuan kepada proses komunikasi yang merentasi rangkaian IP dan menyediakan sebuah perkhidmatan komunikasi antara-muka dan servis pengguna. Contoh risiko keselamatan pada lapisan aplikasi ini adalah berpunca daripada virus, *worms*, spyware, adware, dan serangan *Denial of Service* (DoS).

1.2.2 Lapisan Rangkaian *(Network Layer)*

Lapisan rangkaian merupakan lapisan ketiga dalam model OSI yang berfungsi dalam menyediakan laluan sambungan data bagi komunikasi rangkaian. Data dipindahkan dalam bentuk paket melalui rangkaian logik melalui format yang dikawal oleh aplikasi rangkaian. Contoh risiko keselamatan yang terdapat pada lapisan rangkaian adalah RFID *Spoofing & Cloning***,** *Man In The Middle Attack, dan* Serangan Analisis Trafik

1.2.3 Lapisan Fizikal *(Physical Layer)*

Lapisan fizikal merupakan lapisan pertama bagi model OSI. Lapisan fizikal berfungsi sebagai penghubung antara peranti yang berlainan dan menyokong antara muka elektrikal atau mekanikal yang mempunyai sambungan kepada medium fizikal untuk penyelarasan komunikasi. Jenis serangan ini tertumpu kepada perkakasan komponen sistem IOT dan penyerang perlu mempunyai akses secara fizikal ke dalam sistem IOT untuk serangan ini berfungsi. Antara risiko keselamatan yang terdapat pada tahap lapisan fizikal adalah risiko pengubahan nod ragkaian, Gangguan Frekuensi Radio, dan Suntikan Kod Berbahaya.

1.3 OBJEKTIF KAJIAN

Kajian ini dilaksanakan bertujuan bagi mencadangkan sebuah garis panduan pelan tindakan keselamatan bagi infrastruktur rangkaian IoT yang meliputi 3 lapisan iaitu aplikasi, rangkaian, dan fizikal. Sehubungan itu, objektif dan tujuan kajian ini dilaksanakan adalah untuk:-

a. Mengenal pasti kelemahan penggunaan teknologi "*Internet of Things (IoT)"* terhadap aspek keselamatan rangkaian.

b. Membangunkan sebuah pelan tindakan keselamatan teknologi "*Internet of Things (IoT).*

Demi mencapai objektif tersebut, kajian dan analisis terhadap rujukan kesusasteraan berkenaan pelan dan modul keselamatan rangkaian IoT terdahulu telah dilaksanakan.

1.4 SKOP KAJIAN

Skop kajian melibatkan keperluan terhadap pembentukan model pelan tindakan keselamatan rangkaian IoT. Model ini dicadangkan dengan tujuan untuk dijadikan sebagai panduan dan galakan kepada sesiapa sahaja yang ingin menggunakan teknologi rangkaian IoT pada masa hadapan. Model pelan tindakan ini akan memfokuskan kepada masalah keselamatan yang terdapat pada 3 lapisan rangkaian IoT iaitu:-

a. Lapisan fizikal;
b. Lapisan rangkaian; dan
c. Lapisan aplikasi.

Sampel maklumat yang digunakan dalam penyediaan panduan ini berasaskan kertas-kertas jurnal, buku, serta maklumat dari laman sesawang dalam lingkungan tahun 2000 hingga 2016. Berdasarkan objektif kajian, penilaian dan dapatan sampel akan dilaksanakan bagi mengenal pasti kelemahan yang terdapat pada teknologi IoT dari segi aspek keselamatan data pengguna serta keselamatan rangkaian.

Pelan tindakan yang dibina akan berdasarkan beberapa model piawaian sedia ada bagi teknologi IoT, seperti ITU-T, IEEE, IETF, dan OneM2M. Seterusnya model piawaian keselamatan sedia ada akan dianalisis bagi mengenal pasti teknik keselamatan terbaik berdasarkan 3 lapisan infrastruktur IoT. Hasil daripada analisis ini akan dihimpunkan bagi membina satu model keselamatan IoT yang merangkumi infrastruktur lapisan Aplikasi, Rangkaian, dan Fizikal.

1.5 FAEDAH PROJEK

Dengan berlangsungnya projek ini, satu modul pelan tindakan bagi meningkatkan keselamatan rangkaian bagi teknologi IoT dapat dirangka. Cadangan pelaksanaan ini dapat memberi gambaran bagaimana langkah-langkah untuk memperketat keselamatan seni bina infrastruktur IoT bermula dari lapisan fizikal hingga ke lapisan aplikasi. Dengan penyenaraian beberapa permasalahan berkenaan IoT, seterusnya akan memberi idea bagi pelaksanaan kajian yang lebih mendalam untuk mengurangkan masalah pelaksanaan IoT pada masa hadapan.

1.6 KESIMPULAN

Bahagian ini telah membincangkan pengenalan terhadap kajian dan objektif yang bakal dicapai sepanjang projek ini berlangsung. Bahagian ini juga turut menyentuh pelbagai perkara berkaitan dengan kepentingan untuk menghasilkan satu modul cadangan bagi menangani masalah terhadap penggunaan teknologi IoT. Zaman teknologi maklumat dan komunikasi telah mengubah persepsi dan pendekatan pengguna yang lebih menjurus kepada teknologi mudah alih. Sejajar dengan perubahan teknologi, risiko serta ancaman keselamatan terhadap alatan mudah alih yang menyokong penggunaan konsep IoT kian meningkat.

BAB 2

KAJIAN KESUSASTERAAN

2.1 PENGENALAN

Kajian kesusasteraan ini dilakukan untuk mengkaji kajian yang sedia ada untuk tujuan mendapat maklumat serta penambahbaikan untuk projek yang ingin dijalankan. Kajian kesusasteraan turut membolehkan maklumat yang diperoleh daripada jurnal, dokumen, dan kajian-kajian yang lepas dapat diulas dan dijadikan rujukan. Dengan kajian ini, sesuatu projek yang ingin dijalankan turut dapat ditinjau dan dikenal pasti sama ada telah dilaksanakan atau tidak oleh individu lain.

Daripada hasil pemerhatian yang telah dijalankan, didapati bahawa buat masa kini, penggunaan teknologi IoT adalah meluas, akan tetapi tahap kesedaran pengguna terhadap risiko keselamatan penggunaan teknologi ini amat rendah. Walaupun terdapat beberapa kajian terhadap IoT yang telah dilakukan, masih tiada kajian yang mencadangkan modul penyelesaian yang khusus bagi menangani masalah berhubung penggunaan teknologi ini. Kajian terhadap modul keselamatan terdahulu juga dilakukan bagi menghasilkan perbandingan serta mencadangkan penambahbaikan bagi modul yang ingin dibangunkan.

2.2 DEFINISI ISTILAH

2.2.1 Definisi *Internet Of Things* (IoT)

Istilah 'Internet of Things' pertama kali disebutkan oleh Kevin Ashton pada tahun 1999 (Ashton 2009). Tetapi konsep itu mula menjadi lebih jelas pada pembentangan mereka di Institut Teknologi Massachusetts (MIT) Auto-ID mengenai visi IoT pada tahun 2001. Teknologi IoT menawarkan sambungan antara manusia kepada sambungan komunikasi mesin-ke-mesin (M2M). Di mana, sambungan komunikasi dilakukan melalui rangkaian dan sensor yang mampu mengumpul maklumat pada kadar semasa (*real-time*). Maklumat ini seterusnya akan dianalisis untuk membantu tugasan membuat keputusan.

Kemudian, IOT telah diperkenalkan secara rasmi oleh Kesatuan Telekomunikasi Antarabangsa (ITU) dalam laporan Internet ITU pada tahun 2005. Kelebihan yang bakal dicapai melalui penggunaan teknologi ini adalah meluas, antaranya adalah memberi impak pada sektor pendidikan, kesihatan, perumahan, komunikasi, pengangkutan, pembandaran, perniagaan, sains, sektor kerajaan, dan lain-lain (Elbouanani 2015).

Walau bagaimanapun, terdapat beberapa isu yang mampu mengancam pembangunan IoT timbul, seperti faktor privasi dan risiko keselamatan dalam teknologi ini, tempoh peralihan daripada penggunaan IPv4 kepada IPv6, keperluan untuk mempunyai satu set standard umum untuk pengendalian serta pengurusan data yang banyak (Evans 2011).

