SISTEM PENGAWASAN *CLOSED CIRCUIT TELEVISION* (CCTV) PADA *AUTOMATED TELLER MACHINE* (ATM) SECARA *REAL-TIME* BERBASIS *INTERNET OF THINGS* (IOT)

THESIS

Oleh:

NIKO HERI SETIYAWAN
NIM. 210605210004

PROGRAM STUDI MAGISTER INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG

2025

SISTEM PENGAWASAN *CLOSED CIRCUIT TELEVISION* (CCTV) PADA *AUTOMATED TELLER MACHINE* (ATM) SECARA *REAL-TIME* BERBASIS *INTERNET OF THINGS* (IOT)

THESIS

Oleh:

NIKO HERI SETIYAWAN

NIM. 210605210004

Telah diperiksa dan disetujui untuk di uji:
Tanggal 03 Juni 2025

Pembimbing I	Pembimbing II
Dr. M. Amin Hariyadi, M.T	Dr. Ir. Yunifa Miftachul Arif, S.ST., M.T
NIP. 19670118 200501 1 001	NIP. 19830616 201101 1 004

Mengetahui,
Ketua Program Studi Magister Informatika
Fakultas Sains dan Teknologi
Universitas Islam Maulana Malik Ibrahim Malang

Dr. Yahyo Crysdian
NIP. 19740424 200901 1 008

SISTEM PENGAWASAN *CLOSED CIRCUIT TELEVISION* (CCTV) PADA *AUTOMATED TELLER MACHINE* (ATM) SECARA *REAL-TIME* BERBASIS *INTERNET OF THINGS* (IOT)

THESIS

Oleh:

NIKO HERI SETIYAWAN

NIM. 210605210004

Telah Dipertahankan di Depan Dewan Penguji Thesis

dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan

Untuk Memperoleh Gelar Magister Komputer (M.Kom)

Tanggal 03 Juni 2025

Susunan Dewan Penguji			**Tanda Tangan**
Penguji I	:	Dr. Cahyo Crysdian NIP. 19740424 200901 1 008	( )
Penguji II	:	Prof. Dr. Sri Harini, M.Si NIP. 19731014 200112 2 002	( )
Pembimbing I	:	Dr. M. Amin Hariyadi, M.T NIP. 19670118 200501 1 001	( )
Pembimbing II	:	Dr. Ir. Yunifa Miftachul Arif, S.ST., M.T NIP. 19830616 201101 1 004	( )

Mengetahui,
Ketua Program Studi Magister Informatika
Fakultas Sains dan Teknologi
Universitas Islam Maulana Malik Ibrahim Malang

Dr. Cahyo Crysdian
NIP. 19740424 200901 1 008

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan dibawah ini:

Nama	: Niko Heri Setiyawan
NIM	: 210605210004
Program Studi	: Magister Informatika
Fakultas	: Sains dan Teknologi

Menyatakan dengan sebenarnya bahwa Thesis yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilalihan data, tulisan atau pikiran orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka.

Apabila dikemudian hari terbukti atau dapat dibuktikan Thesis ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 03 Juni 2025

Yang Membuat Pernyataan

Niko Heri Setiyawan

NIM. 210605210004

MOTTO

" Stay Hungry, Stay Foolish "

Steve Job

PERSEMBAHAN

Atas berkah dan rahmat Allah SWT, Thesis ini bisa saya selesaikan dengan lengkap dan baik sesuai dengan arahan bapak ibu pembimbing, oleh karena itu hasil kerja keras atas keberhasilan dari penulisan Thesis ini merupakan dukungan dari beberapa pihak yaitu :

1. Keluarga kecil tercinta antara lain istri
2. Keluarga besar, yaitu ibu, ayah, ayah mertua, kakek, nenek, paman, kakak sepupu dan saudara-saudara yang lain.
3. Bapak ibu dosen Magister Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Teman-teman angkatan Magister Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
5. Teman-teman mahasiswa Magister Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
6. Serta rekan-rekan yang tidak mungkin disebutkan satu persatu atas dukungan terselesaikannya Thesis ini.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb

Syukur Alhamdulillah penulis haturkan kehadirat Allah SWT yang telah melimpahkan Rahmat dan Hidayah-Nya, sehingga penulis dapat menyelesaikan studi di Program Studi Magister Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang sekaligus menyelesaikan Thesis ini dengan baik.

Selanjutnya penulis haturkan ucapan terima kasih seiring do'a dan harapan jazakumullah ahsanal jaza' kepada semua pihak yang telah membantu terselesaikannya Thesis ini. Ucapan terima kasih ini penulis sampaikan kepada:

1. Dr. M. Amin Hariyadi, M.T., dan Dr. Ir. Yunifa Miftachul Arif, S.ST., M.T selaku dosen pembimbing Thesis, yang telah banyak memberikan pengarahan dan pengalaman yang berharga.
2. Segenap civitas akademika Program Studi Magister Informatika, terutama seluruh Bapak / Ibu dosen, terima kasih atas segenap ilmu dan bimbingannya.
3. Keluarga tercinta yang senantiasa memberikan do'a dan semangat
4. Semua rekan-rekan seperjuangan yang ikut mendukung dan membantu.

Penulis menyadari bahwa dalam penyusunan Thesis ini masih terdapat kekurangan dan penulis berharap semoga Thesis ini bisa memberikan manfaat kepada para pembaca khususnya bagi penulis secara pribadi. Amiinn Yaa Rabbal Alamin.

Wasalamu'alaikum Wr. Wb

Malang, 03 Juni 2025

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Setiyawan, Niko Heri. 2025. **Sistem Pengawasan *Closed Circuit Television* (CCTV) Pada *Automated Teller Machine* (ATM) Secara *Real-Time* Berbasis *Internet Of Things* (IOT)**. Thesis Program Studi Magister Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Dr. M. Amin Hariyadi, M.T., (II) Dr. Ir. Yunifa Miftachul Arif, S.ST., M.T.

Kata Kunci: Pengawasan, CCTV, ATM, Real-time, IOT.

Efisiensi laporan kriminalitas terhadap CCTV merujuk pada kemampuan sistem pengawasan menggunakan kamera CCTV dalam mempercepat, mempermudah, dan meningkatkan akurasi proses pelaporan tindakan kriminal. Dengan kata lain, efisiensi ini mencakup bagaimana penggunaan CCTV, terutama yang berbasis Internet of Things (IoT), dapat mengurangi waktu dan tenaga dalam mendeteksi, merekam, serta menyampaikan informasi tentang kejadian kriminal kepada pihak yang berwenang. Penelitian ini termasuk dalam kategori penelitian eksperimen kuantitatif ngan pendekatan sistem berbasis automata, khususnya menggunakan *Finite State Automata* (FSA). Pendekatan ini digunakan untuk memodelkan proses kerja sistem pengawasan CCTV dari status siaga hingga pelaporan kejadian dan respons keamanan. Dengan pendekatan ini, sistem dapat diuji secara sistematis dalam hal efisiensi waktu, bandwidth, dan efektivitas pemantauan. Penelitian ini mngemukakan hasil bahwa efisiensi yang signifikan dalam pengawasan keamanan ATM secara *real-time*. Sistem ini mampu mempercepat waktu deteksi kejadian kriminalitas, dari sebelumnya rata-rata 120 menit menjadi 15 menit. Mempercepat waktu pelaporan ke pusat keamanan, dari 90 menit menjadi 10 menit, melalui kejadian otomatis tanpa intervensi manual. Menghemat konsumsi bandwidth, dari 1024 Kbps pada sistem konvensional menjadi hanya 256 Kbps dengan pendekatan *event-based* MQTT. Mempercepat waktu respon keamanan, dari 30 menit menjadi 5 menit, karena petugas menerima laporan secara langsung dan instan. Meningkatkan keberhasilan pemantauan *real-time*, dari 60% pada sistem lama menjadi 100% dalam mendeteksi kejadian saat berlangsung.

ABSTRACT

Setiyawan, Niko Heri. 2025. **Closed Circuit Television (CCTV) Surveillance System on Automated Teller Machine (ATM) in Real-Time Based on Internet of Things (IOT)**. Thesis of Master's Degree Program in Informatics, Faculty of Science and Technology, Islamic State University Maulana Malik Ibrahim Malang. Supervisor: I) Dr. M. Amin Hariyadi, M.T., (II) Dr. Ir. Yunifa Miftachul Arif, S.ST., M.T.

Keywords: Surveillance, CCTV, ATM, Real-time, IOT.

The efficiency of CCTV crime reporting refers to the ability of a surveillance system using CCTV cameras to speed up, simplify, and improve the accuracy of the crime reporting process. In other words, this efficiency includes how the use of CCTV, especially those based on the Internet of Things (IoT), can reduce time and effort in detecting, recording, and conveying information about criminal incidents to the authorities. This research is included in the category of quantitative experimental research with an automata-based system approach, specifically using Finite State Automata (FSA). This approach is used to model the work process of a CCTV surveillance system from alert status to incident reporting and security response. With this approach, the system can be tested systematically in terms of time efficiency, bandwidth, and monitoring effectiveness. This study shows that there is significant efficiency in real-time ATM security surveillance. This system is able to speed up the detection time of criminal incidents, from an average of 120 minutes to 15 minutes. Accelerate reporting time to the security center, from 90 minutes to 10 minutes, through automatic events without manual intervention. Save bandwidth consumption, from 1024 Kbps on conventional systems to only 256 Kbps with the MQTT event-based approach. Accelerate security response time, from 30 minutes to 5 minutes, because officers receive reports directly and instantly. Increase the success of real-time monitoring, from 60% on legacy systems to 100% in detecting events as they occur.

ملخص البحث

على أجهزة الصراف الآلي (CCTV) سيتياوان، نيكو هيري .٢٠٢٥ .نظام مراقبة تلفزيونية مغلقة أطروحة برنامج .(IOT) في الوقت الفعلي استنادًا إلى إنترنت الأشياء (ATM) الماجستير في المعلوماتية، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية، مالانج .المشرف :١ (الدكتور محمد أمين هريادي، ماجستير في العلوم،)٢(الدكتورة يونيفة مفتاح عارف، ماجستير في العلوم، ماجستير في العلوم

.الكلمات المفتاحية :المراقبة، كاميرات المراقبة، أجهزة الصراف الآلي، الوقت الحقيقي، إنترنت الأشياء

تشير كفاءة الإبلاغ عن الجرائم عبر كاميرات المراقبة إلى قدرة نظام المراقبة الذي يستخدم كاميرات المراقبة على تسريع عملية الإبلاغ عن الجرائم وتبسيطها وتحسين دقتها .بمعنى آخر، تتضمن هذه الكفاءة أن يقلل الوقت ،(IoT) كيف يمكن لاستخدام كاميرات المراقبة، وخاصة تلك القائمة على إنترنت الأشياء يندرج هذا البحث .السلطات والجهد في الكشف عن الحوادث الجنائية وتسجيلها ونقل المعلومات عنها إلى ضمن فئة البحث التجريبي الكمي مع نهج نظام قائم على الأتمتة، وتحديدًا باستخدام أتمتة الحالة المحدودة يُستخدم هذا النهج لنمذجة عملية عمل نظام مراقبة كاميرات المراقبة من حالة التنبيه إلى الإبلاغ .(FSA) عن الحوادث والاستجابة الأمنية .باستخدام هذا النهج، يمكن اختبار النظام بشكل منهجي من حيث كفاءة الوقت وعرض النطاق الترددي وفعالية المراقبة .تُظهر هذه الدراسة وجود كفاءة كبيرة في مراقبة أمن ،أجهزة الصراف الآلي في الوقت الفعلي .هذا النظام قادر على تسريع وقت الكشف عن الحوادث الجنائية من متوسط 120 دقيقة إلى 15 دقيقة .تسريع وقت الإبلاغ إلى مركز الأمن، من 90 دقيقة إلى 10 دقائق، من خلال الأحداث التلقائية دون تدخل يدوي .توفير استهلاك النطاق الترددي، من 1024 القائم MQTT كيلوبت في الثانية على الأنظمة التقليدية إلى 256 كيلوبت في الثانية فقط مع نهج على الأحداث .تسريع وقت الاستجابة الأمنية، من 30 دقيقة إلى 5 دقائق، لأن الموظفين يتلقون التقارير مباشرةً وفوريًا .زيادة نجاح المراقبة الفورية، من 60 %على الأنظمة القديمة إلى 100 %في اكتشاف ..الأحداث فور وقوعها

BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) telah membuka era baru dalam teknologi yang menghubungkan perangkat dan memungkinkan interaksi yang lebih pintar dan terkoneksi melalui internet. Salah satu aplikasi yang menjanjikan dari IoT adalah dalam pengawasan ruangan. Pengawasan ruangan menjadi semakin penting dalam konteks keamanan, manajemen, dan kenyamanan di berbagai lingkungan seperti rumah tangga, kantor, dan fasilitas komersial. Tradisionalnya, pengawasan ruangan menggunakan sistem-sistem terpusat yang terbatas pada kamera CCTV. Namun, dengan adopsi IoT, pengawasan dapat dikembangkan lebih jauh dengan memanfaatkan konektivitas internet untuk mengintegrasikan berbagai perangkat kamera secara *real-time*.

Perkembangan teknologi informasi dan komunikasi telah memberikan dampak signifikan dalam berbagai sektor, termasuk sektor perbankan. Salah satu teknologi yang digunakan untuk meningkatkan keamanan dan kenyamanan nasabah adalah *Automated Teller Machine* (ATM) (Smith et al., 2020). ATM memungkinkan transaksi keuangan dilakukan secara mandiri tanpa memerlukan interaksi langsung dengan petugas bank. Namun, keberadaan ATM juga rentan terhadap berbagai ancaman keamanan, seperti pencurian, perusakan, dan gangguan operasional akibat pemadaman listrik. Oleh karena itu, diperlukan sistem

pengawasan yang andal untuk memastikan ATM tetap beroperasi dengan aman dan efisien (Jones & Brown, 2019).

Sistem *Closed Circuit Television* (CCTV) telah lama digunakan sebagai alat pemantauan keamanan pada ATM. CCTV berfungsi untuk merekam aktivitas di sekitar ATM guna mencegah dan mengidentifikasi tindakan kriminal (Ali & Hassan, 2021). Namun, sistem pengawasan konvensional sering kali memiliki keterbatasan dalam hal pemantauan *real-time* dan respons terhadap kejadian yang tidak diinginkan. Dengan kemajuan teknologi *Internet of Things* (IoT), sistem pengawasan CCTV dapat ditingkatkan dengan fitur pemantauan *real-time* yang memungkinkan pihak berwenang untuk mengakses rekaman secara langsung dari jarak jauh dan mengambil tindakan cepat jika terjadi insiden (Rahman et al., 2022).

Landasan dalam penelitian terkait sistem pengawasan ATM berbasis IoT untuk memperkuat argumen mengenai pentingnya keamanan, keandalan, dan kepercayaan dalam transaksi keuangan berkaitan dengan ayat Al-Baqarah Ayat 282:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْٓا اِذَا تَدَايَنْتُمْ بِدَيْنٍ اِلٰٓى اَجَلٍ مُّسَمًّى فَاكْتُبُوْهُ ۗ وَلْيَكْتُبْ بَّيْنَكُمْ كَاتِبٌۢ بِالْعَدْلِ ۖ وَلَا يَأْبَ كَاتِبٌ اَنْ يَّكْتُبَ كَمَا عَلَّمَهُ اللّٰهُ فَلْيَكْتُبْ ۚ وَلْيُمْلِلِ الَّذِيْ عَلَيْهِ الْحَقُّ وَلْيَتَّقِ اللّٰهَ رَبَّهٗ وَلَا يَبْخَسْ مِنْهُ شَيْـًٔا ۗ فَاِنْ كَانَ الَّذِيْ عَلَيْهِ الْحَقُّ سَفِيْهًا اَوْ ضَعِيْفًا اَوْ لَا يَسْتَطِيْعُ اَنْ يُّمِلَّ هُوَ فَلْيُمْلِلْ وَلِيُّهٗ بِالْعَدْلِ ۗ وَاسْتَشْهِدُوْا شَهِيْدَيْنِ مِنْ رِّجَالِكُمْ ۚ فَاِنْ لَّمْ يَكُوْنَا رَجُلَيْنِ فَرَجُلٌ وَّامْرَاَتٰنِ مِمَّنْ تَرْضَوْنَ مِنَ الشُّهَدَۤاءِ اَنْ تَضِلَّ اِحْدٰىهُمَا فَتُذَكِّرَ اِحْدٰىهُمَا الْاُخْرٰى ۗ وَلَا يَأْبَ الشُّهَدَۤاءُ اِذَا مَا دُعُوْا ۗ وَلَا تَسْـَٔمُوْٓا اَنْ تَكْتُبُوْهُ صَغِيْرًا اَوْ كَبِيْرًا اِلٰٓى اَجَلِهٖ ۗ ذٰلِكُمْ اَقْسَطُ عِنْدَ اللّٰهِ وَاَقْوَمُ لِلشَّهَادَةِ وَاَدْنٰٓى اَلَّا تَرْتَابُوْٓا اِلَّآ اَنْ تَكُوْنَ تِجَارَةً حَاضِرَةً تُدِيْرُوْنَهَا بَيْنَكُمْ فَلَيْسَ عَلَيْكُمْ جُنَاحٌ اَلَّا تَكْتُبُوْهَا ۗ وَاَشْهِدُوْٓا اِذَا تَبَايَعْتُمْ ۖ وَلَا يُضَاۤرَّ كَاتِبٌ وَّلَا شَهِيْدٌ ۗ وَاِنْ تَفْعَلُوْا فَاِنَّهٗ فُسُوْقٌۢ بِكُمْ ۗ وَاتَّقُوا اللّٰهَ ۗ وَيُعَلِّمُكُمُ اللّٰهُ ۗ وَاللّٰهُ بِكُلِّ شَيْءٍ عَلِيْمٌ

Artinya : “Wahai orang-orang yang beriman, apabila kamu berutang piutang untuk waktu yang ditentukan, hendaklah kamu mencatatnya. Hendaklah seorang pencatat di antara kamu menuliskannya dengan benar. Janganlah pencatat menolak untuk menuliskannya sebagaimana Allah telah mengajar-kan kepadanya. Hendaklah dia mencatat(-nya) dan orang yang berutang itu mendiktekan(-nya). Hendaklah dia bertakwa kepada Allah,

> Tuhannya, dan janganlah dia menguranginya sedikit pun. Jika yang berutang itu orang yang kurang akalnya, lemah (keadaannya), atau tidak mampu mendiktekan sendiri, hendaklah walinya mendiktekannya dengan benar. Mintalah kesaksian dua orang saksi laki-laki di antara kamu. Jika tidak ada (saksi) dua orang laki-laki, (boleh) seorang laki-laki dan dua orang perempuan di antara orang-orang yang kamu sukai dari para saksi (yang ada) sehingga jika salah seorang (saksi perempuan) lupa, yang lain mengingatkannya. Janganlah saksi-saksi itu menolak apabila dipanggil. Janganlah kamu bosan mencatatnya sampai batas waktunya, baik (utang itu) kecil maupun besar. Yang demikian itu lebih adil di sisi Allah, lebih dapat menguatkan kesaksian, dan lebih mendekatkan kamu pada ketidakraguan, kecuali jika hal itu merupakan perniagaan tunai yang kamu jalankan di antara kamu. Maka, tidak ada dosa bagi kamu jika kamu tidak mencatatnya. Ambillah saksi apabila kamu berjual beli dan janganlah pencatat mempersulit (atau dipersulit), begitu juga saksi. Jika kamu melakukan (yang demikian), sesungguhnya hal itu suatu kefasikan padamu. Bertakwalah kepada Allah, Allah memberikan pengajaran kepadamu dan Allah Maha Mengetahui segala sesuatu." (QS 2:282)

Ayat ini menekankan pentingnya pencatatan dan pengawasan dalam transaksi keuangan, yang sejalan dengan sistem pengawasan CCTV dan pemantauan *real-time* pada ATM untuk memastikan keamanan dan transparansi dalam layanan perbankan.

Selain aspek keamanan, keberlanjutan operasional ATM juga menjadi perhatian utama. Pemadaman listrik dapat menyebabkan ATM tidak dapat digunakan, yang berpotensi mengganggu layanan perbankan dan merugikan nasabah (Chen et al., 2020). Oleh karena itu, penggunaan *Uninterruptible Power Supply* (UPS) menjadi solusi untuk menjaga pasokan daya cadangan agar ATM tetap berfungsi saat terjadi gangguan listrik. Dengan integrasi berbasis IoT, status UPS dapat dipantau secara *real-time* untuk mendeteksi kondisi daya, kapasitas baterai, dan peringatan dini jika terjadi malfungsi (Singh & Kumar, 2021).

Selain meningkatkan keamanan, sistem pemantauan berbasis IoT juga berperan dalam memaksimalkan ketersediaan ATM dan mengurangi waktu henti akibat berbagai masalah teknis. Dengan pemantauan *real-time*, gangguan operasional dapat dideteksi lebih awal, memungkinkan tindakan korektif dilakukan secara cepat dan efektif. Hal ini membantu memastikan bahwa ATM tetap dapat digunakan oleh nasabah tanpa hambatan, meningkatkan keandalan sistem perbankan secara keseluruhan (Nguyen & Lee, 2023).

Perkembangan teknologi *Internet of Things* (IoT) menawarkan solusi untuk meningkatkan efektivitas sistem pengawasan. Dengan mengintegrasikan protokol komunikasi ringan seperti *Message Queuing Telemetry Transport* (MQTT), sistem pengawasan dapat mengirimkan data secara *real-time* dengan efisiensi tinggi. MQTT dirancang untuk perangkat dengan sumber daya terbatas dan jaringan dengan bandwidth rendah, menjadikannya ideal untuk aplikasi pengawasan berbasis IoT.

Penggunaan IoT dalam sistem pengawasan CCTV dan UPS pada ATM memungkinkan pemantauan yang lebih efektif dan efisien. Teknologi ini memungkinkan pengiriman data secara *real-time* ke server pusat, sehingga pihak terkait dapat melakukan analisis dan tindakan preventif lebih cepat. Dengan sistem ini, keamanan dan keandalan ATM dapat ditingkatkan, memberikan perlindungan yang lebih baik bagi nasabah dan pihak perbankan (Martinez et al., 2023).

Dalam era digitalisasi layanan keuangan, mesin *Automated Teller Machine* (ATM) tetap menjadi salah satu fasilitas yang paling sering digunakan oleh masyarakat dalam melakukan transaksi perbankan. Meskipun demikian,

keberadaan ATM kerap kali menjadi sasaran tindakan kriminal seperti pencurian, perusakan, skimming, bahkan sabotase sistem daya. Berdasarkan data dari Bank Indonesia (2022), terdapat lebih dari 100 ribu unit ATM aktif di Indonesia, dan kasus kejahatan terhadap ATM masih terjadi di berbagai wilayah, terutama pada lokasi yang minim pengawasan langsung.

Efisiensi laporan kriminalitas terhadap CCTV merujuk pada kemampuan sistem pengawasan menggunakan kamera CCTV dalam mempercepat, mempermudah, dan meningkatkan akurasi proses pelaporan tindakan kriminal. Dengan kata lain, efisiensi ini mencakup bagaimana penggunaan CCTV, terutama yang berbasis *Internet of Things* (IoT), dapat mengurangi waktu dan tenaga dalam mendeteksi, merekam, serta menyampaikan informasi tentang kejadian kriminal kepada pihak yang berwenang (Lutviansyah, 2025).

Pada sistem konvensional, pelaporan tindakan kriminal yang terekam oleh CCTV seringkali membutuhkan waktu lama karena rekaman harus diambil, ditinjau secara manual, dan dilaporkan ke pihak berwenang secara terpisah. Proses ini dapat memperlambat respons terhadap kejahatan dan memungkinkan pelaku melarikan diri atau menghilangkan jejak (Susilo, 2024).

Sebaliknya, dengan penerapan sistem CCTV berbasis IoT, informasi dapat dikirim secara otomatis dan *real-time*, dilengkapi dengan dokumentasi digital yang dapat diakses dari jarak jauh. Hal ini memungkinkan pelaporan terjadi dalam waktu singkat setelah kejadian terdeteksi, sekaligus memberikan data yang lebih akurat dan mudah dianalisis. Efisiensi ini berdampak langsung pada penurunan risiko

kerugian, peningkatan keamanan, serta efektivitas kerja aparat atau petugas keamanan.

Sejumlah penelitian terdahulu telah membahas implementasi IoT dalam konteks pengawasan ruangan dengan menggunakan kamera CCTV. Misalnya, penelitian oleh Liu et al. (2017) mengusulkan pendekatan untuk memantau aktivitas dan keamanan ruangan menggunakan jaringan kamera CCTV yang terhubung ke platform IoT. Penelitian ini menunjukkan bahwa integrasi kamera CCTV dalam sistem pengawasan ruangan dapat meningkatkan respons terhadap kejadian dan memungkinkan pemantauan yang lebih akurat. Namun, masih terdapat kebutuhan untuk lebih mendalam mengkaji implementasi yang praktis dan terintegrasi dari berbagai kamera CCTV dalam satu sistem pengawasan ruangan berbasis IoT. Ada gap signifikan terkait dengan pengembangan arsitektur sistem yang optimal untuk menghubungkan dan mengelola data dari kamera-kamera CCTV yang berbeda secara efisien.

Untuk meningkatkan efisiensi lebih lanjut, dibutuhkan sistem yang tidak hanya mampu merekam, tetapi juga dapat mengidentifikasi kejadian penting secara otomatis. Dalam konteks ini, metode *Finite State Automata* (FSA) dapat diterapkan sebagai model sistem untuk mengenali pola kejadian tertentu dalam alur video pengawasan. FSA mampu memetakan transisi antar status dalam suatu sistem berbasis input tertentu ketika suatu kondisi terpenuhi, sistem dapat mengaktifkan perintah otomatis seperti penyimpanan segmen rekaman atau permintaan akses data rekaman oleh sistem terhubung (Juieta, 2023).

Dengan menggabungkan kekuatan FSA dan konektivitas IoT, sistem pengawasan berbasis CCTV dapat dimodifikasi menjadi sistem yang reaktif, efisien, dan mudah diakses, khususnya dalam konteks pelaporan tindak kriminal. Proses verifikasi dan dokumentasi kejadian tidak lagi membutuhkan prosedur manual yang lambat, melainkan dapat dilakukan secara otomatis dan berbasis sistem, sehingga memberikan respons yang lebih cepat terhadap situasi darurat dan mempercepat proses hukum (Juieta, 2023).

Berdasarkan hal tersebut, penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem pengawasan CCTV berbasis IoT pada ATM secara *real-time*. Diharapkan sistem ini dapat meningkatkan efektivitas pengawasan, meminimalkan risiko keamanan, serta memastikan operasional ATM tetap berjalan tanpa hambatan dan memiliki ketersediaan yang optimal.

Oleh karena itu, penelitian ini bertujuan untuk merancang dan mengevaluasi sistem pengawasan CCTV pada ATM yang terintegrasi dengan teknologi IoT menggunakan protokol MQTT. Dengan pendekatan ini, diharapkan sistem dapat memberikan pengawasan yang lebih efektif, responsif, dan efisien dalam mendeteksi serta menanggapi ancaman keamanan pada ATM.

1.2 Pernyataan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana tingkat efisiensi sistem pengawasan CCTV berbasis IoT dalam mengurangi waktu pelaporan kejadian dibandingkan dengan sistem konvensional?

2. Seberapa besar efisiensi penggunaan bandwidth pada sistem CCTV berbasis IoT dengan protokol MQTT dibandingkan sistem CCTV konvensional?
3. Bagaimana perbandingan waktu respon antara sistem pengawasan konvensional dan sistem pengawasan *real-time* berbasis IoT terhadap kejadian kriminal di sekitar ATM?
4. Sejauh mana keberhasilan sistem pengawasan *real-time* berbasis IoT dalam mendeteksi kejadian secara langsung dibandingkan dengan sistem pengawasan konvensional?

1.3 Tujuan Penelitian

Berdasarkan latar belakang dan pernyataan masalah diatas, maka tujuan dari penelitian ini adalah:

1. Menganalisis efisiensi waktu pelaporan kejadian kriminalitas pada sistem pengawasan CCTV berbasis IoT dibandingkan dengan sistem pengawasan konvensional.
2. Menganalisis efisiensi penggunaan bandwidth pada sistem CCTV berbasis IoT dengan protokol MQTT dibandingkan dengan sistem CCTV konvensional.
3. Mengukur waktu respon sistem CCTV berbasis IoT terhadap kejadian kriminalitas dan membandingkannya dengan sistem konvensiona.
4. Mengevaluasi tingkat keberhasilan pemantauan *real-time* sistem pengawasan CCTV berbasis IoT dalam mendeteksi kejadian di sekitar ATM dibandingkan sistem konvensional.

1.4 Manfaat Penelitian

Berikut adalah manfaat yang diharapkan dari penelitian ini:

1. Meningkatkan keamanan ATM dengan sistem pengawasan CCTV berbasis IoT yang memungkinkan pemantauan *real-time* dan respons cepat terhadap insiden keamanan.
2. Meminimalkan downtime ATM akibat gangguan daya dengan pemantauan UPS berbasis IoT, sehingga ketersediaan layanan ATM tetap optimal.
3. Meningkatkan rasa aman saat menggunakan ATM karena adanya pemantauan yang lebih ketat dan sistem respons cepat terhadap ancaman keamanan.
4. Memberikan landasan bagi inovasi dalam manajemen sistem pengawasan keamanan dan kelistrikan berbasis IoT di berbagai sektor lainnya.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Penelitian ini hanya membahas sistem pengawasan *Closed Circuit Television* (CCTV) berbasis IoT untuk pemantauan keamanan ATM secara *real-time*.
2. Fungsi sistem difokuskan pada pemantauan visual (video) secara *real-time*, penyimpanan rekaman.
3. Penelitian ini difokuskan pada ATM yang berada di lokasi tertentu, bukan dalam skala nasional atau seluruh jaringan ATM dari berbagai bank.

4. Penelitian ini tidak membahas bentuk kejahatan perbankan yang terjadi melalui layanan Mobile Banking (M-Banking), seperti penipuan digital, phishing, atau pencurian data melalui aplikasi perbankan seluler.
5. Meskipun kejahatan digital semakin meningkat, penelitian ini difokuskan untuk menjawab kebutuhan pengawasan fisik ATM yang tetap relevan, terutama di wilayah atau situasi dengan tingkat kriminalitas langsung (fisik) yang tinggi.