2.3 TEKNOLOGI UTAMA YANG MEMBOLEHKAN IOT

Bagi merealisasikan penggunaan teknologi ini, IoT menggunakan pelbagai teknologi rangkaian yang sedia ada seperti:-

2.3.1 Pengecaman Frekuensi Radio / *Radio frequency identification (RFID)*

Teknologi RFID menggunakan frekuensi radio membolehkan mikrocip untuk menghantar data melalui medium tanpa wayar. Mereka menggunakan tag (label) yang diletakkan pada objek yang bertindak sebagai pengesan automatik atau kod bar elektronik. Tag RFID wujud dalam dua jenis yang berbeza, sama ada dalam bentuk pasif atau aktif. Tag RFID pasif tidak menggunakan bateri, mereka mendapat kuasa untuk berkomunikasi daripada isyarat soal siasat alat pengesan ID ke alat bacaan RFID. Manakala, tag RFID aktif mempunyai bekalan bateri mereka sendiri dan boleh memulakan proses komunikasi.

2.3.2 Rangkaian Sensor Tanpa Wayar / *Wireless sensor networks (WSN)*

WSN terdiri daripada peranti kecil yang ditempatkan secara autonomi, kos rendah, dan peranti kecil kuasa rendah yang menggunakan sensor untuk memantau keadaan persekitaran secara fizikal. Sistem WSN menggabungkan gerbang (*gateway*) yang menyediakan sambungan tanpa wayar kembali ke sambungan berwayar dan edaran nod.

2.3.3 *Cloud Computing*

Cloud computing membolehkan perkhidmatan penderiaan sentiasa ada, dan pemprosesan berkuasa terhadap data penderiaan dapat dilaksanakan untuk proses penyimpanan dan penggunaan secara autonomi bagi tujuan pemantauan pintar (*smart monitoring)*. Secara umumnya, penggunaan teknologi *cloud computing* khusus bagi memudahkan tugasan pengagihan sumber pengkomputeran bagi tujuan aplikasi teknologi maklumat dan pusat data.

2.4 STRUKTUR INTERNET OF THINGS (IOT)

Struktur asas bagi IoT meliputi 3 lapisan daripada model OSI, iaitu lapisan aplikasi, lapisan rangkaian, dan lapisan fizikal (Song 2013).

2.4.1 Lapisan Aplikasi

Lapisan aplikasi ini berorientasikan perkhidmatan, di mana ia memastikan semua peranti yang disambungkan mendapat jenis perkhidmatan yang sama (Khan 2012). Lapisan aplikasi juga berfungsi untuk menyimpan maklumat ke dalam pangkalan data, sekiranya diberikan ruangan penyimpanan untuk data yang telah dikumpulkan. Selain itu, lapisan aplikasi juga berupaya untuk memudahkan proses komunikasi peranti yang berorientasikan sistem bergantung kepada keperluan pengguna (Gubbi 2013). Contoh aplikasi yang mampu membantu aktiviti seharian pengguna adalah, aplikasi Smart Home, eHealth, Pengangkutan Smart, Objek Pintar, dan lain-lain.

2.4.2 Lapisan Rangkaian

Sama seperti mana-mana model OSI yang sedia ada, lapisan rangkaian ini merangkumi pecahan seperti rangkaian antara muka, saluran komunikasi, rangkaian pengurusan, penyelenggaraan maklumat, dan pemprosesan bijak. Lapisan ini bertanggungjawab terutamanya dalam proses komunikasi dan penyambungan peranti di dalam sistem IoT melalui sokongan beberapa protokol komunikasi (Yang 2012). Pada ketika ini, tidak ada sebarang protokol standard yang dicadangkan bagi penggunaan teknologi IoT, akan tetapi protokol yang paling kerap digunakan adalah protokol sambungan "*Machine-to-machine (M2M)/"Internet of Things"* MQTT 3.1.1 (Hunkler 2008) dan Protokol Kekangan Aplikasi (CoAP) (Shelby 2014).

Maklumat yang dikumpulkan dari Lapisan Fizikal akan dihantar ke mana-mana sistem pemprosesan maklumat di dalam rangkaian yang sama, menggunakan Sensor Wayarles atau menggunakan infrastruktur komunikasi sedia ada seperti Internet atau Rangkaian Mudah Alih (Yick 2008). Setiap peranti fizikal di dalam sistem IoT biasanya akan menghantar maklumatnya dengan menggunakan teknologi sensor tanpa wayar.

Sensor yang digunakan ini mempunyai saiz yang lebih kecil, kuasa pemprosesan terhad, dan penggunaan tenaga elektrik yang lebih rendah sebagai sumber kuasa pengkomputeran. Data yang diterima daripada sensor ini akan diproses, dihantar secara wayarles, dan dibentangkan kepada pengguna akhir. Justeru itu, fungsi lapisan rangkaian secara dasarnya adalah sebagai medium yang membantu dalam proses pengasingan, penyambungan laluan komunikasi daripada pelbagai sumber peranti (Gubbi 2008).

2.4.3 Lapisan Fizikal

Lapisan paling bawah bagi seni bina teknologi IoT pada dasarnya bertanggungjawab untuk menghubungkan peranti secara sambungan fizikal. Alat-alat sambungan peranti ini boleh didapati dalam pelbagai jenis, contohnya (Arduino, ZigBee, Raspberry). Bagaimanapun, untuk menjadikan sambungan peranti ini menyokong teknologi IoT, mereka perlu mempunyai medium komunikasi rangkaian yang bakal membolehkan mereka untuk berhubung sama ada secara langsung atau secara tidak langsung menggunakan internet.

Sambungan melalui peranti Arduino memerlukan sambungan Ethernet, manakala Pi Raspberry menggunakan sambungan Wi-Fi, Bluetooth, dan sambungan radio kuasa rendah (Fremantle 2014). Di samping itu, setiap peranti perlu mempunyai tag yang unik yang membolehkan ia untuk berjaya mempunyai sambungan ke rangkaian. Menurut P. J. Leach, Pengecam Unik Universal/*Universal Unique Identifiers* (UUID) boleh digunakan untuk peranti yang berbeza di seluruh Internet yang perlu ditetapkan ke peranti IoT, melalui *Sistem-on-Chip* (Song 2010).

2.4.4 Protokol IoT

Walaupun seni bina sistem IoT adalah sama dengan yang Stack TCP/IP, ia tidak menggunakan protokol yang sama pada tiap-tiap lapisan kerana peranti yang terdapat dalam IoT menggunakan sumber kuasa yang rendah. Telah menjadi keperluan untuk peranti IoT terus beroperasi pada tempoh yang panjang tanpa memerlukan sebarang kuasa tambahan. Oleh itu, semakin kurang kuasa, semakin kurang potensi proses komputasi pada sesebuah peranti. Oleh itu, protokol standard TCP/IP tidak sesuai dan sub-optimal untuk menampung ciri-ciri dan cabaran penggunaan teknologi IoT. Ini menimbulkan kebimbangan keselamatan kerana kekurangan asas keselamatan bagi protokol IoT, dan piawaian keselamatan terbuka IoT masih lemah berbanding Stack Protokol TCP/IP.

2.5 RISIKO KESELAMATAN TERHADAP PENGGUNAAN IOT

Keselamatan rangkaian merupakan salah satu konsep penting dalam konteks keselamatan data, kerana data yang akan dimuat naik perlu dalam keadaan selamat (Liu. Et al., 2012). Bagi menjamin tahap keselamatan maklumat terjamin, terdapat beberapa algoritma keselamatan yang diterbitkan antaranya ialah Standard Enkripsi Maju/*Advanced Encryption Standard* (*AES*), dan Algoritma Enkripsi Data Antarabangsa/*International Data Encryption Algorithm* (*IDEA*).

Risiko ancaman keselamatan yang kerap berlaku terhadap teknologi IoT adalah berpunca daripada RFID dan sensor peranti (Gupta, 2016). Jadual 2.1 memaparkan contoh senarai ancaman keselamatan yang berpunca daripada penggunaan RFID.

Jadual 2.1 Senarai Ancaman Keselamatan RFID

Mod Serangan Keselamatan	**Penerangan**
Serangan Replikasi *(Replication Attack)*	Proses menyalin atau memalsukan label RFID mangsa.
Sekatan Saluran *(Channel Blocking)*	Penyerang akan menduduki siaran masa panjang dan komunikasi yang sah tidak boleh dipindahkan.
Serangan Pemalsuan *(Forgery Attack)*	Label RFID yang sah boleh didapati menggunakan fasiliti *hardware* khas atau tiruan.
Serangan Penyamaran *(Impersonation Attack)*	Penyerang akan menyamar sebagai pembaca yang sah untuk mencuri atau mengubah maklumat pada tag RFID.
Serangan Mengganggu *(Tampering Attack)*	Penyerang ini akan mengubah suai maklumat sebelum signal sampai ke alat penerima.