BAB II

STUDI PUSTAKA

2.1 Kajian Penelitian Terkait

Penelitian telah dilakukan untuk mengembangkan sistem pengawasan ATM, baik dalam aspek keamanan maupun keandalan operasionalnya. Penelitian-penelitian ini mencakup penerapan teknologi *Closed Circuit Television* (CCTV), *Uninterruptible Power Supply* (UPS), serta pemanfaatan *Internet of Things* (IoT) dalam pemantauan sistem. Berikut adalah beberapa penelitian yang relevan:

Tabel 2. 1 Penelitian Terdahulu

No	Nama Peneliti dan Tahun	Judul	Metode	Ekstraksi Fitur	Persamaan	Perbedaan
1	Dharmawan et al. (2021)	Efektivitas CCTV dalam Meningkatkan Keamanan ATM	Studi Kasus	CCTV untuk pemantauan keamanan ATM	Membahas keamanan ATM menggunakan CCTV	Tidak mendukung pemantauan *real-time*
2	Hussain et al. (2019)	Pemantauan UPS Berbasis Sensor untuk ATM	Eksperimen	Sensor pemantauan UPS untuk menjaga daya cadangan	Fokus pada keandalan daya ATM	Tidak terintegrasi dengan CCTV
3	Zhang et al. (2022)	Integrasi IoT pada Sistem Keamanan ATM	Pengembangan Sistem	IoT untuk pemantauan CCTV ATM	Sama-sama menggunakan IoT untuk pemantauan	Tidak membahas aspek daya/UPS
4	Rahman et al. (2020)	Sistem IoT untuk Pemantauan Kondisi Listrik ATM	Eksperimen	IoT dan sensor listrik untuk deteksi	Sama-sama menggunakan IoT dan pemantauan *real-time*	Tidak secara khusus membahas ATM

No	Nama Peneliti dan Tahun	Judul	Metode	Ekstraksi Fitur	Persamaan	Perbedaan
				anomali daya		
5	Santoso et al. (2018)	Keandalan UPS dalam Operasional ATM	Studi Kasus	UPS sebagai solusi cadangan daya ATM	Fokus pada keandalan daya ATM	Tidak mendukung pemantauan jarak jauh
6	Putra et al. (2021)	Model Integrasi CCTV dan UPS Berbasis IoT	Pengembangan Sistem	Pemantauan ATM dengan integrasi CCTV dan UPS berbasis IoT	Membahas pengawasan *real-time* ATM	Belum optimal dalam respons otomatis
7	Kim et al. (2019)	Penerapan AI pada CCTV ATM untuk Deteksi Kejahatan	Pengembangan AI	AI dan IoT untuk analisis rekaman CCTV ATM	Sama-sama menggunakan IoT untuk pemantauan	Menggunakan AI, bukan UPS
8	Yusuf et al. (2023)	Sensor IoT untuk Pemantauan Lingkungan ATM	Eksperimen	Sensor IoT untuk mendeteksi suhu dan kelembaban ATM	Sama-sama menggunakan IoT untuk pemantauan ATM	Tidak secara langsung membahas keamanan

Tabel ini menunjukkan bahwa penelitian sebelumnya telah mengkaji berbagai aspek sistem keamanan ATM, baik dari sisi pemantauan CCTV maupun penerapan IoT. Namun, penelitian ini menawarkan pendekatan yang lebih komprehensif dengan mengintegrasikan CCTV berbasis IoT dalam satu sistem pemantauan *real-time*, sehingga dapat meningkatkan keamanan dan keandalan ATM secara simultan.

2.2 Efisiensi

Efisiensi adalah istilah yang dipakai untuk mengukur kemampuan pemanfaatan asset produksi. Semakin mendekati ideal, dikatakan semakin efisien, begitu juga sebaliknya. Oleh karena itu efisensi berkaitan dengan bagaimana seharusnya suatu asset dikelola. Efisiensi di ukur dengan sebagaimana seharusnya penggunaan asset atau membatasi hal-hal yang mubazir, pengukuran diperlukan untuk banyak hal dalam rangka pengembangan bisnis. Oleh karena itu efisiensi ini berkaitan dengan rantai nilai (*value chain*), yaitu keterkaitan antar aktifitas yang dilakukan dalam menciptakan barang dan jasa (Noor, 2017).

Menurut Farel dalam Ascaraya menyebutkan bahwa efisiensi dari perusahaan terdiri dari dua komponen, yaitu efisiensi teknis dan efisiensi alokatif. Efisiensi teknis menggambarkan kemampuan dari perusahaan dalam menghasilkan output dengan sejumlah input yang tersedia. Sedangkan efisiensi alokatif menggambarkan kemampuan perusahaan dalam mengoptimalkan penggunaan inputnya dengan struktur harga dan teknologi produksinya (Ascarya, 2019).

Ahmad Syakir Kurnia dalam Maflachatun menjelaskan bahwa secara keseluruhan efisiensi perbankan dapat didekomposisikan dalam efisiensi skala (*scale efficiency*), efisiensi cakupan (*scope efficiency*), efisiensi teknik (*technical efficiency*), dan efisiensi alokasi (*allocative efficiency*). Bank dikatakan mencapai efisiensi dalam skala ketika bank bersangkutan mampu beroperasi dalam skala hasil yang konstan (*constant return to scale*), sedangkan efisiensi cakupan tercapai ketika bank mampu beroperasi pada diversifikasi lokasi. Efisiensi alokasi tercapai ketika bank mampu menentukan berbagai output yang memaksimumkan keuntungan,

sedangkan efisiensi teknik pada dasarnya menyatakan hubungan antara input dengan output dalam suatu proses produksi. Proses produksi dikatakan efisien, apabila pada penggunaan input sejumlah tertentu dapat dihasilkan output yang maksimum atau untuk menghasilkan output sejumlah tertentu digunakan input yang paling minimum (Maflachatun, 2020)

2.3 *Finite State Automata* (FSA)

Finite State Automata atau biasa disebut FSA, merupakan sebuah model matematika dari suatu sistem yang menerima suatu input dan menghasilkan sebuah output diskret. FSA memiliki state yang banyaknya terbatas, dan dapat dipindahkan dari satu state ke state lain. State adalah kondisi, keadaan, atau kedudukan. Prinsip kerja Finite State Automata sendiri adalah dengan cara mesin pembaca perintah membaca memori masukan yang berupa tape yaitu 1 karakter di setiap menggunakan head baca yang dikendalikan oleh kontak kendali state berhingga dimana pada mesin tersebut terdapat sejumlah state berhingga. Finite State Automata selalu dalam kondisi yang disebut dengan state awal pada saat finite automata mulai membaca. Perubahan dari state terjadi pada mesin saat sebuah karakter selanjutnya dibaca. Ketika sebuah head telah sampai pada akhir-an tape dan dalam kondisi state akhir, maka string yang terdapat pada tape akan dikatakan diterima Finite Automata (Sujana, 2019).

Teori Bahasa Otomata merupakan cabang ilmu yang menerapkan model dan ide tentang komputer. Tahapan paling vital dalam pembuatan model dan pemikiran untuk menyampaikan metode perancangan dalam perencanaan, baik

sebagai peralatan maupun pemrograman dapat menggunakan konsep teori bahasa dan otomata (Aston, 2019).

Finite State Automata atau disebut Finite State Machine merupakan salah satu metode dalam teori bahasa otomata yang dapat digunakan dalam mengamati dan menangkap contoh dalam informasi. Finite State Automata adalah model matematika yang digunakan untuk merepresentasikan suatu sistem yang memiliki berbagai keadaan (state) yang dapat berubah-ubah seiring dengan waktu dimana terdiri dari beberapa komponen seperti simbol masukan, fungsi transisi, keadaan awal, dan keadaan akhir (Hamdan, 2021).

2.4 Topologi Jaringan Komputer

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan (Kurnia, 2017:30). Topologi menggambarkan struktur dari suatu jaringan atau bagaimana jaringan didesain. Topologi dibagi menjadi beberapa jenis, dibawah ini adalah beberapa jenis topologi yang paling sering digunakan :

1. Topologi *Bus*

   Topologi *Bus* adalah sebuah topologi yang media pengirimannya menggunakan sebuah kabel pusat (*backbone*) yang menghubungkan antara *client* dan *server*. Topologi Bus menggunakan kabel BNC dan dibagian kedua ujung kabel diberi *terminator*. Adapun kelebihan dan kekurangan topologi *Bus*.

   a. Kelebihan

      1) Hemat kabel.

2) Denah kabel sederhana.

3) Pemasangan pengguna baru dapat dilakukan dengan mudah tanpa menggangu pengguna lain.

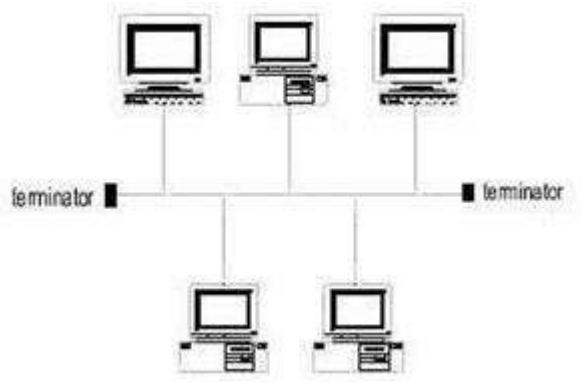
b. Kekurangan

1) Jika terjadi kerusakan deteksi dan perbaikan sangat sulit.

2) Rawan terjadi tabrakan data.

3) Kepadatan di jalur *backbone.*

4) Diperlukan *repeater* untuk jarak jauh



Gambar 2. 1 Topologi Bus

2. Topologi *Ring*

Topologi *Ring* adalah topologi berbentuk rangkaian titik yang masing-masing terhubung ke dua titik lainnya, sedemikian jalur melingkar membentuk cincin. Pada topologi ini setiap titik/*node* berfungsi sebagai *repeater* yang akan memperkuat sinyal disepanjang jalur kabel. Adapun kelebihan dan kekurangan dari topologi ini, yaitu sebagai berikut :

a. Kelebihan

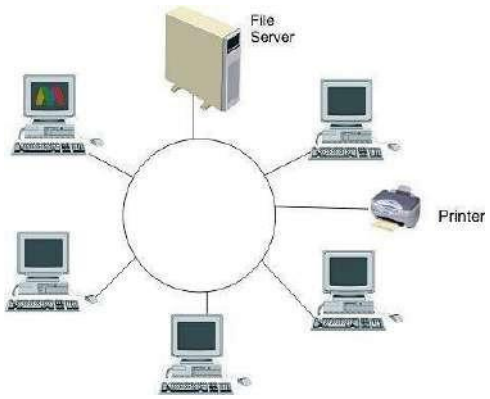
1) Mudah untuk dirancang dan diimplematasikan.

2) Memiliki performa yang lebih baik dari topologi *Bus.*

3) Mudah untuk melakukan pelacakan dan pengisolasian kesalahan jaringan.
4) Hemat kabel.
5) Tidak akan ada tabrakan pengiriman data (*collision*).

b. Kekurangan

1) Pengembangan jarigan kaku.
2) Kinerja komputer tepusat pada *node* sebelah.



Gambar 2. 2 Topologi *Ring*

2. Topologi *Star*

Topologi *Star* adalah toplogi yang berupa kovergensi dari *nod*e tengah ke setiap pengguna. Masing-masing pengguna terhubung langsung ke *server* atau *switch/hub*. Adapun keuntungan dan kekurangan topologi adalah sebagai berikut :

a. Keuntungan

1) Kerusakan pada satu saluran hanya akan mempengaruhi pada saluran tersebut dan *client* yang terhubung.
2) Tingkat keamanan paling tinggi.
3) Penambahan dan pengurangan *client* dapat dilakukan

dengan mudah tanpa menggangu *client* lain.

4) Akses kontrol terpusat.

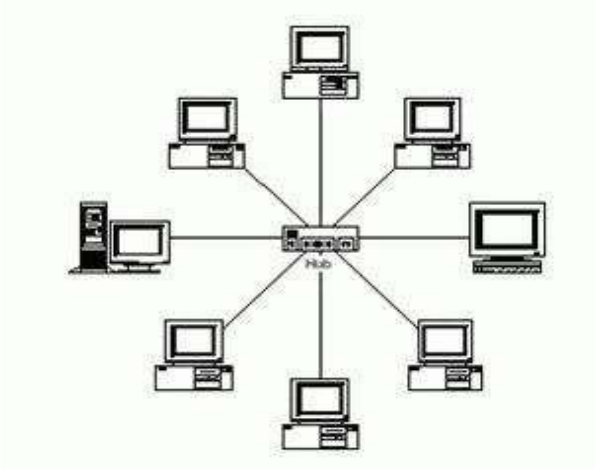
5) Paling fleksibel

b. Kerugian

1) Boros dalam pemakaian kabel.

2) *Switch/hub* sebagai elemen pusat.

3) Jika *node* tengah rusak maka semua jaringan akan terputus.



Gambar 2. 3 Topologi *Star*

2.5 *Closed Circuit Television* (CCTV)

CCTV (*Closed Circuit Television*) adalah kamera video digital yang digunakan untuk mengirim sinyal ke layar monitor di suatu ruang atau tempat tertentu. Hal tersebut memiliki tujuan untuk dapat memantau situasi dan kondisi tempat tertentu. Pada umumnya CCTV seringkali digunakan untuk mengawasi area *public*. Awalnya gambar dari kamera CCTV hanya dikirim melalui kabel ke sebuah ruang monitor tertentu dan dibutuhkan pengawasan secara langsung oleh operator/petugas keamanan dengan resolusi gambar yang masih rendah. Namun seiring dengan perkembangan teknologi yang sangat pesat seperti saat ini, banyak

kamera CCTV yang telah menggunakan sistem teknologi yang modern. Sistem kamera CCTV digital saat ini dapat dioperasikan maupun dikontrol melalui Personal Computer atau Telephone genggam, serta dapat dimonitor dari mana saja dan kapan saja selama ada komunikasi dengan internet maupun akses GPRS. (Astra, Mardiana, 2018).

Sistem CCTV biasanya terdiri dari komunikasi fixed (*dedicated*) antara kamera dan monitor. Teknologi CCTV modern terdiri dari sistem terkoneksi dengan kamera yang bisa digerakkan (diputar, ditekuk, dan di-*zoom*) serta dapat dioperasikan dari jarak jauh lewat ruang kontrol, dan dapat dihubungkan dengan suatu jaringan baik LAN, *Wireless*-LAN maupun internet. (Atmoko, 2005)

Keberhasilan sistem CCTV ditentukan oleh kualitas elemen-elemen yang mendukung sistem tersebut diantaranya adalah:

1. Kamera: Berdasarkan kategori bentuk terbagi menjadi dua macam yaitu *fixed camera* (Posisi Kamera tidak bisa berubah ubah) dan PTZ (*Pan Tilt Zoom*) camera (Posisi Kamera dapat berubah dan dapat di zoom).
2. Media Transmisi: Media transmisi dari CCTV menggunakan kabel koaksial atau UTP sedangkan *wireless* menggunakan *acces point* berupa *Router*.
3. Monitor: menampilkan objek yang ditangkap oleh kamera.
4. Aplikasi piranti lunak: suatu aplikasi yang dapat mengontrol CCTV dari suatu tempat dan dapat diintergrasikan dengan *server* penyimpanan *video*.

5. Media Penyimpanan: DVR (*Digital Video Recorder*) atau *Hardisk*.

CCTV (*Closed Circuit Television*) adalah suatu alat yang dapat mengirimkan informasi video transmisi melalui kelokasi terentu yang dapat dipasang di suatu tempat seperti dalam ruangan yang ingin dapat dilihar secara real time. (Hadiwijaya, 2014:1). Pada umumnya fungsi dari CCTV adalah sebagai pemantau baik pada bidang keamanan ataupun industry. Kebutuhan manusia akan sistem pemantauan terus meningkat seiring dengan perkembangan teknologi yang semakin canggih. Perangkat kamera pun beralih dari kamera yang menggunakan kabel kamera analog menuju kamera nirkabel (*wireless*) yaitu *webcam*. Kelebihan kamera webcam ini sistem mampu memantau kondisi ruangan dari jarak jauh, selain dapat merekam video secara manual dan dapat dikembangkan dengan fitur dapat mendeteksi adanya suatu gerakan.

1. *Digital Video Recorder* (DVR)

   Pengertian DVR adalah sebuah alat perekam yang sangat mudah digunakan terhadap kamera CCTV. Dengan alat perekam ini memungkinkan kamera CCTV bisa diakses atau dimonitoring dari mana saja di seluruh dunia dengan menggunakan kabel telepon, internet dan handphone yang sudah disupport GPRS/3G. Beberpa model terbaru dengan tambahan fitur motion dectection, remote viewing, MPEG-4 dan H264 video format, sistem backup yang mudah baik itu ke USB, CD RW, DVD RW dan bisa juga diakses lewat LAN ataupun internet. Adapun beberapa kelebihan DVR dalam pengaplikasiannya terhadap CCTV yakni: 1) DVR lebih stabil. Hal ini dikarenakan DVR dirancang khusus didalam

satu circuit board dan dapat ditambah dengan *harddisk* sebagai media penyimpanan data. 2) DVR membututhkan daya yang lebih sedikit dari pada PC *Based System*. Di Era yang harus hemat listrik ini, setidaknya faktor ini juga bisa dijadikan pertimbangan tentang sistem CCTV mana yang akan digunakan. (Atmoko, 2005).

DVR atau banyak disebut Digital Video Recorder adalah perangkat yang digunakan oleh camera CCTV untuk merekam semua gambar yang dikirim oleh camera ke dalam perangkat ini. Terbagi dalam 2 kategori utama, yaitu Stand Alone DVR PC Card DVR. Banyak fitur dari DVR yang bisa dimanfaatkan untuk pelengkap keamanan, salah satunya adalah merekam semua kejadian dimana hasil rekaman bisa dan seringkali dipergunakan didalam peradilan untuk membuktikan suatu kejadian atau perkara. Terdapat berbagai jenis DVR yang bisa dipergunakan dengan fitur dan spesifikasi yang berbeda-beda. Spesifikasi DVR inilah yang menetukan berapa jumlah kamera yang bisa dipasang dan kualitas gambar yang dihasilkan. Adapun jenis-jenis DVR adalah sebagai berikut :

a. DVR 4 Channel (untuk 1-4 Kamera) DVR 4 Channel adalah jenis DVR yang memiliki hanya 4 saluran video. Macam DVR ini cocok untuk rumah, toko, gudang, atau kantor scala kecil. Untuk anda yang memiliki budget terbatas tersedia berbagai dvr murah namun memiliki fitur yang cukup seperti remote kontrol untuk kemudahan penggunaan, port USB utk back up data, dan format

H.264 kompresi tinggi terbaru untuk menghemat kapasitas media penyimpanan rekaman CCTV anda.

b. DVR 8 Channel Kamera CCTV, Jenis DVR ini memiliki 8 saluran video. Cocok untuk perumahan, bisnis ritel dan komersial skala menengah. Fitur yang tersedia hampir sama dengan dvr 4 channel seperti remote kontrol untuk penggunaan jarak jauh, CD / DVD Rewriters dan port USB untuk back up data, dan format kompresi tinggi terbaru H.264.

c. *Digital Video Recorder* DVR 16 Channel Saat ini, jenis *Digital Video Recorder* terbaik adalah DVR 16 channel yang mampu menghubungkan hingga 16 kamera CCTV analog. DVR 16 channel sangat cocok untuk rumah berukuran luas, gudang, perkantoran, pabrik, mall dan berbagai fasilitas publik lainnya.

Definisi resolusi pada DVR adalah dimensi gambar yang ditangkap oleh CCTV dan diproses oleh DVR, baik itu proses displaying maupun record. Proses *displaying* adalah menampilkan gambar yang ditangkap dari hasil tangkapan kamera CCTV ke tempat penyimpanan berupa *harddisk*. Dimensi gambar hasil tanggapan CCTV tersebut berupa lebar x panjang. Ada 3 macam resolusi yang digunakan pada DVR seperti CIF (360x288), Half D1 (720x288), dan D1 (720x576). Resolusi paling tinggi adalah D1. Kebanyakan *installer* menggunakan resolusi CIF, alasannya selain lebih sedikit memakan ruang harddisk juga *frame rate*

yang digunakan lebih cepat, baik itu pada saat *playback* maupun *streaming* via jaringan Gambar 2.2 Tampilan Resolusi DVR (Artikel CCTV, 2010).

Pengadaan sebuah DVR lebih mendasar mempunyai titik berat pada aspek keamanan. DVR untuk keperluan keamanan dapat dibagi menjadi 2 kategori yaitu DVR berbasis *personal computer* (PC) dan DVR sebagai *embedded system*. DVR berbasis PC adalah sebuah PC yang dilengkapi oleh sebuah video capture card. DVR sebagai *embedded system* yaitu DVR yang sudah dilengkapi dengan sistem operasi dan piranti lunak aplikasi (Budi, 2009).

2. *IP Camera*

IP Camera merupakan perkembangan dari CCTV. Yang membedakannya dengan CCTV biasa F-12 adalah setaip kamera memiliki IP sendiri sehingga kita bisa memilih kamera mana yang mau dilihat. IP Camera memungkinkan pemilik rumah dan bisnis untuk melihat kamera mereka melalui koneksi internet yang tersedia baik melalui computer maupun mobile phone yang mendukung 3G. IP Camera dalam konfigurasinya yang lebih mudah serta kinerja yang lebih baik menjadikan banyak orang mulai beralih ke IP Camera, sehingga banyak orang menamakan IP Camera sebagai IP Camera CCTV. (Mahatma dkk, 2010:12)

IP Camera atau biasa disebut Netcam (*Network Camera*) merupakan perangkat peng-*capture* dan *recording* objek terkini yang memiliki kemampuan memproses visual dan audio serta dapat diakses PC

serta langsung, atau melalui LAN, internet, dan jaringan telepon seluler. (Aryanto, 2010:6)

Instalasinya sangat sederhana. Sebuah IP Camera ditempatkan di lokasi yang telah di tentukan guna memantau keadaan, kemudian lakukan setting melalui PC secara langsung atau melalui jaringan. Perangkat ini dapat di akses dari mana saja selama terkoneksi dengan internet, baik dengan laptop maupun telepon seluler. Ada dua jenis IP Camera yang tersedia yaitu, tipe Sentralisasi dan desentralisasi.

a. IP Camera Sentralisasi : Jenis IP Camera ini memerlukan pusat *Network Video Recorder* (NVR) untuk merekam video dan manajemen alarm.
b. IP Camera desentralisasi : Jenis IP Camera ini tidak memerlukan pusat NVR karena kamera telah memiliki fungsi perekam *built-in* sehingga dapat merekam langsung ke media penyimpanan seperti SD Card, NAS (*Network Attached Atorage*), komputer, atau server.

3. Konfigurasi NVR

Konfigurasi NVR (*Network Video Recorder*) adalah serangkaian langkahlangkah yang dilakukan untuk mengatur dan mengoptimalkan fungsi NVR dalam suatu sistem pengawasan CCTV. *Network Video Recorder* (NVR) adalah sistem yang menampilkan aplikasi perangkat lunak. Sistem ini dirancang untuk mengumpulkan dan menyimpan video yang diambil oleh semua kamera yang terhubung ke jaringan. NVR

merekam video ini pada perangkat penyimpanan massal. Tidak seperti perangkat penyimpanan lainnya, perangkat ini tidak memiliki perangkat keras perekam video khusus, dan perangkat lunak dioperasikan pada perangkat khusus. NVR biasanya digunakan pada sistem pengawasan video IP, dan mampu melakukan streaming data video/audio pada satu kabel (Versitron, 2023).

Komponen NVR meliputi

a. Kamera IP, yang memproses data video sebelum mengirimkannya ke NVR
b. Perekam, yang merekam video dari kamera IP
c. Sistem penyimpanan, yang menyimpan rekaman video ke *hard disk*, *flash drive* USB, *disk drive*, kartu memori SD, atau penyimpanan *cloud*
d. Kemampuan jaringan, yang mentransfer video dan gambar melalui jaringan

Pada umumnya fungsi dari CCTV adalah sebagai pemantau baik pada bidang keamanan ataupun industri. Kebutuhan manusia akan sistem pemantauan terus meningkat seiring dengan perkembangan teknologi yang semakin canggih. Perangkat kamera pun beralih dari kamera yang menggunakan kabel kamera analog menuju kamera nirkabel (*wireless*) yaitu *webcam*. Kelebihan kamera *webcam* ini sistem mampu memantau kondisi ruangan dari jarak jauh selain dapat merekam video secara manual dan dapat dikembangkan dengan fitur dapat mendeteksi adanya suatu

gerakan yang akan menangkap gambar apabila adanya suatu gerakan. (Hadiwijaya, 2014)

Type kamera CCTV (*Closed Circuit Television*) terbagi menjadi dua, yaitu:

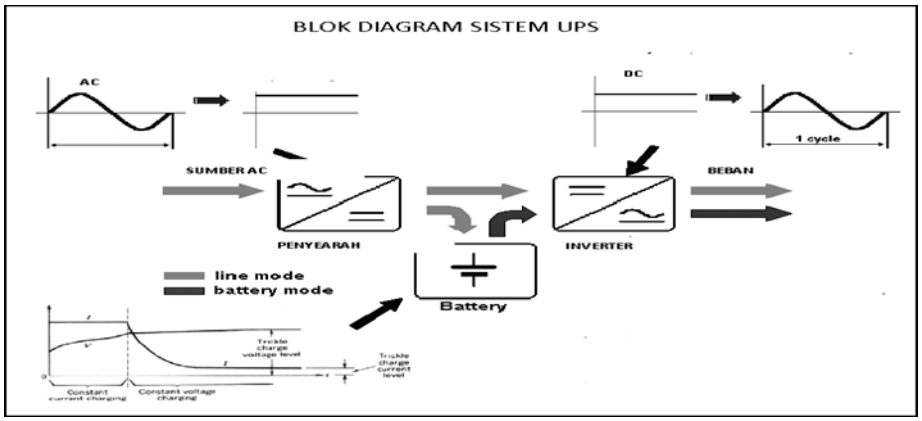
1. Kamera CCTV *Indoor*, yaitu kamera yang ditempatkan didalam gedung, umumnya berupa *Dome* (*Ceiling*) *Standard Box Camera*.
2. Kamera CCTV *Outdoor*, yaitu kamera yang ditempatkan di luar gedung dan memiliki casing yang dapat melindungi kamera terhadap hujan, debu, maupun temperatur yang extreme. Umumnya berupa *Bullets Camera* yang telah dilengkapi dengan *Infra Red Led* (Infra Red Camera). Disamping outdoor kamera, *standard box* kamera juga seringkali ditempatkan diluar dengan menggunakan tambahan *Outdoor Housing*. (Amin, 2018)

2.6 *Uninterruptible Power Supply* (UPS)

Uninterruptible Power Supply (UPS) adalah perangkat yang menggunakan baterai backup sebagai catuan daya alternatif, untuk dapat memberikan suplai daya sementara yang tidak terganggu untuk perangkat elektronik yang terpasang. UPS merupakan sistem penyedia daya listrik yang sangat penting dan diperlukan sekaligus dijadikan sebagai benteng dari kegagalan daya serta kerusakan sistem dan *hardware.*

Secara umum UPS terdiri dari tiga komponen utama yaitu *rectifier* (penyearah), baterai dan *inverter*. Prinsip kerja dari UPS secara umum terdiri atas 2 mode yaitu mode normal dan mode *back up*. Dalam mode normal, *rectifier* menyearahkan tegangan AC menjadi DC yang digunakan untuk mengisi baterai

dan menyuplai beban dengan melalui inverter terlebih dahulu. Sedangkan dalam mode *Back up* atau saat terjadi gangguan di suplai listrik utama, baterai menggantikan peran suplai utama untuk menyuplai beban. Pada keadaan ini, *inverter* akan mengubah tegangan DC baterai menjadi tegangan. Selanjutnya tegangan AC keluaran dari *inverter* kemudian dilewatkan filter inverter untuk mengurangi harmonisa orde tinggi sehingga didapatkan tegangan AC yang diinginkan.

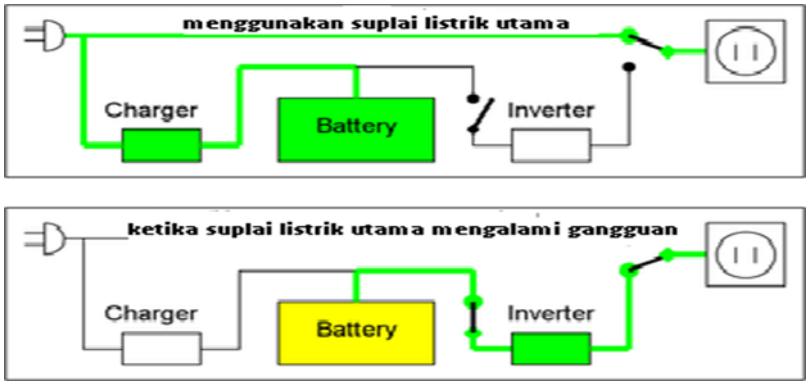


Gambar 2. 4 Blok Diagram UPS

Menurut standar IEC 62040-3 yang dikeluarkan oleh *International Electrotechnical Commission*, topologi UPS dibagi menjadi tiga jenis, yaitu :

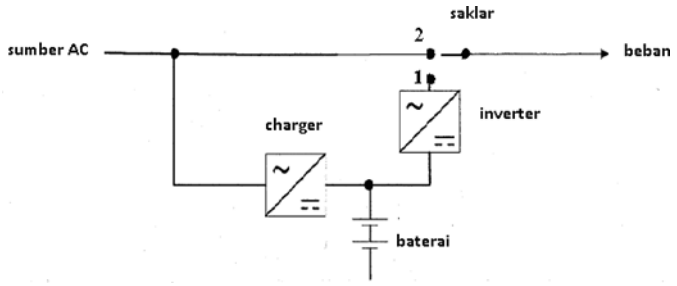
1. *Off-Line* / *standby*

   Pada *Off-Line*//*standby* UPS, beban system secara langsung disuplai oleh sumber listrik utama dan batterai akan bekerja menggantikan suplai listrik utama jika supplai listrik utama mengalami kegagalan atau gangguan. Blok diagram sistem kerja *standby* UPS ditunjukkan pada gambar 2.6.

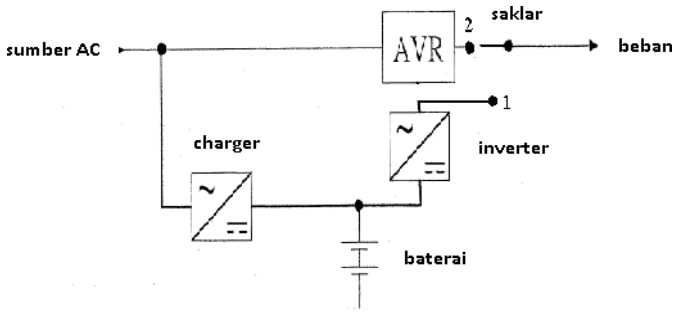


Gambar 2. 5 Blok diagram sistem kerja standby UPS

Blok rangkaian Offline UPS adalah seperti yang ditunjukkan pada gambar 2.7 dan 2.8.



Gambar 2. 6 Blok Rangkaian *Off-line* UPS



Gambar 2. 7 Blok Rangkaian *Off-line* UPS dengan AVR

Inverter dihubungkan paralel terhadap beban dan bekerja secara sederhana untuk menyalurkan daya pada beban. Mode operasi dari *Off-line* UPS ini dibagi menjadi 2 mode sesuai dengan posisi *switch* yaitu :

a. Normal mode

Pada mode ini, *switch* berada pada posisi 2, sehingga tegangan pada beban disuplai secara langsung oleh sumber AC dari PLN. Pada umumnya sebelum sampai pada beban terdapat peralatan tambahan seperti AVR yang berfungsi sebagai stabilisator tegangan. Pada saat mode ini juga baterai mengalami *charge* atau pengisian energi listrik.

b. *Back Up / Stored Energy* mode

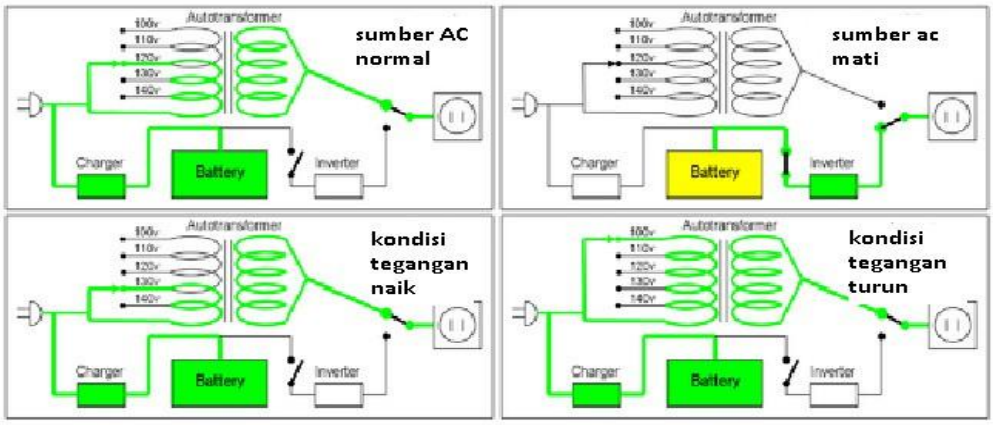
Ketika tegangan AC pada input UPS diluar spesifikasi tegangan yang diperbolehkan, *switch* akan berpindah dari posisi 2 ke posisi 1. Pada saat ini, tegangan pada beban disuplai oleh baterai yang sebelumnya telah dilakukan konversi tegangan DC pada baterai menjadi AC oleh *inverter*. Pergantian mode dari normal menuju *back up* mengakibatkan adanya waktu tunda *switching* dari posisi 2 ke posisi 1. UPS ini beroperasi sampai tegangan pada sisi input kembali pada keadaan normal.