Menurut Xingmei., 2013, ancaman keselamatan yang boleh didapati berpunca daripada rangkaian sensor meliputi serangan keselamatan *Link-layer, Witch Attack, HELLO Flooding Attack,* dan siaran autentifikasi. Lapisan yang menghubungkan pengguna dan teknologi IoT melalui paparan antara muka, dikenali sebagai lapisan aplikasi. Lapisan aplikasi bertanggungjawab dalam proses mendapatkan data berguna melalui penggunaan teknologi *data mining*, pengkomputeran awan, pengecaman *fuzzy*, dan pelbagai teknologi pengkomputeran bagi memproses maklumat serta memberi maklumat secara efektif.

Di samping itu, menurut kertas kajian yang dilakukan oleh Heer pada tahun 2011, beliau mendapati bahawa masalah keselamatan kerap berlaku pada lapisan aplikasi seperti masalah dalam memilih kandungan pangkalan data yang sama mengikut kelebihan akses yang berbeza, memberikan perlindungan privasi maklumat pengguna, menyelesaikan masalah kebocoran maklumat, mengambil maklumat forensik komputer, memusnahkan data komputer, melindungi produk elektronik, dan perisian harta intelek. Jadual 2.2 memaparkan klasifikasi serangan terhadap teknologi IoT.

Jadual 2.2 Klasifikasi Serangan Terhadap IoT

Serangan Fizikal	**Serangan Rangkaian**	**Serangan Perisian**	**Serangan Enkripsi**
Pengubahan Nod	Serangan Analisis Trafik	Virus dan *Worms*	Serangan Saluran Sampingan
Gangguan Frekuensi Radio	RFID *Spoofing*	*Spyware* dan *Adware*	Serangan *Man In The Middle*
Sleep Deprivation Attack	Serangan Sybil	*Trojan Horse*	Serangan Kriptoanalisis: • *Ciphertext* • *Plaintext* • *Chosen Plaintext / Ciphertext*
Suntikan Nod Berbahaya	Pengklonan RFID	Skrip Berbahaya	
Kerosakan Fizikal	Serangan DoS	Serangan DoS	

2.6 SKEMA PENGESAHAN DAN KAWALAN AKSES PERANTI IoT

Bahagian ini akan menerangkan mengenai skema pengesahan dan kawalan akses terhadap peranti IoT. Turut diberikan contoh kajian terdahulu yang menyumbang kepada penubuhan skema keselamatan rangkaian teknologi IoT.

2.6.1 *Heterogenous Identity-Based Scheme* (Salman et al.)

Salman et al. telah mencadangkan sebuah skema pengesahan IoT yang dinamakan "*heterogenous identity-based"*yang mengaplikasikan konsep rangkaian perisian yang ditakrifkan (*Software Defined Networking, SDN)* terhadap peranti IoT. SDN boleh diaplikasikan menggunakan nod taburan berkabus. Ini bermaksud, setiap set perisian IoT akan berkomunikasi dengan *gateway* yang akan melakukan proses pengesahan keaslian terhadap peranti tersebut.

Sekuriti *gateway* ini bersambung secara langsung dengan pusat kawalan yang mempunyai akses ke pusat data. Proses pengesahan ini dilakukan melalui *gateway* dan pusat kawalan bagi mendapatkan akses ke peranti IoT. Aliran mesej di antara ketiga-tiga peringkat ini (peranti IoT, *gateway* kawalan, dan pusat kawalan) berlaku dalam 3 fasa. Fasa pertama merangkumi proses mendapatkan sijil autentikasi ke *gateway* kawalan daripada pusat kawalan. Seterunya, fasa kedua merangkumi proses pendaftaran terhadap *gateway* kawalan. Akhir sekali, fasa ketiga yang berfungsi untuk mendapatkan permohonan autentikasi yang dihantar dari peranti IoT kepada *gateway* kawalan.

2.6.2 PAuthKey (Porambage et al.)

Porambage et al. telah mencadangkan satu protokol pengesahan autentikasi secara meluas dan skema penubuhan yang dinamakan PAuthKey (*A Pervasive Aunthentication Protocol and Key Establishment Scheme*). Tujuan skema ini adalah bagi kegunaan aplikasi IoT yang mempunyai fungsi sebagai sekatan sumber terhadap rangkaian sensor tanpa wayar. Protokol PAuthKey yang dicadangkan oleh Porambage merangkumi 2 fasa iaitu:-

a. **Fasa Pendaftaran**: Mendapatkan serta mendaftar maklumat kriptografi pada perisian IoT.

b. **Fasa Pengesahan**: Mengesahkan dan mewujudkan kunci keselamatan bagi tujuan komunikasi antara perisian dan aplikasi IoT.

Kelebihan penggunaan protokol ini akan membolehkan pengguna untuk membuat proses pengesahan terhadap peranti mereka ke sensor secara terus bagi mendapatkan maklumat serta servis IoT. Protokol ini menyokong penggunaan pada aplikasi IoT yang pelbagai, disebabkan perakuan yang dibuat adalah bersifat mudah dan boleh dikawal oleh peranti yang menggunakan sumber yang tinggi, tanpa mengira faktor keaslian mereka.

2.6.3 Teknik Pemindahan Pelajaran (Sharaf et al.)

Menurut kajian yang dilakukan oleh Sharaf et al., beliau mendapati bahawa setiap peranti IoT mempunyai proses pengesahan autentikasi yang menggunakan data unik pada peranti tersebut. Menurut Sharaf, ciri-ciri data unik yang terdapat dalam sesebuah peranti IoT adalah seperti maklumat lokasi peranti, keadaan fizikal peranti, dan keadaan pemancar peranti IoT tersebut. Setiap kumpulan peranti IoT mungkin mempunyai maklumat ciri-ciri cap jari yang berbeza. Oleh sebab itu, teknik konvensional pengesahan cap jari peranti tidak boleh dilakukan terhadap peranti IoT.

Menurut rumusan dari kajian yang dilakukan oleh Sharef et al., beliau mengesyorkan penggunaan teknik pemindahan pelajaran (*transfer learning)*, bagi proses pengesahan peranti yang mempunyai ciri-ciri data unik yang berbeza. Bagi mengaplikasikan idea ini, kajian beliau dilakukan melalui dua (2) pendekatan. Pertamanya, proses pengesahan akan dibuat terhadap mesej yang dihantar oleh peranti tunggal. Seterusnya, ia akan mengesahkan keaslian peranti IoT yang menghantar mesej tersebut bagi mengelakkan pemalsuan mesej yang berpunca dari penipuan peranti.

2.6.4 Algoritma Penangkis Serangan DDoS (Zhang et al.)

Algoritma yang dicadangkan beliau meliputi proses mengenal pasti masalah keselamatan pada setiap nod rangkaian yang berpotensi diserang melalui teknik DDoS. Kajian yang dilaksanakan oleh Zhang et al. bertujuan bagi menangkis serangan DDoS terhadap peranti IoT yang mempertimbangkan rangkaian meliputi 4 kumpulan nod iaitu: nod bekerja, nod pemantauan, nod pengguna asli, dan nod penyerang.

Nod bekerja dianggap sebagai peranti yang akan mengumpul maklumat dan melaksanakan tugasan mudah. Nod ini mempunyai memori bagi urusan komputasi, memori storan, dan kekangan sumber tenaga. Bagi menangkis serangan DDoS, nod bekerja perlu membezakan antara mesej *malicious* atau mesej asli. Sekiranya terdapat peranti yang telah menghantar mesej yang sama berulang kali, maklumat identifikasi peranti tersebut akan dikenal pasti dan disimpan di dalam senarai perkhidmatan penghantaran yang telah berjaya bagi proses semakan untuk membezakan antara mesej dari penyerang dan mesej dari pengguna.

Senarai tersebut hendaklah mempunyai saiz fail yang kecil kerana kekangan storan pada peranti IoT. Oleh itu, pengguna asli perlu menghantar mesej permintaan pada kadar frekuensi rendah dan kandungan yang munasabah. Merujuk kepada algoritma yang dicadangkan oleh Zhang, mesej yang dihantar dari penyerang hanya mempunyai satu (1) peluang untuk dihantar secara jayanya. Ini kerana sekiranya terdapat cubaan kali kedua dari penyerang, ID penyerang tersebut akan dimasukkan ke dalam senarai penyerang, dan semua paket dari ID penyerang tersebut akan digugurkan. Simulasi terhadap kajian yang dilakukan berjaya membuktikan bahawa algoritma tersebut efektif dalam usaha mengenal pasti dan menghindari serangan DDoS.

2.6.5 *Smart Organization-based Access* Control, SmartOrBAC (Bouij et al.)

Kajian yang dilaksanakan oleh Bouij et al.telah telah dinamakan sebagai model pengawalan akses kebenaran (SmartOrBAC) yang merupakan penambahbaikan kepada model kawalan akses berasaskan organisasi (OrBAC) supaya dapat memenuhi kriteria rangkaian yang terdapat pada teknologi IoT. Ciri-ciri yang terdapat dalam model ini adalah konsep konteks peka, fungsi kolaborasi, dan pembahagian struktur rangkaian IoT kepada empat (4) lapisan abstrak:-

a. **Dikekang**: Mempunyai perisian di mana beberapa keupayaannya atau fungsi utamanya dikekang dan tidak berfungsi secara penuh.

b. **Kurang kekangan**: Perisian yang dikelaskan sebagai kurang kekangan dikaitkan dengan kumpulan pada komponen lapisan pertama untuk menjalankan tugas sebagai petugas pengiraan secara intensif di dalam domain keselamatan yang sama.

c. **Lapisan organisasi**: Lapisan ini memberi penerangan secara spesifik berkenaan polisi akses keselamatan bagi setiap kumpulan klien dan sumber organisasi. Lapisan organisasi juga bertanggungjawab dalam menstrukturkan kumpulan tersebut kepada domain keselamatan yang berbeza.

d. **Lapisan kolaborasi**: Lapisan yang terakhir ini berfungsi dalam mengukuhkan lagi model akses OrBAC dengan penambahan konsep berkaitan kolaborasi. Lapisan ini bertanggungjawab dalam mewujudkan persetujuan dan peraturan merentasi kawalan akses domain.

Berdasarkan penilaian yang dijalankan, model ini lebih mudah dan kurang kompleks berbanding model berdasarkan keupayaan. Model ini juga merendahkan risiko berlakunya kesilapan dan menambah baik pengurusan kos polisi keselamatan.

2.7 BADAN ORGANISASI PIAWAIAN KESELAMATAN IoT

Badan organisasi piawaian IoT boleh diklasifikasikan mengikut beberapa kriteria yang spesifik. Pada seksyen ini, dua (2) kriteria yang akan digunakan untuk memperkenalkan badan piawaian IoT adalah tahap sumbangan dan kewibawaan organisasi tersebut. Berikut merupakan contoh badan piawaian bagi teknologi IoT pada masa kini:-

2.7.1 Kesatuan Telekomunikasi Antarabangsa - Telekomunikasi (ITU-T)

ITU merupakan organisasi global nombor satu yang bernaung di bawah Pertubuhan Bangsa Bersatu (UN) yang bertanggungjawab dalam hal ehwal telekomunikasi. ITU-T pula merupakan organisasi pertama yang memulakan langkah penubuhan piawaian IoT sejak tahun 2005.

2.7.2 Pertubuhan Standardisasi Antarabangsa / Suruhanjaya Elektroteknikal Antarabangsa (ISO/IEC JTC1)

ISO merupakan salah satu badan organisasi piawaian antarabangsa yang terkenal serta diyakini oleh majoriti negara di dunia. Manakala IEC pula berfungsi sebagai organisasi antarabangsa yang menubuhkan piawaian bagi barangan elektronik, elektrik, dan komunikasi. Oleh itu, tujuan gabungan antara ISO & IEC melalui gabungan komiti teknikal adalah bagi memastikan IEC mampu mencipta, mengekalkan, mempromosi, dan memudahkan piawaian IT.

2.7.3 Institut Piawaian Telekomunikasi Eropah (ETSI)

ETSI merupakan sebuah organisasi bebas yang bertanggungjawab bagi industri telekomunikasi di Eropah. Piawaian Mesin-ke-Mesin (M2M) yang dibangunkan oleh ETSI merupakan tapak asas bagi piawaian OneM2M. Di Eropah, struktur spesifikasi IoT dilaksanakan melalui projek Senibina-IoT (IoT-A). ETSI merupakan organisasi piawaian utama bagi tujuan pembangunan piawaian teknologi IoT-A.

2.7.4 Pasukan Petugas Kejuruteraan Internet (IETF)

Pasukan Petugas Kejuruteraan Internet, IETF merupakan organisasi piawaian yang membangunkan piawaian Internet di bawah kelolaan Lembaga Seni Bina Internet (IAB). Mereka merupakan sebuah organisasi piawaian bebas, tanpa sebarang keahlian formal dan syarat pendaftaran.

Piawaian yang berkaitan dengan teknologi IoT adalah menjurus ke arah IPv6 – Rangkaian Peribadi Tanpa Wayar Berkuasa Rendah (6LoWPAN). Selain itu, IETF juga bertanggungjawab dalam pembikinan Protokol Aplikasi Terkekang (CoAP) yang lazim digunakan pada rangkaian komunikasi IoT.

2.7.5 Institut Jurutera Elektrik dan Elektronik (IEEE)

Organisasi piawaian IEEE merupakan organisasi profesional yang diiktiraf dalam membangunkan piawaian kebangsaan bagi Amerika Syarikat. Organisasi ini diasaskan bagi tujuan pelaksanaan piawaian pembangunan bagi kejuruteraan elektronik, elektrik, dan komputer. IEEE bertanggungjawab mengasaskan IEEE P2413TM WG pada tahun 2014 yang bertujuan mengawal selia tugasan berkaitan teknologi IoT.

2.7.6 OneM2M

Organisasi piawaian OneM2M merupakan sebuah gabungan agensi piawaian yang ditubuhkan secara bersama oleh 8 agensi antaranya ETSI, TIA *Telecommunication Industry Association (TIA), Alliance for Telecommunications Industry Solutions (ATIS) of USA, Association of Radio Industry and Business (ARIB), dan Telecommunications Technology Committee (TTC).*

OneM2M merupakan organisasi yang menggubal standard piawaian khusus bagi teknologi IoT. Mereka mempunyai 4 kumpulan kerja (WG) yang mempunyai tanggungjawab berbeza dalam penggubalan piawaian teknologi IoT. WG1 bertanggungjawab menggubal keperluan standard bagi servis IoT, WG2 pula bertugas dalam menghasilkan standard reka bentuk dan entiti rangkaian IoT. Manakala, WG3 bertanggungjawab dalam menggubal piawaian bagi protokol yang digunakan oleh teknologi IoT seperti *Hypertext Transfer Protocol* (HTTP), CoAP, *Message Queue Telemetry Transport* (MQTT), dan lain-lain. Akhir sekali, WG4 bertugas dalam menggubal standard keselamatan sebagai wakil kepada kumpulan kerja (WG). Jadual 2.3 memaparkan ringkasan analisis berkenaan peranan organisasi piawaian terhadap fungsi penggubalan piawaian bagi teknologi IoT .

Jadual 2.3 Analisis Peranan & Sumbangan Organisasi Piawaian Terhadap Piawaian Teknologi IoT

Klasifikasi		**Organisasi**	**Kandungan Keselamatan IoT**
Tahap Sumbangan	**Tahap Penguatkuasaan**		
Antarabangsa	Dengan Hak (*De Jure*)	ITU-T	• Keperluan keselamatan terhadap pelbagai rangka kerja IoT yang melibatkan proses Pengesahan, Pengenalan, Kawalan Akses, dan Perlindungan Privasi. • Perlindungan data dan privasi bagi aplikasi IoT.
		ISO/IEC JTC1	• Keselamatan bagi antaramuka rangkaian aplikasi Sensor
Rantau	Dengan Fakta (*De Facto)*	ETSI	• Sama seperti OneM2M
Kebangsaan		IETF	• Pengesahan, Enkripsi/Deskripsi, Pemberian kebenaran, kawalan akses bagi 6LoWPAN dan CoAP bagi peranti sumber terhad. • Keselamatan bagi TSCH & RELOAD
		OneM2M	• Keselamatan reka bentuk fungsian IoT bagi proses kawalan akses, pengesahan dan kebenaran. • Keperluan keselamatan IoT secara menyeluruh. • Reka bentuk keselamatan IoT bagi TLS & DTLS • Piawaian keselamatan bagi HTTP, MQTT, CoAP, dan *WebSocket Binding*. • Keselamatan bagi peranti pengurusan teknologi (Cth: OMA, DM, LWM2M) • Kawalan akses bagi ujian kesalingfungsian. • Kawalan akses bagi AllJoyn & seni bina OIC.