UPS jenis ini mempunyai beberapa kelebihan seperti desain yang sederhana, biaya yang rendah, dan bentuk fisik yang relatif kecil. Kekurangan yang terdapat pada sistem ini yaitu kurangnya perlindungan atau sistem proteksi beban terhadap regulasi tegangan output, adanya waktu tunda *inverter* menyuplai tegangan pada beban. Waktu *switching* pergantian mode normal menuju mode *back up* hanya dapat diijinkan

untuk peralatan tertentu. Peralatan listrik lain yang sangat sensitif dan membutuhkan kekontinuitasan daya yang sempurna kurang sesuai menggunakan UPS jenis ini.

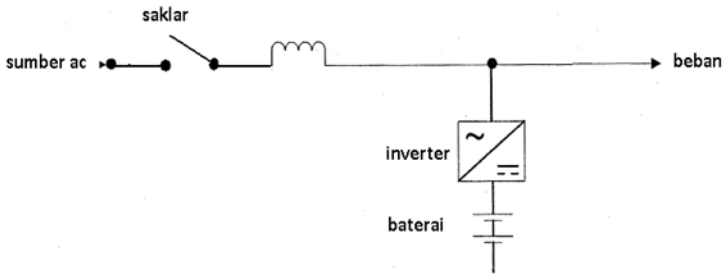
2. *Line-Interactive*

Pada *line-interactive* UPS, prinsip operasinya hampir sama dengan *offline/standbye* UPS tetapi dengan penambahan multi-tap variable-voltage autotransformer. Ini adalah tipe khusus dari transformer elektronik yang dapat menambah atau mengurangi lilitan kawat sehingga menambah atau mengurangi medan magnet dan tegangan keluaran dari transformer. Blok diagram sistem kerja *line interactive* UPS ditunjukkan pada gambar 2.9.

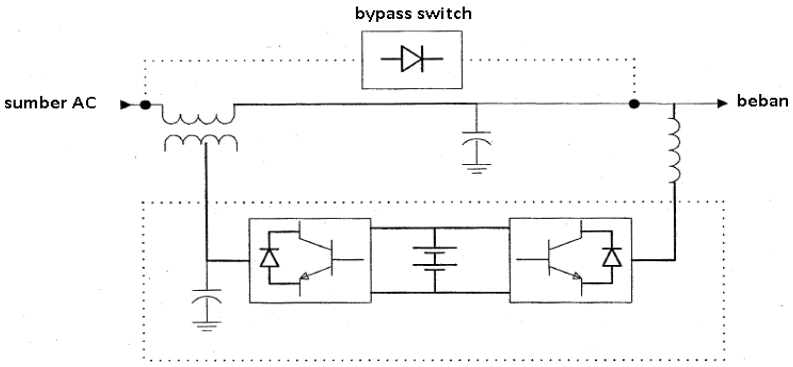


Gambar 2. 8 Blok Diagram Sistem Kerja Line Interactive

UPS Rangkaian UPS jenis ini dapat ditunjukkan pada Gambar 2.10 dan Gambar 2.11.



Gambar 2. 9 Line-Interactive UPS dengan Bidirectional Inverter



Gambar 2. 10 Line-Interactive UPS dengan Dua Konverter

Pada gambar 2.11, UPS jenis ini memerlukan induktor yang dipasang secara seri pada input dan bilateral inverter yang dipasang secara paralel dengan beban. Sedangkan pada Gambar 2.10 menggunakan dua konverter. Untuk konverter yang pertama dihubungkan secara seri dengan input, dan yang kedua dihubungkan secara paralel dengan beban. Pengoperasian dari UPS ini dibagai menjadi :

a. Normal mode

Pada mode ini, beban disuplai oleh sumber AC dari PLN. Pada saat ini juga baterai mengalami charge atau pengisian energi listrik melalui inverter *bidirectional*.

b. *Back Up / Stored Energy* mode

Ketika tegangan AC pada input UPS diluar spesifikasi tegangan yang diperbolehkan, tegangan DC pada baterai akan menggantikan sebagai penyuplai daya pada beban dengan diubah menjadi tegangan AC oleh inverter. Pada mode ini *switch* pada input akan open sehingga arus listrik tidak akan mengalir ke sumber PLN. Pergantian *switch* dari normal mode ke *back up mode* seolah-olah tidak terputus sehingga hampir tidak ada waktu *switching*.

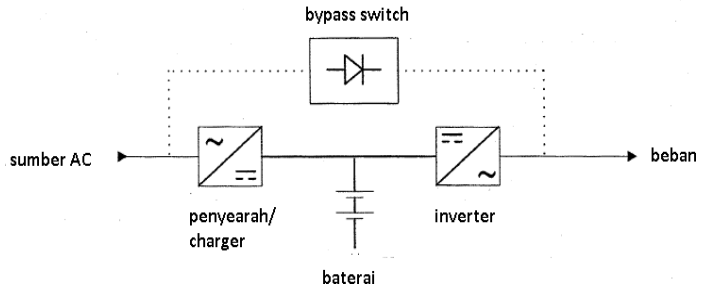
UPS jenis ini mempunyai beberapa kelebihan seperti regulator tegangan yang lebih baik dari pada konvensional UPS, menyuplai tegangan pada beban dengan tanpa waktu tunda saat terjadi gangguan, mempunyai kemampuan untuk mereduksi harmonisa dengan berfungsi sebagai filter aktif. Kekurangannya adalah biayanya yang relatif lebih mahal dari pada konvensional, dan memerlukan algoritma kontrol yang kompleks.

3. *Double Conversion* (*On-Line*)

Prinsip dasar dari *Double Conversion* (*On-Line*) UPS juga hampir sama dengan *Off-Line/standby* UPS dan *Line-Interactive* UPS tetapi dengan biaya pembuatan yang lebih mahal dengan adanya *rectifier*/*charger* AC-ke-DC yang lebih baik dan inverter yang bekerja terus menerus tanpa adanya waktu tunda (*switching*) dengan system pendingin yang lebih baik.

On-line UPS secara kontinyu menyuplai daya pada beban

melalui *rectifier* dan inverter baik pada saat normal mode maupun keadaan gangguan pada sumber PLN sehingga pada UPS jenis ini ada atau tidak ada gangguan akan mengalami dua proses konversi. Ketika terjadi gangguan, energi pada baterai melalui inverter akan menggantikan peran sumber utama untuk memberi daya pada beban. Dapat dikatakan pula bahwa UPS ini memberikan sistem proteksi pada beban secara kontinyu ketika sumber PLN mengalami perubahan tegangan. UPS ini memiliki performa yang paling baik dari pada jenis UPS yang lain, tetapi biaya pembuatannya paling besar diantara yang lainnya. Gambar 2.12 menunjukkan rangkaian dari *On-Line* UPS.



Gambar 2. 11 Blok Rangkaian *On Line* UPS

Komponen-komponen dasar penyusun UPS terdiri atas 3 komponen utama yaitu :

1. *Rectifier*, yang berfungsi sebagai penyearah tegangan bolak-balik (ac) dari sumber utama yang nantinya akan digunakan untuk pengisian baterai. *Rectifier* yang digunakan adalah penyearah jembatan tiga phasa.
2. Baterai, yang berfungsi sebagai cadangan energi listrik jika supplai listrik utama mengalami gangguan.

3. Inverter, yang berfungsi sebagai pengubah tegangan searah (DC) yang berasal dari baterai menjadi tegangan bolak-balik (AC) untuk menyuplai tegangan pada beban. Inverter yang digunakan adalah inverter tiga phasa Selain ketiga komponen dasar tersebut, memungkinkan terdapat juga komponen-komponen lain yang digunakan seperti *switch*, induktor, AVR, filter, DC-DC konverter dan lain-lain yang penggunaannya tergantung sesuai dengan topologi masing-masing UPS.

2.7 RS-232

RS-232 adalah standatr komunikasi serial perangkat terminal data adalah komputer dan perangkat komunikasi data adalah modem walaupun pada kenyataannya tidak semua produk antar muka adalah perangkat komunikasi data. Komunikasi RS-232 diperkenalkan pada tahun 1962 dan pada tahun 1997, *Electronic Industries Association* mempublikasikan tiga modifikasi pada standar RS-232 dan menamainya menjadi EIA-232.

Standar RS-232 mendefinisikan kecepatan 256 kbps atau lebih rendah dengan jarak kurang dari 15 meter, namun belakangan ini sering ditemukan jalur kecepatan tinggi pada komputer pribadi dan dengan kabel berkualitas tinggi, jarak maksimum juga ditingkatkan secara signifikan. Dengan susunan pin khusus yang disebut null *modem cable*, standar RS232 dapat juga digunakan untuk komunikasi data antara dua komputer secara langsung.

Pada tesis ini komunikasi serial dibutuhkan sebagai komunikasi antara modem dengan mikrokontroler. Untuk dapat berkomunikasi dengan mikrokontroler

dibutuhkan sebuah *serial conveter driver* yang dibuat menggunakan IC MAX232. IC MAX232 berfungsi untuk mengubah level tegangan TTL ke RS232 atau sebaliknya.

2.8 *Message Queuing Telemetry Transport* (MQTT)

Message Queuing Telemetry Transport (MQTT) adalah protokol komunikasi ringan yang dirancang untuk pengiriman data secara efisien antara perangkat IoT, khususnya di lingkungan dengan sumber daya terbatas dan jaringan yang memiliki bandwidth rendah. MQTT sangat cocok digunakan dalam aplikasi pengawasan, termasuk pada ATM, karena protokol ini mengutamakan efisiensi dalam penggunaan sumber daya dan kecepatan dalam pengiriman data.

Menurut Rivard et al. (2019), MQTT bekerja dengan cara mengirimkan pesan-pesan kecil yang terstruktur melalui server perantara yang dikenal sebagai broker. Broker bertanggung jawab untuk mengarahkan pesan dari pengirim ke penerima yang terhubung ke sistem pengawasan. Dalam konteks ATM, perangkat seperti kamera pengenal wajah atau sensor gerak akan mengirimkan data ke *server* pusat menggunakan MQTT. Data yang dikirimkan dapat mencakup gambar atau rekaman video dari kejadian di sekitar ATM, yang kemudian diproses secara otomatis untuk mendeteksi potensi ancaman atau kejadian yang mencurigakan.

Keuntungan utama dari penggunaan MQTT dalam sistem pengawasan berbasis IoT adalah kemampuannya untuk beroperasi dengan sumber daya terbatas dan mengirimkan data secara *real-time*. Hal ini memungkinkan petugas keamanan

untuk segera menanggapi ancaman atau kejadian yang terdeteksi oleh sensor atau kamera di ATM.

2.9 *Automated Teller Machine* (ATM)

ATM (*Automated Teller Machine*) menurut Ellen Florian (2004) adalah sebuah alat elektronik yang memudahkan nasabah perbankan untuk mengambil uang dan mengecek rekening tabungan nasabah tanpa perlu dilayani oleh seorang "*teller*" di Bank. Sementara itu defenisi ATM menurut Kasmir (2007:327) ATM merupakan mesin yang memberikan kemudahan kepada nasabah dalam melakukan transaksi perbankan secara otomatis selama 24 jam dalam 7 hari termasuk hari libur. ATM juga berfungsi untuk melakukan penyetoran uang atau pengecekan nominal rekening, transfer uang dan transaksi perbankan lainnya. EDC (*Electronic Data Capture*) adalah mesin yang dapat digunakan oleh nasabah perbankan sebagai alat pembayaran elektronik (mesin gesek kartu ATM baik Debit ataupun *Credit Card*). Mesin EDC menggunakan teknologi *wireless* (GSM) dan *fixed line* (line telepon). Alat ini akan terhubung secara online dengan sistem jaringan bank.

1. Fungsi dan Mafaat ATM

   Secara umum fungsi ATM adalah agar untuk melakukan penarikan uang secara tunai, selain itu masih banyak fungsi ATM yang dapat mempermudah kepentingan nasabah untuk melakukan aktivitas perbankan, seperti:

   a. Informasi Saldo
   b. Pembayaran Umum: tagihan telepon, kartu kredit, listrik, air, handphone, dan uang kuliah

c. Pembelian: tiket penerbangan, isi ulang pulsa
d. Pemindah bukuan (open transfer)
e. Pengubahan PIN

2. Penempatan atau Lokasi ATM Mesin ATM sering ditempatkan di lokasi-lokasi strategis, seperti restoran, pusat perbelanjaan, bandar udara, stasiun kereta api, terminal bus, pasar tradisional, kampus, dan kantor-kantor bank itu sendiri.
3. Bank Penyedia Mesin ATM Bank di Indonesia berjumlah lebih dari limapuluh yang dikelompokkan menjadi enam kategori yaitu bank persero, bank devisa, bank non devisa, BPD, Bank campuran, dan Bank asing. Tidak semua bank di Indonesia menyediakan mesin ATM, namun ada beberapa bank yang memberikan pelayanan bagi nasabahnya dengan menyediakan mesin ATM dibeberapa tempat atau lokasi strategis disetiap sudut kota, antara lain yaitu BCA, BNI, BRI, BTN/Bank Jateng, Mandiri, CIMB Niaga, BPD, Danamon.ngan nasabah untuk melakukan aktivitas perbankan, seperti: a. Informasi Saldo

2.10*Internet Of Things* (IOT)

Internet of Thing (IoT) merupakan sebuah jaringan yang terhubung dengan benda-benda fisik yang dilengkapi dengan sensor untuk memindahkan data melalui koneksi jaringan yang memungkinkan saling bertukar data dan tanpa memerlukan interaksi manusia secara langsung (Fadly, et al., 2021). Jaringan luas teknologi *Internet of Things* (IoT) merambah berbagai bidang, dari industri, kesehatan, hingga ke dalam rumah. Konsep IoT ini menghubungkan perangkat pintar, jaringan

komputer, dan lingkungan fisik di sekitarnya. Beragam data dari bendabenda yang terhubung internet ini diolah menjadi *big data* yang bernilai bagi berbagai lembaga, perusahaan, dan instansi pemerintahabn untuk memenuhi kebutuhan mereka. Perangkat seperti ponsel, komputer, dan tablet yang berfungsi untuk alat komunikasi elektronik untuk menghubungkan individu atau kelompok, tergolong sebagai *hardware* dan *software* yang termasuk dalam *Internet of Things* (IoT) (Hermawan 2023).

IoT beroperasi dengan menggunakan logika pemrograman, di mana setiap perintah memicu interaksi antar mesin secara otomatis tanpa campur tangan manusia dan tanpa batasan jarak. Mesin saling berinteraksi melalui internet, sedangkan manusia berfungsi sebagai pengatur dan pengawas langsung operasi alat tersebut. (Heru Sandi and Fatma 2023).