2.8 KESIMPULAN

Penggunaan internet telah mengubah gaya kita hidup secara drastik, ia memberi impak tinggi dalam mengatur bagaimana kita berkomunikasi, bekerja, dan berinovasi. Sehingga kini, tahap kepekaan terhadap isu keselamatan dan privasi berkaitan IoT masih diabaikan dan ia boleh menjadi isu utama yang boleh menjejaskan pembangunan teknologi IoT. Cabaran itu adalah untuk menentukan prinsip-prinsip dan rangka kerja bagi mengawal selia aspek pembangunan IoT dengan menerapkan tahap keselamatan dan privasi yang tinggi. Sehubungan itu, jadual di bawah menerangkan secara ringkas berkenaan kelebihan dan kekurangan yang terdapat pada piawaian teknologi IoT. Seterusnya memberi pandangan tentang keperluan bagi usaha penambahbaikan terhadap piawaian teknologi IoT pada masa kini.

Jadual 2.4 Analisis Kelebihan & Kekurangan Di Antara Badan Piawaian IoT

Piawaian	Kelebihan	Kekurangan
ITU-T	Inisiatif piawaian standard bagi IoT yang diguna pakai sedunia. Memperkenalkan konsep dan skop IoT terhadap ekosistem serta keperluan asas IoT.	Pemberian kuasa penentu kepada ahli yang terdapat di awal proses pembangunan standard piawaian. - Kurang kepelbagaian di dalam pendekatan teknikal, terutamanya di awal kitaran hidup produk.
ISO/IEC JTC1	Mengenal pasti keperluan pengguna serta jurang di dalam piawaian IoT. Menyediakan laporan kajian terhadap reka bentuk serta rangka kerja IoT terkini.	- Berlaku ketidakadilan di kalangan syarikat besar. - Berlaku ketidakadilan terhadap pembeli
ETSI	Memfokuskan kepada piawaian interaksi antara mesin ke mesin (M2M) yang menjadi asas kepada pembentukan OneM2M.	- Bakal meningkatkan kos berkaitan dengan gerbang teknologi dan maklumat
IETF	Penghasilan piawaian IoT yang memfokuskan kepada teknologi IPv6 dan protokol CoAP.	Risiko berlakunya manipulasi terhadap pasaran yang menguntungkan para pemegang saham.
IEEE	Badan piawaian yang memantau serta menyokong projek pembangunan standard, projek ilmiah, dan syarahan yang berkaitan dengan teknologi IoT.	Memaksa pesaing dan pihak industri untuk mengguna pakai standard piawaian baharu atau berisiko mengalami kekangan terhadap pasaran.
OneM2M	Inisiatif piawaian secara global yang berkaitan dengan teknologi komunikasi antara mesin ke mesin (M2M) dan teknologi IoT.	Kurangnya kepelbagaian di pasaran kerana industri terikat dengan piawaian yang ketat.

BAB 3

METODOLOGI

3.1 PENGENALAN

Perancangan projek memerlukan kaedah prosedur yang perlu dilaksanakan mengikut fasa-fasa yang telah ditetapkan untuk memastikan bahawa projek berjalan dengan lancar seperti yang telah dirancang. Pemilihan kaedah yang sesuai adalah salah satu faktor yang menyumbang kepada kejayaan modul keselamatan yang bakal dicadangkan. Pemilihan kaedah yang sesuai akan memberi kesan kepada hasil dapatan kajian serta perincian keselamatan yang diperlukan untuk pembangunan sesebuah modul keselamatan IoT.

Proses penyelidikan atau penghasilan kajian merupakan satu tugasan mendapatkan, mengkaji, dan menganalisis maklumat yang dilakukan secara sistematik bagi menyelesaikan tujuan projek dijalankan. Sehubungan itu, setiap kajian yang dijalankan memerlukan metodologi dalam usaha mendapatkan dapatan kajian. Bab ini akan membincangkan jenis-jenis metodologi, struktur modul, fasa modul, aliran kerja dan pengurusan projek. Terdapat beberapa perkara yang perlu diselesaikan semasa kajian untuk bab ini bagi memastikan bahawa apa yang telah dirancang dapat dilaksanakan dengan sistematik dan cekap.

3.2 METODOLOGI PENGHASILAN PROJEK

Dalam usaha penghasilan projek ini, perancangan terperinci telah dibuat dalam menjalankan rumusan terhadap segala maklumat dan kajian semasa berkenaan IoT bagi penghasilan satu kerangka model keselamatan terhadap teknologi IoT. Kajian ini dilaksanakan berdasarkan pendekatan kualitatif, dengan tujuan bagi mencari perbezaan di antara rangkaian Internet tradisional dan rangkaian IoT.

Tujuan mengenal pasti ciri-ciri yang membezakan IoT dengan rangkaian Internet biasa adalah bagi memberi takrif khusus berkenaan reka bentuk IoT secara terperinci, dan mengenal pasti prinsip yang akan membantu dalam memenuhi keperluan reka bentuk model ini.

Selepas prinsip reka bentuk IoT ini dikenal pasti, proses untuk mengkaji contoh piawaian teknikal terhadap rangkaian IoT dilakukan bagi menentukan contoh model piawaian yang sesuai untuk digunakan di dalam analisis perbandingan. Kajian terperinci terhadap piawaian keselamatan IoT terdahulu dapat membantu dalam mengenal pasti faktor kelebihan dan kelemahan yang terdapat pada seni bina rangkaian IoT.

3.2.1 Pendekatan Kualitatif

Pendekatan kualitatif bermaksud pendekatan kajian yang memfokuskan kepada pengalaman subjektif seseorang yang perlu dianalisis secara kualitatif, serta faktor realiti sosial yang mempunyai makna subjektif atau pandangan persendirian. Dengan erti kata lain, pendekatan secara kualitatif bertujuan untuk mendapatkan maklumat, seterusnya menganalisis maklumat tersebut bagi membantu dalam proses menerangkan sesuatu perkara. Proses ini dicapai melalui tugasan menganalisis kertas kajian lampau.

Bagi mendapatkan hasil rujukan kajian yang berkaitan, sumber yang digunakan adalah melalui laman sesawang jurnal IEEE Xplore, ScienceDirect, dan carian jurnal melalui Google Scholars. Sehubungan itu, demi mendapatkan keputusan carian yang berkaitan, kata carian yang merangkumi frasa "Internet of Things", "rangkaian", "panduan" dan "keselamatan" diutamakan.

3.2.2 Kaedah Pengumpulan Data

Data yang digunakan dalam projek ini didapati menggunakan sumber rujukan data primer iaitu melalui kertas kajian terdahulu, jurnal-jurnal berkaitan IoT, laman sesawang, dan tesis yang diperoleh dari laman sesawang Internet. Data yang dikumpulkan seterusnya akan dianalisis bagi mendapatkan pencerahan terhadap objektif projek.

3.2.3 Kaedah Penganalisisan Data

Kaedah penganalisisan data merupakan langkah kedua setelah melaksanakan proses pengumpulan data. Terdapat tiga teknik pemprosesan data kajian yang dijalankan, penerangannya adalah seperti berikut:-

a) Kaedah Induktif

Pendekatan induktif juga dikenali dalam penghujahan induktif, bermula dengan proses pemerhatian dan menganalisis maklumat, seterusnya modul keselamatan IoT akan dicadangkan pada akhir penyelidikan hasil daripada pemerhatian yang telah dibuat (Goddard 2004). Pendekatan ini bertujuan untuk menjana maklumat dari set data yang telah dikumpulkan bagi mengenal pasti corak dan hubungan untuk membina sesebuah modul keselamatan IoT.

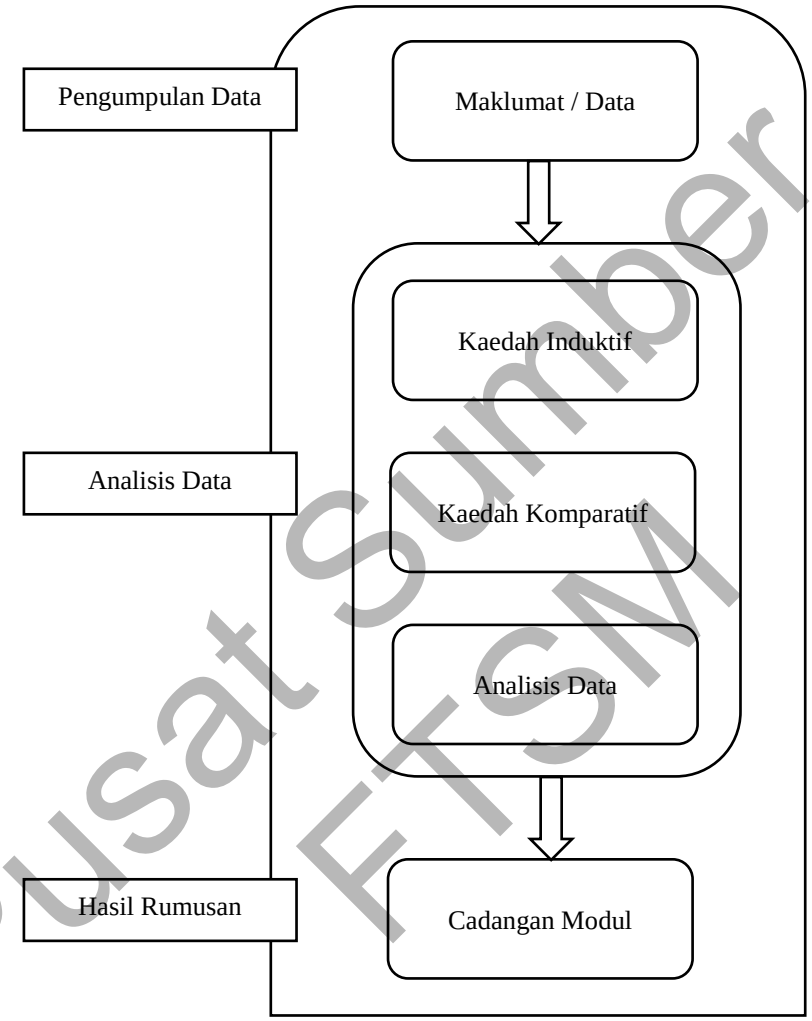
b) Kaedah Komparatif

Pendekatan kaedah kajian berdasarkan komparatif bertujuan untuk membuat perbandingan terhadap beberapa modul keselamatan IoT yang terdahulu bagi mencapai satu rumusan, iaitu modul standard keselamatan IoT. Modul yang bakal terhasil ini akan meliputi beberapa faktor penting dalam seni bina teknologi IoT. Oleh itu, perbandingan terhadap pelbagai modul telah dilakukan bagi memenuhi segala aspek keselamatan teknologi IoT.

c) Analisis

Proses analisis dibuat bagi mendapatkan rumusan daripada kesemua kaedah-kaedah penyelidikan yang telah dijalankan. Hasil daripada dapatan kajian ini akan digunakan untuk mengenal pasti faktor kekuatan dan kelemahan modul terdahulu bagi mencadangkan satu modul penyelesaian yang akan mengatasi masalah yang wujud pada sumber rujukan terdahulu.

Oleh itu, dapat dirumuskan bahawa pendekatan metodologi bagi kajian ini merangkumi beberapa aspek pendekatan seperti yang dinyatakan di atas. Untuk lebih memahami bagaimana metodologi ini berfungsi, Rajah 3.1 akan memaparkan proses tersebut.



Rajah 3.1 Kaedah Metodologi

BAB 4

DAPATAN KAJIAN

4.1 PENGENALAN

Dapatan kajian membincangkan segala maklumat yang di dapati melalui analisis kertas kajian yang dibuat di antara tahun 2010 – 2016. Data yang diperoleh ini merangkumi faktor keselamatan dalam rangkaian bagi teknologi *Internet of Things (*IoT*),* serta contoh-contoh modul rangkaian yang digunakan dalam teknologi IoT. Dapatan kajian ini dibahagikan kepada dua bahagian, iaitu yang pertama akan menghuraikan dapatan berkenaan faktor keselamatan IoT, dan bahagian kedua akan menghuraikan dapatan berkenaan modul keselamatan rangkaian IoT. Secara umumnya huraian yang diberikan di dalam bab ini bertujuan untuk merangka sebuah pelan tindakan bagi proses penambahbaikan terhadap aspek keselamatan pada infrastruktur rangkaian IoT. Oleh itu, model pelan tindakan bagi rangkaian IoT perlu mengambil kira objektif berikut:-

a. Mengenal pasti kelemahan teknologi "*Internet of Things (IoT)"* terhadap aspek keselamatan data pengguna.

b. Mengenal pasti kelemahan teknologi "*Internet of Things (IoT)"* terhadap aspek keselamatan rangkaian.

4.2 CABARAN TERHADAP TEKNOLOGI IoT

Menurut laporan dapatan kajian yang dilakukan oleh badan piawaian IEEE pada tahun 2016, mereka mendapati bahawa cabaran yang paling besar bagi IoT pada waktu kini adalah berkenaan faktor keselamatan dalam penggunaan teknologi tersebut. Dari segi aspek penggunaan, data dari pengguna merupakan salah satu maklumat yang bernilai serta penting bagi tugasan analisis sistem peranti IoT. Data aplikasi IoT boleh merangkumi pelbagai sektor serta kegunaan seperti perindustrian, perdagangan, data pengguna atau data peribadi. Data aplikasi ini perlu dirahsiakan dan disimpan di lokasi selamat bagi menghindari berlakunya kecurian serta pengubahan data. Sehubungan itu, cabaran terhadap teknologi IoT yang akan dibincangkan merangkumi topik berikut.

Jadual 4.1 Cabaran Terhadap Teknologi IoT

Cabaran	**Penerangan**
Privasi Maklumat	Terdapat sebilangan syarikat yang bertindak mendapatkan data tahap penggunaan peranti mereka yang mampu terdedah kepada masalah kebocoran privasi pada proses transmisi data dilakukan..
Keselamatan Maklumat	Keselamatan maklumat juga penting kerana walaupun proses transmisi data dapat dilakukan dengan mudah melalui rangkaian, ianya penting untuk merahsiakan maklumat penting daripada sebarang peranti tengah yang mampu memantau maklumat pada transmisi tersebut.
Masalah Teknikal	Disebabkan peningkatan penggunaan peranti IoT, keperluan terhadap kapasiti rangkaian juga meningkat. Sehubungan itu, ia menjadi cabaran bagi mendapatkan storan yang luas bagi menyimpan data bagi tujuan analisis.
Kekurangan Piawaian Umum	Terdapat pelbagai standard piawaian yang merangkumi penggunaan serta industri pembuatan peranti IoT. Oleh itu, cabaran semakin meningkat bagi membezakan jenis peranti IoT yang dibenarkan serta tidak dibenarkan untuk mengakses ke internet. Cabaran terhadap keselamatan IoT dapat di bahagikan kepada tiga perkara, iaitu:-

bersambung...

...sambungan

Serangan Terhadap Keselamatan Dan Kelemahan Sistem	a) Keselamatan Sistem Keselamatan sistem memfokuskan kepada keseluruhan sistem IoT bagi mengenal pasti cabaran keselamatan yang berbeza, mengenal pasti rangka kerja keselamatan yang sesuai, dan mendapatkan piawaian keselamatan yang sesuai bagi menjamin keselamatan pada rangkaian. b) Keselamatan Aplikasi Keselamatan aplikasi merangkumi tugasan yang perlu dilaksanakan oleh pembangun aplikasi pada peranti IoT bagi menangani sebarang isu keselamatan yang dapat memberi risiko kepada kebocoran maklumat pengguna. c) Keselamatan Rangkaian Keselamatan rangkaian berfungsi bagi memastikan komunikasi pada rangkaian IoT selamat tanpa sebarang risiko berlakunya kebocoran maklumat ketika proses transmisi di antara peranti IoT berjalan.