Menurut Hermawan (2023), IoT memiliki beberapa keuntungan, antara lain:

1. Informasi dapat dijangkau di mana saja, oleh siapa saja, dan menggunakan perangkat apa pun.;
2. Meningkatkan hubungan antar perangkat elektronik melalui jaringan;
3. IoT memungkinkan pengiriman data lebih hemat dan optimal melalui jaringan;
4. Meminimalkan intervensi manusia dan mendongkrak produktivitas melalui otomatisasi tugas-tugas yang berkaitan dengan kualitas layanan bisnis.

Selain itu, IoT juga memiliki beberapa keterbatasan, yaitu:

1. Meningkatnya jumlah perangkat yang terhubung ke internet dan pertukaran data antar perangkat, membuka peluang bagi pihak-pihak yang tidak bertanggung jawab untuk mencuri data sensitif. Semakin banyak data yang beredar, semakin tinggi pula risikonya;
2. Di masa depan, organisasi dihadapkan dengan kemungkinan untuk mengelola ribuan atau bahkan jutaan perangkat IoT. Hal ini akan menimbulkan tantangan dalam mengumpulkan dan mengelola data yang berasal dari berbagai sumber yang beragam;
3. Setiap perangkat yang terhubung ke jaringan internet berisiko mengalami kerusakan jika terdapat bug atau kesalahan dalam sistem perangkat tersebut;
4. Kurangnya standar kompatibilitas internasional dapat menyebabkan kesulitan bagi perangkat dari berbagai produsen untuk berkomunikasi satu sama lain melalui IoT.

Di tahap awal, perangkat IoT dapat mengenali identitasnya sendiri dan memantau lingkungan sekitarnya, seperti lokasi, cuaca, pergerakan mesin, kondisi kesehatan, dan lainnya.

2.11 Efisiensi Sistem Pengawasan *Closed Circuit Television* (CCTV)

Efisiensi sistem pengawasan Closed Circuit Television (CCTV) pada *Automated Teller Machine* (ATM) sangat penting untuk meningkatkan kualitas dan responsivitas pengawasan tanpa mengorbankan penggunaan sumber daya yang berlebihan. Efisiensi ini dapat dilihat dari beberapa aspek utama, yaitu pengelolaan data, waktu respon, kualitas pengawasan, dan pemanfaatan sumber daya. Dalam hal

ini, sistem CCTV yang efisien tidak hanya mengoptimalkan perangkat keras dan perangkat lunak, tetapi juga memastikan bahwa pengawasan dapat berjalan dengan efektif tanpa menambah beban yang terlalu berat pada jaringan atau perangkat yang digunakan.

Menurut Zhao et al. (2020)**,** sistem pengawasan CCTV yang efisien harus mampu mengelola rekaman secara otomatis dan menyimpannya dalam format yang mudah diakses. Hal ini meminimalisir waktu yang dibutuhkan untuk mengakses rekaman ketika terjadi insiden, serta memungkinkan sistem untuk bekerja lebih cepat dan lebih efisien. Sistem pengelolaan data otomatis seperti penghapusan rekaman lama yang tidak diperlukan atau pengarsipan data penting ke penyimpanan yang lebih aman dapat membantu menjaga efisiensi operasional sistem CCTV.

Salah satu aspek efisiensi sistem CCTV yang perlu diperhatikan adalah pengiriman data yang cepat dan efisien. Penggunaan protokol komunikasi ringan, seperti MQTT (*Message Queuing Telemetry Transport*), memungkinkan pengiriman data dengan kecepatan tinggi dan konsumsi bandwidth yang rendah. Dalam sistem pengawasan berbasis IoT, protokol MQTT sangat efektif untuk mengirimkan data dalam jumlah besar secara *real-time* dengan latensi rendah, yang sangat penting untuk memastikan respon yang cepat terhadap insiden.

Menurut Lin et al. (2020), implementasi protokol MQTT pada sistem CCTV berbasis IoT memungkinkan perangkat untuk mengirimkan data yang relevan (seperti video atau gambar) langsung ke server atau pusat pengawasan dalam waktu nyata, meminimalkan waktu tunda dan mengurangi risiko kehilangan data.

2.12 Mikrokontroler

Mikrokontroler merupakan *suatu Integrated Circuit* (IC) yang di dalamnya berisi *Central Processing Unit* (CPU), *Read Only Memory* (ROM), *Random Access Memory* (RAM), dan Input/Output. Mikrokontroler dapat melakukan proses berfikir berdasarkan program yang telah dimasukkan, hal ini dikarenakan sudah tertanam di dalamnya berupa CPU. Mikrokontroler banyak terdapat pada peralatan elektronik yang serba otomatis. Mikrokontroler dapat disebut sebagai komputer yang berukuran kecil yang rendah sehingga sebuah baterai dapat memberikan daya (Putra et al., 2017).

Salah satu mikrokontroler keluarga AVR 8 bit adalah ATMega328. ATMega328 adalah mikrokontroler keluaran dari Atmel yang mempunyai arsitektur *Reduce Instruction Set Computer* (RISC) yang dimana setiap proses eksekusi data lebih cepat dari pada arsitektur *Completed Instruction Set Computer* (CISC). Mikrokontroler ATmega328 memiliki arsitektur Harvard yaitu memisahkan memori untuk kode program dan memori untuk data sehingga dapat memaksimalkan kerja (Paramarta et al., 2016).

Mikrokontroler dapat disimpulkan yaitu suatu alat elektronika digital yang mempunyai masukan, keluaran serta sistem kendali dengan suatu program yang bisa ditulis dan dihapus seperti membaca dan menulis data.

Beberapa tipe mikrokontroler yang sama dengan ATMega8 ini yaitu ATMega8535, ATMega16, ATMega32, ATMega328. Pembeda antara mikrokontroler yang satu dengan yang lain adalah ukuran memori, banyaknya GPIO (pin *input/output*), peripheral (USART, *timer, counter* dan lain-lain). Dilihat

dari ukuran fisik, ATMega328 memiliki ukuran fisik lebih kecil dibandingkan dengan beberapa mikrokontroler diatas. Namun untuk segi memori dan *peripheral* lainnya ATMega328 tidak kalah dengan yang lainnya karena ukuran memori dan *peripheralnya* relatif sama dengan ATMega8535, ATMega32 hanya saja jumlah GPIO lebih sedikit dibandingkan mikrokontroler lainnya (Astuti & Fauzi, 2018).

(Putra et al., 2017) Menjelaskan bahwa mikrokontroler standar memiliki komponen - komponen sebagai berikut:

1. *Central Processing Unit* merupakan bagian utama dalam suatu mikrokontroler. CPU pada mikrokontroler ada yang berukuran 8 bit dan ada yang berukuran 16 bit. CPU ini membaca program yang tersimpan di dalam ROM dan melaksanakannya.
2. *Read Only Memory* merupakan suatu memori yang sifatnya hanya dibaca saja, ROM tidak dapat ditulisi. Dalam dunia mikrokontroler ROM digunakan untuk menyimpan program bagi mikrokontroler tersebut. Program tersimpan dalm format biner („0“ atau „1“). Susunan bilangan biner tersebut bila telah terbaca oleh mikrokontroler memiliki arti tersendiri.
3. *Random Access Memory* merupakan jenis memori selain dapat dibaca juga dapat ditulis berulang kali. Pemakaian mikrokontroler ada semacam data yang bisa berubah pada saat mikrokontroler tersebut bekerja. Perubahan data tersebut akan tersimpan ke dalam memori. Isi pada RAM akan hilang jika catu daya listrik hilang.

4. *Input/Output* (I/O) digunakan untuk berkomunikasi dengan dunia luar, mikrokontroler menggunakan terminal I/O yang digunakan untuk masukan atau keluaran.
5. Beberapa mikrokontroler memiliki timer atau counter, *Analog to Digital Converter* (ADC), dan komponen lainnya. Pemilihan komponen tambahan yang sesuai dengan tugas mikrokontroler akan sangat membantu perancangan sehingga dapat mempertahankan ukuran yang kecil. Apabila komponen komponen tersebut belum ada pada suatu mikrokontroler, umumnya komponen tersebut masih dapat ditambahkan pada sistem mikrokontroler melalui port-portnya.

Kehadiran mikrokontroler membuat kontrol elektrik dalam berbagai proses menjadi lebih praktis dan ekonomis. Produk dan alat yang dikendalikan secara otomatis menggunakan mikrokontroler yaitu sistem kontrol mesin, peralatan rumah tangga, mesin kantor, alat berat, mainan dan masih banyak lagi. Dengan adanya mikrokontroler akan sangat membantu dalam hal mengurangi biaya, ukuran dan konsumsi tenaga dibandingkan dengan menggunakan mikroprosesor memori dan alat masuk keluar yang terpisah.

2.13 ESP32

ESP32 adalah mikrokontroler yang dikenalkan oleh Espressif System merupakan penerus dari mikrokontroler ESP8266. Pada mikrokontroler ini sudah tersedia modul WiFi dalam chip sehingga sangat mendukung untuk membuat sistem aplikasi *Internet of Things*. Untuk spesifiasi dari ESP32 dapat dilihat pada gambar 2.3 dan pada gambar 2.4 merupakan pinout dari ESP32. Pin tersebut dapat

dijadikan input atau output untuk menyalakan LCD, lampu, bahkan untuk menggerakan motor DC (Aulia, 2021).

Spesifikasi modul ESP32-WROOM-32 :

1. Microprosesor Xtensa Dual-Core 32 Bit LX6
2. Freq Clock up to 240 MHz
3. SRAM 520 kB
4. Flash memori MB
5. 11b/g/n WiFi transceiver
6. Bluetooth 4.2/BLE
7. 48 pin GPIO
8. 15 pin channel ADC (*Analog to Digital Converter*)
9. 25 pin PWM (*Pulse Width Modulation*)
10. 2 pin channel DAC (*Digital to Analog Converter*)

ESP32 Dev Kit V1 adalah sebuah board pengembangan (*development board*) yang didukung oleh mikrokontroler Tensilica 32-bit Single-/Dual-core CPU Xtensa LX6 dengan kecepatan clock 240 Mhz. Board ini dilengkapi dengan 520 KiB SRAM dan 4 MB flash memory untuk menyimpan program dan data. Board ini juga memiliki 25 digital input/output (DIO) pins, 6 analog input (ADC) pin, dan 2 analog output (DAC) pin yang dapat digunakan untuk berbagai keperluan seperti mengendalikan perangkat elektronik atau membaca sensor. Selain itu, ESP32 Dev Kit V1 juga dilengkapi dengan 3 UARTs, 2 SPIs, dan 3 I2Cs, yang memungkinkan board ini untuk berkomunikasi dengan perangkat lain secara serial atau menggunakan protokol komunikasi seperti SPI dan I2C. Board ini juga dilengkapi

dengan Wi-Fi yang mendukung standar IEEE 802.11 b/g/n/e/, sehingga board ini dapat terhubung ke jaringan Wi-Fi dan berkomunikasi dengan perangkat lain melalui jaringan tersebut. Dengan ukuran 51.5x29x5mm, board ini cukup kecil dan mudah untuk diintegrasikan ke dalam proyek-proyek yang lebih kompleks. Keseluruhan, ESP32 Dev Kit V1 adalah board pengembangan yang kuat dan serbaguna, yang cocok untuk berbagai aplikasi *Internet of Things* (IoT) atau proyekproyek elektronika yang membutuhkan konektivitas Wi-Fi.

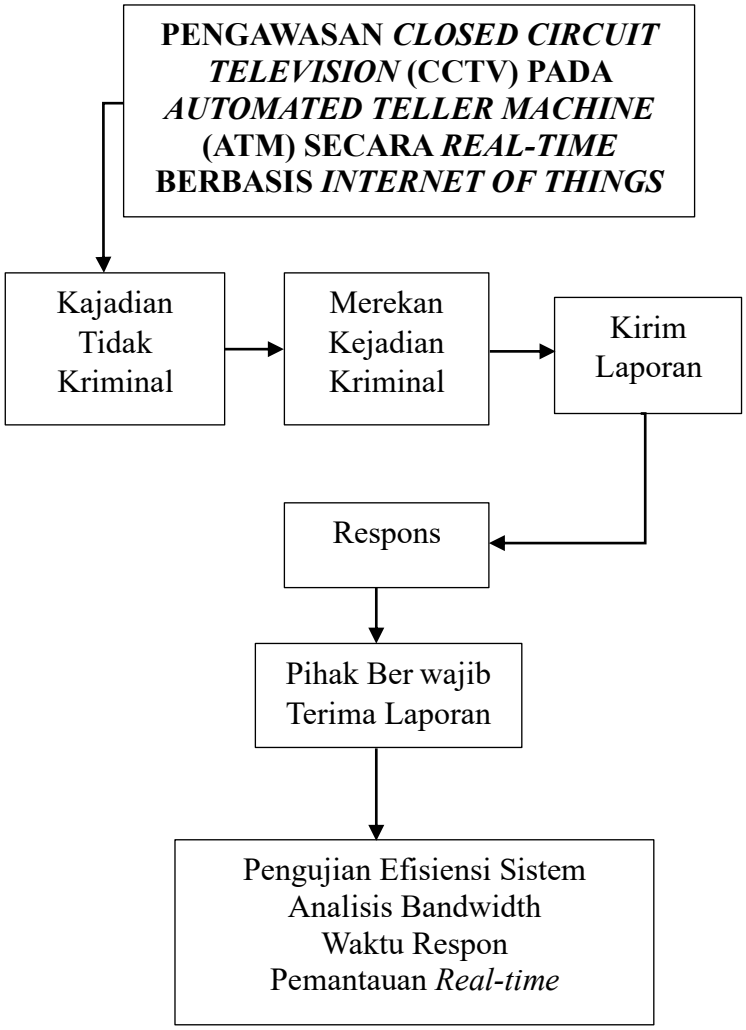
2.14Kerangka Teori

Penelitian dengan topik dirangkum dalam sistem pengawasan *closed circuit television* (CCTV) pada *automated teller machine* (ATM) secara *real-time* berbasis *internet of things* (IOT) dirangkum dalam 3 parameter yaitu dataset, proses dan output ditunjukkan dalam Tabel 2.1.

Tabel. 2.3 Literatur Review

Input	Proses	Output	Jurnal
Kamera CCTV + Modul IoT (ESP32)	Perekaman video	Tampilan video dan aktivitas di sekitar ATM	Zhang et al., 2022; Putra et al., 2021
Modul IoT	Transmisi data video real-time	Akses monitoring secara real-time melalui dashboard	Yusuf et al., 2023
Mikrokontroler + Kamera + Sensor	Kompresi dan enkripsi data video	Efisiensi bandwidth dan keamanan transmisi	Dharmawan et al., 2021
Kamera + FSA (Finite State Automata)	Transisi status	Respons cepat berdasarkan status sistem	Hussain et al., 2019; Santoso et al., 2018
Dashboard pengawasan	Tampilan video real-time, log, dan notifikasi	Monitoring terpusat, laporan insiden	Putra et al., 2021; Zhang et al., 2022
Penyimpanan cloud/local	Logging & backup data video	Rekaman arsip untuk audit keamanan	Yusuf et al., 2023; Dharmawan et al., 2021

2.15 Kerangka Konsep Penelitian



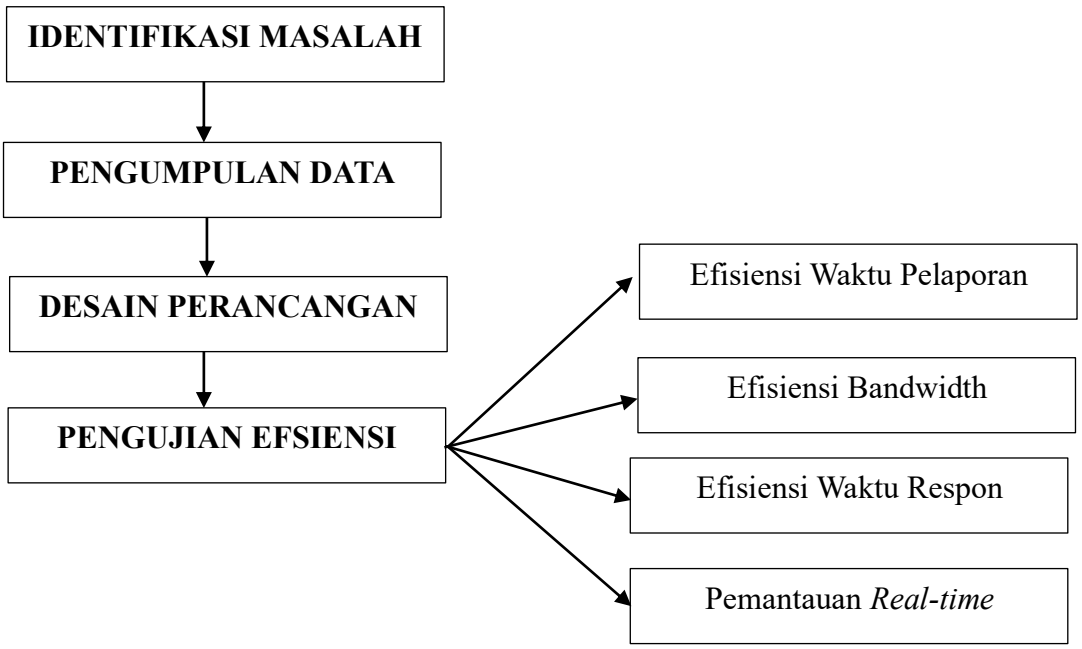
Gambar 2. 12 Kerangka Konsep Penelitian

BAB III

METODOLOGI PENELITIAN

Dalam penelitian ini, pengambilan data dilakukan melalui beberapa metode yang bertujuan untuk mendapatkan informasi terkait sistem pengawasan *Closed Circuit Television* (CCTV) berbasis *Internet of Things* (IoT) pada *Automated Teller Machine* (ATM) secara *real-time*.

Penelitian ini termasuk dalam kategori penelitian eksperimen kuantitatif ngan pendekatan sistem berbasis automata, khususnya menggunakan *Finite State Automata* (FSA). Pendekatan ini digunakan untuk memodelkan proses kerja sistem pengawasan CCTV dari status siaga hingga pelaporan kejadian dan respons keamanan. Dengan pendekatan ini, sistem dapat diuji secara sistematis dalam hal efisiensi waktu, bandwidth, dan efektivitas pemantauan.



Gambar 3. 1 Metode Penelitian

3.1 Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan untuk mendapatkan informasi langsung dari sumber yang relevan mengenai sistem pengawasan *Closed Circuit Television* (CCTV) berbasis *Internet of Things* (IoT) pada *Automated Teller Machine* (ATM) secara *real-time*. Data primer diperoleh melalui beberapa metode berikut:

1. Observasi Lapangan

   Observasi dilakukan dengan mengunjungi lokasi ATM yang telah dilengkapi dengan sistem CCTV dan UPS guna memahami kondisi nyata dalam pengawasan dan pemeliharaan sistem tersebut. Aspek yang diamati meliputi:

   a. Pola penggunaan CCTV untuk memantau keamanan ATM.
   b. Keandalan UPS dalam menjaga pasokan daya cadangan saat terjadi pemadaman listrik.
   c. Identifikasi potensi ancaman seperti pencurian, perusakan, atau serangan siber terhadap sistem ATM.
   d. Evaluasi sistem pemantauan konvensional, termasuk keterbatasan dalam respons waktu nyata.

2. Eksperimen Sistem (Uji Teknis)

   Eksperimen dilakukan secara langsung dengan menguji sistem yang telah dirakit dan dikonfigurasi untuk memantau aktivitas di area ATM secara *real-time*, meliputi:

a. Uji kamera: Menyalakan CCTV dan memantau tangkapan video secara langsung.
b. Uji koneksi IoT: Memastikan ESP32-CAM atau IP Camera dapat mengirim data ke MQTT Broker.
c. Uji dashboard monitoring: Melihat data yang dikirim dari perangkat ditampilkan secara *real-time*.
d. Simulasi kejadian: Menciptakan aktivitas mencurigakan (gerakan mendekati ATM) untuk melihat apakah sistem memberikan notifikasi otomatis.

3. Dokumentasi Pengujian

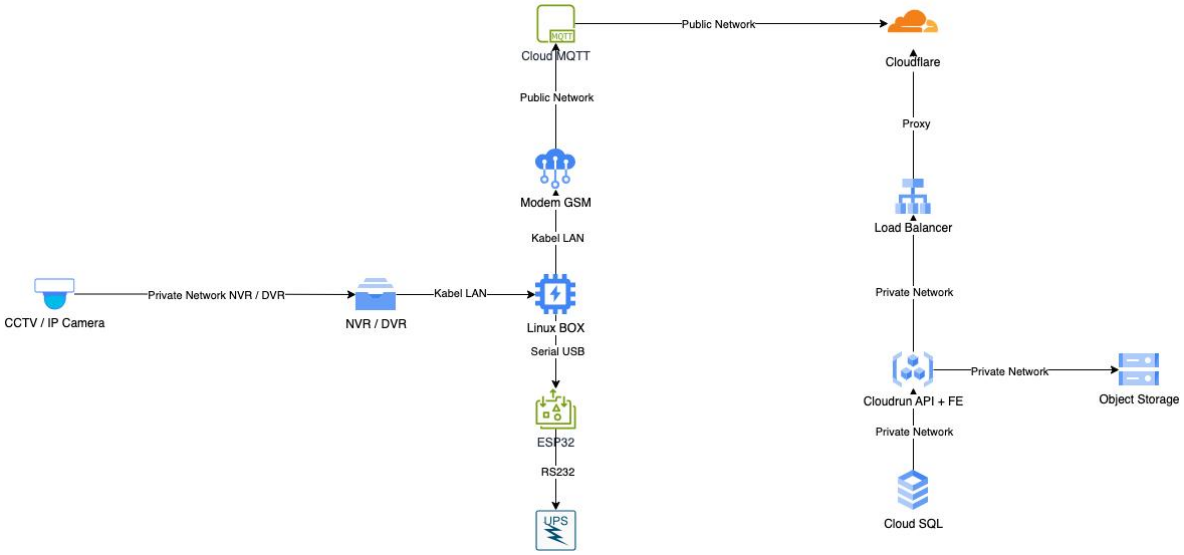
Eksperimen dilakukan dengan mengembangkan dan menguji sistem CCTV untuk memastikan efektivitasnya dalam pemantauan ATM secara *real-time*, meliputi:

a. Lembar observasi teknis: berisi catatan waktu, kejadian, tanggapan sistem, dan hasil.
b. Log file sistem: mencatat aktivitas data dari perangkat ke server (misalnya dari MQTT ke dashboard).
c. Screenshot atau screen recording: untuk menunjukkan bukti hasil tampilan monitoring dan rekaman video.
d. File rekaman video: hasil tangkapan kamera ketika kejadian uji berlangsung.
e. Data uji akurasi: berupa tabel yang memuat jumlah kejadian yang terdeteksi dan tidak terdeteksi oleh sistem.

3.2 Desain Perancangan

Penelitian ini termasuk dalam kategori penelitian eksperimen kuantitatif ngan pendekatan sistem berbasis automata, khususnya menggunakan *Finite State Automata* (FSA). Pendekatan ini digunakan untuk memodelkan proses kerja sistem pengawasan CCTV dari status siaga hingga pelaporan kejadian dan respons keamanan. Dengan pendekatan ini, sistem dapat diuji secara sistematis dalam hal efisiensi waktu, bandwidth, dan efektivitas pemantauan.

1. Desain dan Perancangan



Gambar 3. 2 Desain dan Perancangan

CCTV/IP Camera menangkap rekaman video dan mengirimkannya ke NVR/DVR melalui jaringan pribadi (*Private Network*). Dari NVR/DVR, data dikirim melalui kabel LAN ke *Linux BOX*, yang bertindak sebagai server penghubung antara perangkat IoT dan sistem *cloud*. Sementara itu, UPS yang berfungsi sebagai cadangan daya dikendalikan oleh ESP32, yang menerima data melalui RS232. ESP32

kemudian mengirimkan informasi status UPS ke *Linux BOX* melalui koneksi serial USB.

Untuk konektivitas ke *cloud*, sistem menggunakan modem GSM yang menghubungkan Linux BOX ke *Cloud MQTT* melalui jaringan publik. Data yang dikirim ke *Cloud MQTT* kemudian diteruskan ke *Cloudflare*, yang berfungsi sebagai *proxy* untuk mengamankan lalu lintas data sebelum diteruskan ke *Load Balancer*. *Load Balancer* mendistribusikan permintaan ke *Cloudrun API* + *Frontend* (FE) yang menangani antarmuka pengguna dan pengolahan data.

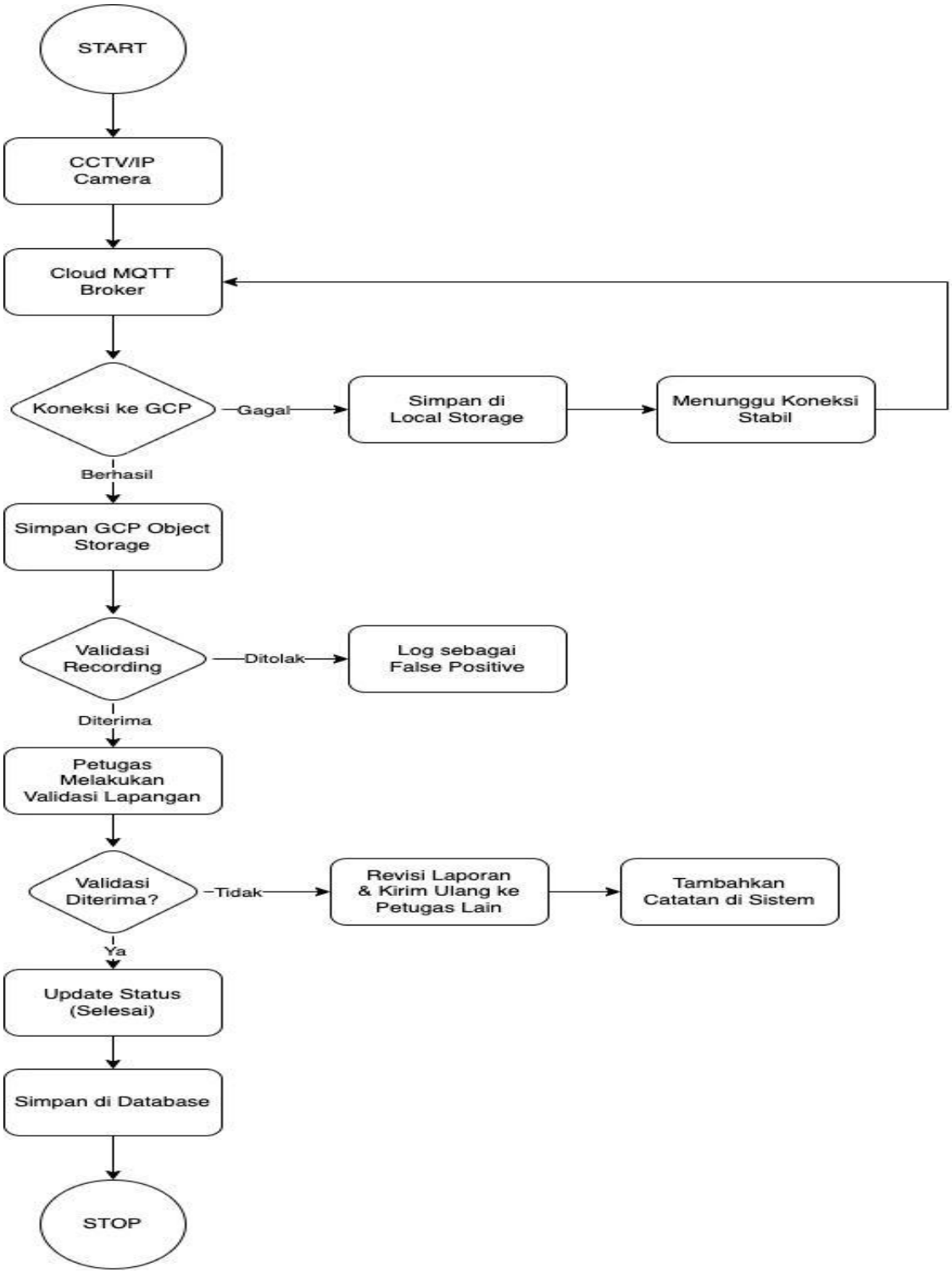
Rekaman CCTV dan status UPS disimpan dalam *Cloud SQL* untuk *database* dan *Object Storage* untuk penyimpanan video. Administrator dapat memantau kondisi ATM secara *real-time* melalui dashboard berbasis *cloud*. Jika terjadi gangguan daya atau aktivitas mencurigakan, sistem akan mengirimkan notifikasi otomatis agar tindakan cepat dapat diambil.

Secara keseluruhan, sistem ini mengintegrasikan CCTV, UPS, dan IoT untuk meningkatkan keamanan ATM dengan pemantauan yang lebih efisien, pencatatan data yang aman, serta kemampuan respons yang lebih cepat terhadap potensi risiko.

2. *Flowchart*

Flowchart adalah representasi fisual dari alur logika atau proses dalam bentuk diagram. Flowchart digunakan untuk menggambarkan

urutan. Langkah-langkah atau keputusan yang diambil dalam suatu algoritma atau prosedur.



Gambar 3. 3 *Flowchart*

3.3 Pengujian Efsiensi

Pengujian efisiensi dilakukan untuk mengevaluasi sejauh mana penerapan sistem CCTV berbasis IoT yang memanfaatkan protokol MQTT dapat meningkatkan kecepatan pelaporan, menghemat bandwidth, dan mempercepat respon terhadap tindakan kriminal yang terjadi di lingkungan ATM.

1. Efisiensi Waktu Pelaporan

   Pengujian ini bertujuan untuk mengukur perbedaan waktu yang dibutuhkan untuk melaporkan tindakan kriminal antara sistem konvensional (manual) dan sistem berbasis IoT menggunakan MQTT. Dalam sistem konvensional, pelaporan sering kali harus menunggu proses manual seperti rekaman ditarik dari DVR dan dilaporkan oleh petugas di lokasi. Sedangkan pada sistem IoT, notifikasi dan data visual dikirim secara otomatis dan *real-time* ke perangkat petugas keamanan.

   $$Efisiensi\ Waktu = \frac{Wsebelum - Wsesudah}{Wsebelum} x100\%$$

   Keterangan

   Wsebelum = rata-rata waktu pelaporan sebelum sistem IoT diterapkan

   Wsesudah = rata-rata waktu pelaporan setelah sistem IoT diterapkan.

2. Efisiensi Bandwidth

   Pengujian ini bertujuan untuk mengetahui efisiensi penggunaan jaringan data antara sistem CCTV konvensional (streaming terus menerus) dengan sistem berbasis MQTT (mengirim data hanya saat ada aktivitas).

$$Efisiensi\ Bandwidth = \frac{Blama - BMQTT}{Blama} x100\%$$

Keterangan

Blama = rata-rata bandwidth pada sistem CCTV konvensional (streaming)

BMQTT = rata-rata bandwidth setelah sistem MQTT diterapkan (*event-based*).