4.3 KLASIFIKASI SERANGAN TERHADAP TEKNOLOGI IoT

Telah banyak kajian menyeluruh mengenai faktor keselamatan IOT yang dijalankan sebelum ini, dan ia banyak membantu dalam memberi klasifikasi terperinci terhadap serangan IOT serta penyelesaiannya. Andrea pada tahun 2015 telah mencadangkan satu klasifikasi baru bagi jenis serangan teknologi IoT, beliau juga telah mengklasifikasikan serangan tersebut kepada 4 jenis, iaitu: serangan fizikal, rangkaian, perisian, dan enkripsi. 3 daripadanya merangkumi lapisan pada struktur teknologi IOT (fizikal, rangkaian, dan aplikasi) serta tambahan pada protokol IOT iaitu bagi tujuan enkripsi data.

Serangan secara fizikal dapat dilakukan apabila penyerang itu berhampiran atau mempunyai akses secara terus kepada peranti IOT tersebut. Dengan mempunyai akses kepada peranti, sebarang eksploitasi dan pengubahsuaian terhadap peranti IOT tersebut dapat dilakukan. Berdasarkan kajian oleh Xingmei pada tahun 2013, bagi membendung masalah keselamatan ini berlaku pada lapisan fizikal, peranti tersebut perlu mempunyai fungsi *secure booting*, algoritma kriptografik hash dan tandatangan digital bagi mengesahkan keaslian serta integriti perisian IoT tersebut. Selain itu, setiap peranti baru perlu melalui proses autentikasi dan verifikasi ke rangkaian sebelum sebarang transmisi data dapat dilakukan. Tambahan pula, setiap peranti seharusnya mempunyai sistem pengesanan ralat dan segala maklumat mengenainya perlu di enkripsi bagi mengekalkan integriti dan kerahsiaan data (Joshy, A. 2017).

Serangan melalui rangkaian merangkumi beberapa percubaan untuk memanipulasi sistem rangkaian peranti IOT seterusnya melakukan kerosakan pada peranti tersebut. Manakala serangan melalui perisian dapat dilakukan sekiranya terdapat beberapa kelemahan pada sistem pengoperasian yang digunakan pada peranti IOT tersebut. Seterusnya, serangan enkripsi dilakukan apabila penyerang cuba untuk memecah masuk ke dalam enkripsi sistem pada peranti tersebut. Jadual di bawah menerangkan mengenai jenis serangan enkripsi pada sistem IoT.

Jadual 4.2 Jenis Serangan Enkripsi Pada Sistem IoT.

Jenis Serangan	**Penerangan**
Side Channel	Serangan ini dilakukan berdasarkan maklumat yang diperoleh dari aspek implementasi fizikal terhadap *cryptosystem.* Contoh maklumat yang boleh dieksploitasi bagi tujuan serangan ini adalah maklumat penggunaan sumber tenaga peranti, dan maklumat *cache* pada sistem.
Cryptanalysis	Proses mengkaji dan menganalisa sistem maklumat yang bertujuan bagi memecahkan enkripsi pada data penting di dalam sistem.

Manakala, taksonomi klasifikasi serangan terhadap IoT berdasarkan cara penyerang melakukan penyelewengan terhadap peranti IoT telah diperkenalkan oleh Ronen et al. pada tahun 2016. Kategori yang diperkenalkan meliputi fungsi: mengabaikan, mengurangkan, menyalahgunakan, dan memperluaskan fungsi sistem. Kajian yang dibuat oleh Ronen memfokuskan kepada fungsi sambungan IoT terhadap lampu pintar (*smart lights*). Dapatan daripada kajian tersebut meringkaskan bahawa ianya penting untuk memberi fokus terhadap isu keselamatan ketika fasa reka bentuk, implementasi, dan integrasi bagi setiap peranti IoT.

4.4 PEMBANGUNAN PIAWAIAN DAN ENTITI PENETAPAN PIAWAIAN

Berdasarkan senarai piawaian yang telah disenaraikan sebelum ini dapat dirumuskan terdapat 3 kategori umum yang dapat disenaraikan sebagai entiti penetapan piawaian dilakukan. Kategori tersebut merangkumi: sebuah syarikat, gabungan organisasi pembangunan piawaian, dan melalui forum atau konsortium. Jadual 4.4 akan menerangkan dengan lebih lanjut berkenaan entiti penetapan piawaian tersebut.

Jadual 4.3 Entiti Penetapan Piawaian

Entiti Penetapan Piawaian	Hasil	Contoh
Sebuah Syarikat	Spesifikasi bersifat proprietari.	Piawaian khusus yang terhasil dari sesebuah syarikat atau vendor.
Gabungan Organisasi Pembangunan Piawaian	Piawaian Umum yang akan menjadi "piawaian De Jure" jika proses implementasinya diberikan mandat dari segi perundangan.	ITU, ISO, ETSI, Badan - badan piawaian kebangsaan.
Forum / Konsortium	Secara amnya, ia merupakan standard terbuka namun boleh menjadi standard tertutup, ianya bergantung kepada organisasi yang terdapat pada forum / konsortium tersebut.	IETF, Forum Jalur lebar, W3C, Konsortium Teknologi Bluetooth, OASIS, dll.

4.5 PIAWAIAN KESELAMATAN RANGKAIAN IoT

Organisasi piawaian yang bertanggungjawab dalam mengurus piawaian keselamatan teknologi IoT adalah seperti yang telah dinyatakan pada seksyen 4.4, iaitu: ITU-T, ISO/IEC, ETSI, IETF, OneM2M.

4.5.1 Kesatuan Telekomunikasi Antarabangsa – Telekomunikasi, ITU-T

Piawaian keselamatan oleh ITU-T dikelaskan menggunakan huruf, bagi piawaian IoT ia dikelaskan menggunakan siri huruf F, X, dan Y. Maklumat lanjut berkenaan siri piawaian keselamatan IoT ITU-T adalah seperti berikut:-

a. **Siri F**: Piawaian siri F menetapkan perihal berkaitan servis telekomunikasi tanpa menggunakan telefon, dan siri F.700 – F.799 adalah berkenaan servis audio visual. Manakala siri yang berkaitan dengan faktor keselamatan adalah F.748, yang menerangkan secara maklumat secara menyeluruh, ciri-ciri keselamatan, dan keperluan khusus bagi penggunaan aplikasi IoT berdasarkan siri ITU-T Y.2060. Berdasarkan dokumen tersebut, akibat daripada peningkatan ancaman keselamatan yang berkaitan teknologi IoT, ia adalah satu keperluan untuk mengintegrasikan pelbagai teknik dan polisi keselamatan dalam peranti serta teknologi IoT.

b. **Siri X**: Piawaian yang mempunyai siri X menerangkan berkenaan rangkaian data, komunikasi sistem terbuka, dan keselamatan. Siri X.650 – X.679 adalah berkenaan penamaan, menujukan, dan pendaftaran terhadap rangkaian OSI serta aspek sesebuah sistem. Siri X.1310 – X.1339 adalah berkenaan rangkaian keselamatan sensor peranti IoT. Nombor siri yang menerangkan berkenaan keselamatan adalah X.675 dan X.1314.

   i. **X.675**: Meliputi resolusi berdasarkan rangka kerja pengecaman objek yang bertujuan untuk memberi fungsi antara-operasi terhadap proses pengecaman dan pengesan pelbagai. Proses pengesahan dan pemberian kuasa perlu di ambil kira bagi mengekang ancaman keselamatan dari pihak ketiga terhadap rangka kerja IoT.

   ii. **X.1314**: No siri 1314 bertujuan dalam memberi maklumat lengkap berkenaan rangka kerja keselamatan terhadap rangkaian sentiasa-ada dan domain keselamatan yang meliputi analisis terhadap ancaman keselamatan pada rangka kerja.

c. **Siri Y**: Nombor siri Y menerangkan berkenaan infrastruktur maklumat global, aspek protokol internet, dan teknologi rangkaian generasi-hadapan. Y.2000 – Y.2099 adalah berkaitan dengan rangka kerja dan model seni bina fungsian bagi teknologi rangkaian masa-hadapan. Y.4000 – Y.4899 adalah berkenaan komuniti berkaitan dengan teknologi IoT, dan bandar pintar. Piawaian berkaitan dengan keselamatan adalah pada nombor siri Y.2060, Y.2063, Y.2066 - Y.2068, Y.4111 – Y.4112, Y.2075- Y.2078, Y.4552 – Y.4553, dan Y.4702.

i. **Y.2060**: Berkenaan konsep, ciri-ciri, keperluan, dan model rujukan terhadap teknologi IoT. Siri ini juga memaparkan keupayaan keselamatan secara generik pada setiap lapisan dan pada keperluan spesifik aplikasi IoT pada model rujukan.

ii. **Y.2063**: Meliputi rangka kerja terhadap *Web of Things* (WoT) dan maklumat keselamatan berkenaan proses pengesahan pada peranti WoT.

iii. **Y.2066**: Menerangkan maklumat keperluan am pada teknologi IoT berkenaan faktor perlindungan keselamatan dan privasi seperti keselamatan komunikasi, keselamatan pengurusan data, keselamatan servis pemantauan, integrasi terhadap teknik & polisi keselamatan, proses pengesahan & pengenalan, serta audit keselamatan.

iv. **Y.20267**: Menerangkan maklumat am dan keupayaan terhadap *gateway* aplikasi serta peranti IoT. Siri ini menetapkan mekanisma keselamatan pada *gateway* IoT seperti proses pengesahan, pengenalan, enkripsi data, dan perlindungan privasi.

v. **Y.2068**: Maklumat berkenaan konsep, pandangan fungsian terhadap rangka kerja dan keupayaan teknologi IoT. Selain itu, terdapat sokongan tambahan pada ciri-ciri keselamatan pada komunikasi, pengurusan data, servis pemantauan keselamatan, integrasi keselamatan, proses pengesahan bersama, dan audit keselamatan.

vi. **Y.2075**: Menerangkan berkenaan konsep rangka kerja pemantauan e-kesihatan (EHM) dan rangka keupayaan EHM.

vii. **Y.4111/Y.2076**: Menerangkan keperluan semantik dan rangka kerja IoT seperti gambar rajah kes, keperluan, dan keupayaan berdasarkan kepada semantik. Sokongan keselamatan berkeupayaan semantik (SSSC) terhadap faktor keselamatan amatlah disyorkan.

viii. **Y.4112/Y.2077**: Menerangkan berkenaan konsep, tujuan, komponen dan keperluan terhadap fungsi *plug-and-play* (PnP) pada teknologi IoT. Keupayaan keselamatan fungsi PnP berkait rapat dengan keperluan am seperti proses pengesahan, kawalan akses, perlindungan *firewall*, dan keselamatan data pada peranti dan aplikasi IoT.

ix. **Y.4552/Y.2078**: Menerangkan berkenaan model sokongan aplikasi terhadap teknologi IoT. Model sokongan ini bertindak memberikan fungsi pemantauan servis konfigurasi pada aplikasi IoT berdasarkan keperluan komunikasi peranti IoT.

x. **Y.4553**: Menerangkan keperluan spesifik terhadap peranti mudah alih yang berfungsi sebagai nod bagi aplikasi dan servis IoT. Perlindungan dan pengesahan data dinyatakan sebagai keperluan keselamatan siri ini.

xi. **Y.4702**: Menerangkan keperluan umum dan keupayaan terhadap pengurusan peranti pada teknologi IoT. Keupayaan pengurusan keselamatan meliputi fungsi komunikasi, pengesanan & laporan ujian keselamatan, jaminan keselamatan peranti, dan kawalan keselamatan peranti IoT.

4.5.2 ISO/IEC JTC1

Dokumen standard bagi piawaian ISO/IEC 30128 menerangkan kandungan keselamatan yang mempertimbangkan faktor keselamatan antara muka aplikasi rangkaian pada sensor rangkaian umum peranti IoT.

4.5.3 Institut Piawaian Telekomunikasi Eropah, ETSI

Piawaian ETSI yang menerangkan berkenaan IoT di dalam peringkat spesifikasi teknikal (TS) merupakan piawaian yang terbaik di antara spesifikasi lain yang pernah dikeluarkan oleh organisasi tersebut. OneM2M menganggap spesifikasi piawaian ini sebagai asas kepada piawaian IoT oleh ETSI.

4.5.4 Pasukan Petugas Kejuruteraan Internet, IETF

Piawaian bagi keselamatan IoT majoritinya adalah berkenaan rangkaian dan protokol yang digunakan di dalam persekitaran IoT. Senarai piawaian yang berkaitan keselamatan teknologi IoT adalah seperti berikut:-

a. **RFC 4919**: Menerangkan gambaran umum berkaitan 6LoWPAN dan kelebihan rangkaian IPv6. Selain itu, ia turut mengambil kira maklumat terperinci berkaitan keperluan keselamatan IoT.
b. **RFC 6606**: Menerangkan berkenaan masalah dan ruang reka bentuk laluan 6LoWPAN yang melibatkan penggunaan kuasa rendah dan ciri-ciri peranti IoT, serta proses pengesahan siaran dan pautan bagi operasi laluan protokol selamat.

c. **RFC 7228**: Menerangkan terminologi bagi rangkaian nod yang dikekang termasuk terminologi berkaitan keselamatan.

d. **RFC 7252**: Menerangkan berkenaan CoAP yang direka oleh IETF, ini menjamin keselamatan CoAP dan Lapisan Keselamatan Penghantaran Datagram (DTSL) serta mengambil kira faktor keselamatan bagi menghuraikan protokol, proksi, dan pengagregatan senarai keselamatan CoAP.

e. **RFC 7388**: Menerangkan asas pengurusan maklumat (MIB) untuk kegunaan protokol pengurusan rangkaian dan objek bagi menguruskan 6LowPANs termasuk rangkaian selamat bagi modul MIB.
f. **RFC 7554**: Menerangkan berkenaan persekitaran, pernyataan masalah, dan objektif dalam menggunakan *Time-Slotted Channel Hopping* (TSCH). Komunikasi secara selamat diperlukan dalam menyatakan proses pengenalan dan penghantaran data serta signal aplikasi secara selamat.

g. **RFC 7641**: Meliputi pemantauan sumber di dalam CoAP yang mengambil kira faktor keselamatan.

h. **RFC 7650**: Menerangkan kegunaan CoAP bagi model keselamatan Sumber Lokasi dan Penemuan, *Resource Location and Discovery* (RELOAD). Model tersebut juga berdasarkan persijilan kunci awam dan polisi kawalan akses bagi penamaan dasar RELOAD.

4.5.5 OneM2M

Projek piawaian OneM2M disertai oleh pelbagai agensi piawaian yang turut menyumbang secara aktif dalam penggubalan piawaian terhadap teknologi IoT. Oleh itu, standard piawaian yang dikeluarkan oleh OneM2M adalah khusus bagi kegunaan IoT sahaja.

a. **TS-0001**: Menerangkan reka bentuk fungsian bagi OneM2M secara penuh. Reka bentuk keselamatan ini meliputi pengendalian data sensitif, pengurusan keselamatan, penubuhan kawalan akses berkaitan keselamatan seperti proses pengenalpastian, pengesahan, pengenalan, dan pengurusan identiti.

b. **TS-0002**: Menerangkan contoh fungsian informatif dan keperluan teknikal bagi oneM2M. Terdapat 63 keperluan keselamatan yang disenaraikan di bawah piawaian oneM2M.

c. **TS-0003**: Menerangkan solusi keselamatan yang boleh diimplementasikan pada sistem M2M yang meliputi sistem keselamatan reka bentuk, lapisan servis keselamatan, pemberian kebenaran, rangka kerja keselamatan (prosedur & parameter), reka bentuk perlindungan privasi, dan maklumat spesifik jenis data keselamatan oneM2M.

d. **TS-0004**: Menerangkan protokol komunikasi bagi sistem aduan oneM2M, aplikasi M2M, format data umum, antara muka dan turutan mesej.

e. **TS-0005**: Menerangkan terjemahan protokol dan proses pemetaan di antara lapisan servis oneM2M, *Open Mobile Alliance Device Management* (OMA DM), *Light-Weight Machine to Machine* (LWM2M), dan pengurusan kawalan akses.

f. **TS-0007**: Menerangkan servis pada M2M, supaya proses permintaan bagi tugasan pengesahan dan pengenalan bagi servis diambil kira.

g. **TS-0008 – TS-0010/TS-0020**: Meliputi CoAP, HTTP, MQTT, pengkhususan *Websocket*, dan mengambil kira penerimaan mesej bagi proses pengesahan serta pengenalan.

h. **TS-0013**: Memastikan ujian kesalingfungsian dan keselamatan di antara nod asal dan nod penerima berfungsi dengan jayanya.

i. **TS-0014/TS-0021/TS-0024**: Menerangkan fungsi kerjasama antara LWM2M, AllJoyn dan perisian OIC/OCF. Maklumat keselamatan adalah dikhususkan di bahagian pemetaan dan polisi kawalan akses.