3. Efisiensi Waktu Respon

Waktu respon diartikan sebagai selang waktu antara kejadian kriminal terdeteksi oleh CCTV hingga tindakan atau notifikasi diterima oleh pusat keamanan. Pada sistem konvensional, waktu respon cenderung lebih lambat karena proses pemantauan bersifat manual dan tidak terhubung secara *real-time*. Sebaliknya, sistem IoT dengan protokol MQTT memungkinkan pengiriman notifikasi otomatis dan instan hanya ketika terjadi aktivitas, sehingga mempercepat waktu respon secara signifikan.

$$Efisiensi\ Waktu\ Respon = \frac{Rkonvensional - RIoT}{Rkonvensional} x100\%$$

Keterangan:

$R_{konvensional}$ = Rata-rata waktu respon pada sistem CCTV konvensional

RioT = Rata-rata waktu respon setelah sistem IoT + MQTT diterapkan

4. Pemantauan *Real-time*

Keberhasilan pemantauan *real-time* menunjukkan kemampuan sistem dalam mendeteksi dan melaporkan kejadian secara langsung (tanpa delay) kepada pihak yang berwenang, seperti pusat keamanan atau petugas. Pada sistem konvensional, proses pemantauan memerlukan waktu lebih lama karena bergantung pada rekaman video yang harus dicek secara manual oleh petugas. Sementara itu, sistem IoT + MQTT memberikan pemantauan secara langsung jika ada kejadian tertentu yang terjadi.

$$Keberhasilan\ (\%) = \frac{Kejadian}{Total\ Kejadian} x100\%$$

Keterangan:

Kejadian : Jumlah kejadian yang berhasil terdeteksi oleh sistem pengawasan.

Total Kejadian: Jumlah seluruh kejadian yang terjadi selama pengujian.

3.4 Alat dan Bahan Penelitian

Penelitian ini menggunakan perangkat keras dan perangkat lunak berikut:

1. Perangkat Keras
   a. CCTV / IP Camera untuk pemantauan visual berbasis jaringan.
   b. NVR / DVR untuk penyimpanan rekaman video.
   c. *Linux BOX* (*Single Board Computer*, seperti *Raspberry Pi* atau *Jetson Nano*) sebagai *gateway* utama sistem.

d. Modem GSM / Wi-Fi untuk koneksi ke *cloud* melalui jaringan seluler atau Wi-Fi.
e. ESP32 dengan RS232 sebagai modul komunikasi antara *Linux BOX* dan UPS.
f. UPS (*Uninterruptible Power Supply*) dengan sensor pemantauan daya.

2. Perangkat Lunak
   a. Platform IoT untuk pemantauan data (misalnya *ThingsBoard*, *Blynk*, atau *MQTT*), serta sistem database untuk menyimpan log pemantauan.
   b. *Cloud MQTT* (*Mosquitto/HiveMQ/AWS IoT Core*) untuk komunikasi data antar perangkat.
   c. *Cloudflare* sebagai *proxy* dan perlindungan terhadap serangan siber.
   d. *Load Balancer* untuk distribusi lalu lintas jaringan dan peningkatan efisiensi sistem.
   e. *Cloudrun API* + FE (*Frontend* dan *Backend* berbasis *cloud*) untuk mengelola data pemantauan.
   f. *Cloud SQL* dan *Object Storage* untuk menyimpan data video dan status UPS.

3.5 Analisis Data

1. Analisis Keamanan Sistem Pengawasan CCTV Berbasis IoT

   Keamanan ATM menjadi perhatian utama dalam sistem ini, terutama dalam mendeteksi aktivitas mencurigakan, mencegah tindakan kriminal, dan meningkatkan respons keamanan. Data dianalisis berdasarkan parameter berikut:

a. Efektivitas Deteksi Ancaman Keamanan

1) Kecepatan sistem dalam mendeteksi pergerakan mencurigakan di sekitar ATM sebelum dan sesudah implementasi IoT.
2) Tingkat akurasi sistem dalam mengenali wajah dan objek mencurigakan menggunakan fitur computer vision dan machine learning jika diterapkan.
3) Jumlah insiden keamanan yang dapat dicegah sebelum terjadi tindak kriminalitas.
4) Tingkat *false positive* dan *false negative* dalam deteksi ancaman untuk mengetahui akurasi sistem.

b. Respon Keamanan Berbasis Notifikasi *Real-Time*

1) Kecepatan pengiriman peringatan ke pusat pemantauan setelah sistem mendeteksi anomali.
2) Keandalan sistem dalam mengirimkan notifikasi ke perangkat operator keamanan.
3) Efektivitas sistem dalam mendukung pengambilan keputusan cepat untuk mengatasi ancaman.

2. Analisis Keandalan UPS dalam Menjaga Operasional ATM

UPS berperan dalam menjaga ATM tetap beroperasi meskipun terjadi gangguan listrik. Analisis dilakukan dengan mempertimbangkan faktor berikut:

a. Ketahanan UPS terhadap Pemadaman Listrik

1) Durasi daya tahan UPS dalam mempertahankan fungsi ATM setelah terjadi pemadaman listrik.
2) Efisiensi daya UPS dalam mempertahankan operasional ATM sebelum sumber listrik utama kembali normal.

b. Integrasi IoT untuk Pemantauan UPS

1) Kinerja sensor daya berbasis IoT dalam memantau status baterai UPS secara *real-time*.
2) Efektivitas sistem notifikasi otomatis dalam memberikan peringatan dini ketika UPS mengalami gangguan daya atau kapasitas baterai berkurang.
3) Data historis konsumsi daya ATM sebelum dan sesudah implementasi UPS berbasis IoT.

3. Analisis Kinerja Sistem IoT dalam Pemantauan ATM Secara *Real-Time*

a. Kestabilan dan Kecepatan Koneksi IoT

1) Latensi dalam pengiriman data dari CCTV dan UPS ke server pusat.
2) Keandalan koneksi internet dalam memastikan sistem IoT bekerja tanpa gangguan.
3) Efektivitas redundansi data dalam mencegah kehilangan informasi saat sistem mengalami kendala.

b. Evaluasi Dashboard Pemantauan *Real-Time*

1) Tampilan dan fungsionalitas dashboard pemantauan berbasis IoT.

2) Kemudahan akses dan penggunaan dashboard bagi operator keamanan dan teknisi.
3) Efektivitas dashboard dalam menampilkan informasi krusial seperti status ATM, rekaman CCTV, dan status UPS.

4. Perbandingan Sebelum dan Sesudah Implementasi IoT
5. Analisis Hasil Pengujian Sistem Secara Keseluruhan

Berdasarkan analisis data yang diperoleh, penerapan sistem pengawasan CCTV dan UPS berbasis IoT pada ATM secara *real-time* memberikan peningkatan signifikan dalam aspek berikut:

a. Keamanan: Meningkatkan kecepatan deteksi dan respons terhadap ancaman keamanan.
b. Efisiensi Operasional: UPS dapat dipantau secara *real-time*, mengurangi risiko downtime ATM akibat pemadaman listrikk.
c. Pemantauan *real-time*: Dengan IoT, sistem dapat mengirimkan data secara langsung ke pusat pemantauan, memungkinkan tindakan cepat saat terjadi masalah.
d. Kinerja Sistem: Data menunjukkan peningkatan stabilitas koneksi, keandalan sistem, dan efektivitas dashboard pemantauan dalam mendukung pengawasan ATM.

6. Hubungan kajian teori, kerangka konsep dan metode penelitian

Penelitian ini termasuk dalam kategori eksperimen kuantitatif dengan pendekatan sistem berbasis automata, khususnya menggunakan *Finite State Automata* (FSA), untuk memodelkan proses kerja sistem

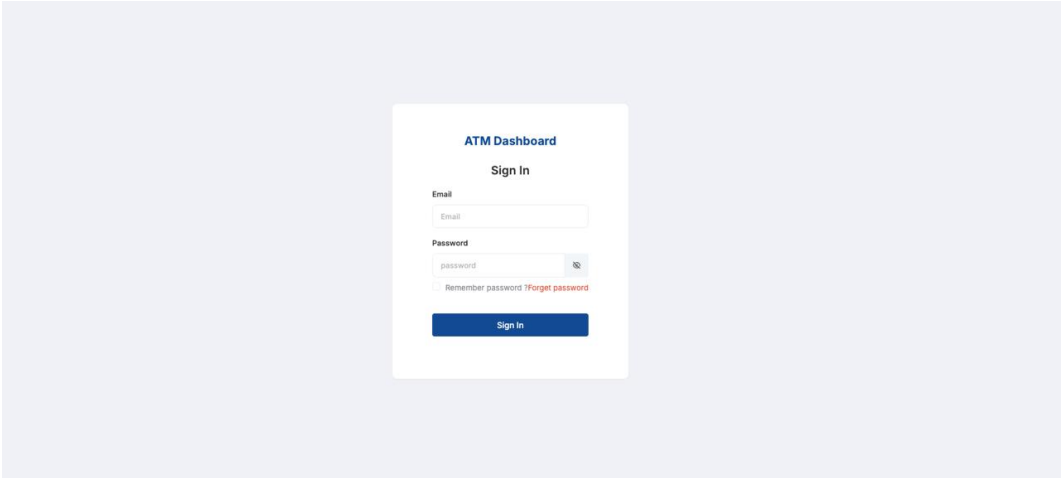
pengawasan *Closed Circuit Television* (CCTV) pada *Automated Teller Machine* (ATM) secara *real-time* berbasis *Internet of Things* (IoT). Pendekatan FSA digunakan untuk menggambarkan transisi sistem dari status siaga, merekam kejadian kriminal, mengirim laporan, hingga diterimanya laporan oleh pihak berwenang. Setiap proses tersebut dimodelkan sebagai suatu "state" dalam sistem automata, yang memungkinkan dilakukan pengujian terhadap waktu respons, efisiensi pemantauan, dan penggunaan bandwidth. Dalam kerangka konsep, sistem dimulai dari identifikasi kondisi apakah terjadi kejadian kriminal atau tidak. Jika tidak, sistem tetap dalam kondisi siaga; namun jika ada kejadian kriminal, maka CCTV merekam kejadian, mengirim laporan melalui jaringan IoT, dan sistem merespons hingga laporan diterima pihak berwenang. Dalam konteks ini, teori efisiensi sistem digunakan untuk menilai kinerja keseluruhan perangkat dalam merespons kejadian secara cepat dan tepat. Teori topologi jaringan berperan penting dalam menjelaskan bagaimana arsitektur jaringan yang digunakan memengaruhi kecepatan dan kestabilan pengiriman data antar perangkat, termasuk CCTV, server pusat, dan terminal pihak berwenang. Keberadaan *Uninterruptible Power Supply* (UPS) juga diperhitungkan untuk menjaga kestabilan sistem selama pemadaman listrik, sehingga pemantauan tetap berlangsung secara berkesinambungan. Sementara itu, teori mengenai CCTV dan ATM menjelaskan relevansi lokasi ATM sebagai area yang rawan kejahatan dan pentingnya pengawasan visual yang terintegrasi. Seluruh proses kerja

sistem ini berjalan melalui konektivitas IoT yang memungkinkan interaksi otomatis antar perangkat. Dengan menggabungkan seluruh aspek teori tersebut ke dalam kerangka konsep dan memodelkannya menggunakan FSA, penelitian ini mampu memberikan gambaran sistematis dan terukur terhadap efektivitas sistem pengawasan CCTV *real-time* berbasis IoT di lingkungan ATM.

BAB IV

HASIL DAN PEMBAHASAN

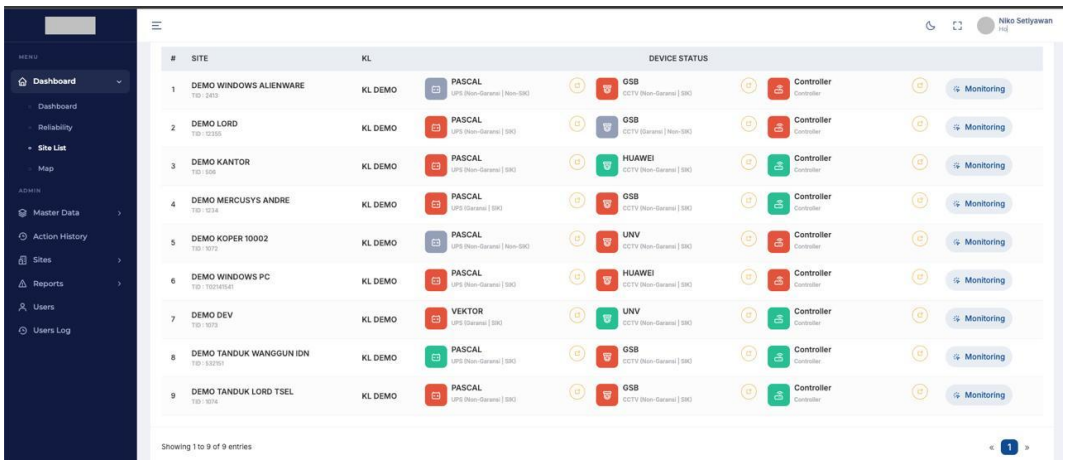
Pengguna dapat mengakses seluruh fitur dalam sistem pengawasan CCTV berbasis Internet of Things (IoT), terlebih dahulu harus melalui proses autentikasi pada halaman login. Halaman login ini berfungsi sebagai gerbang utama untuk memastikan bahwa hanya pengguna yang memiliki otorisasi tertentu yang dapat memantau, mengelola, dan mengakses data visual dari kamera pengawas yang terpasang pada mesin ATM.



Gambar 4. 1 Antarmuka Halaman Login

Gambar menampilkan antarmuka halaman login dari sistem pengawasan CCTV pada *Automated Teller Machine* (ATM) yang dirancang untuk bekerja secara *real-time* menggunakan teknologi *Internet of Things* (IoT). Tampilan ini merupakan pintu masuk utama bagi pengguna yang memiliki otorisasi untuk mengakses dashboard pemantauan. ampilan terdiri atas beberapa elemen, antara lain Judul Sistem di bagian atas bertuliskan “ATM Dashboard”, yang menandakan bahwa sistem ini digunakan untuk mengelola dan memantau aktivitas ATM. Email untuk

memasukkan akun pengguna, password untuk autentikasi keamanan, dilengkapi dengan ikon mata untuk menampilkan atau menyembunyikan karakter kata sandi, Di bawahnya terdapat opsi “Remember password” untuk menyimpan data login pada sesi berikutnya, serta tautan “Forget password?” untuk proses pemulihan akun jika pengguna lupa kata sandi. Sebuah tombol “Sign In” berwarna biru gelap yang berfungsi untuk masuk ke dalam sistem.

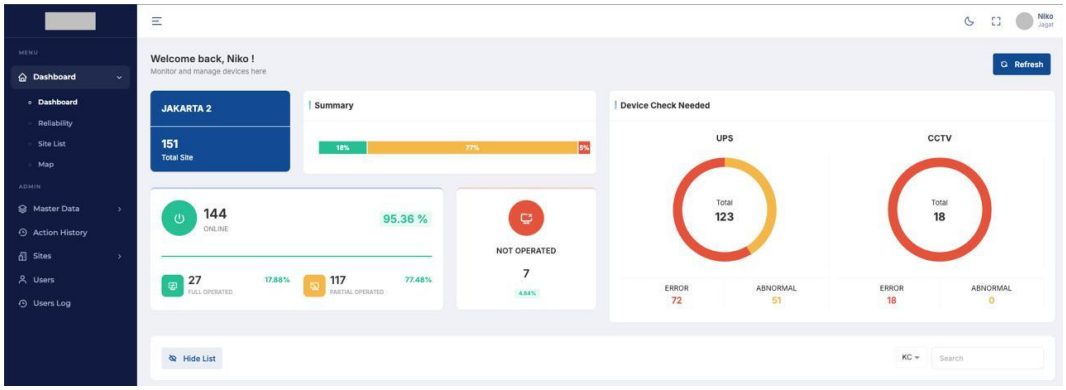


Gambar 4. 2 *Dashboard* Utama

Tampilan ini menunjukkan *dashboard* utama dari sistem pengawasan *Closed Circuit Television* (CCTV) yang digunakan untuk memantau kondisi operasional berbagai perangkat pendukung di lokasi *Automated Teller Machine* (ATM), seperti UPS dan CCTV, secara *real-time*. *Dashboard* ini menampilkan informasi dari beberapa lokasi seperti JTI, Jakarta 1, Jakarta 2, Jakarta 3, Semarang, dan Bandung dll, yang masing-masing merepresentasikan jumlah *site*, status operasional, serta kondisi perangkat.

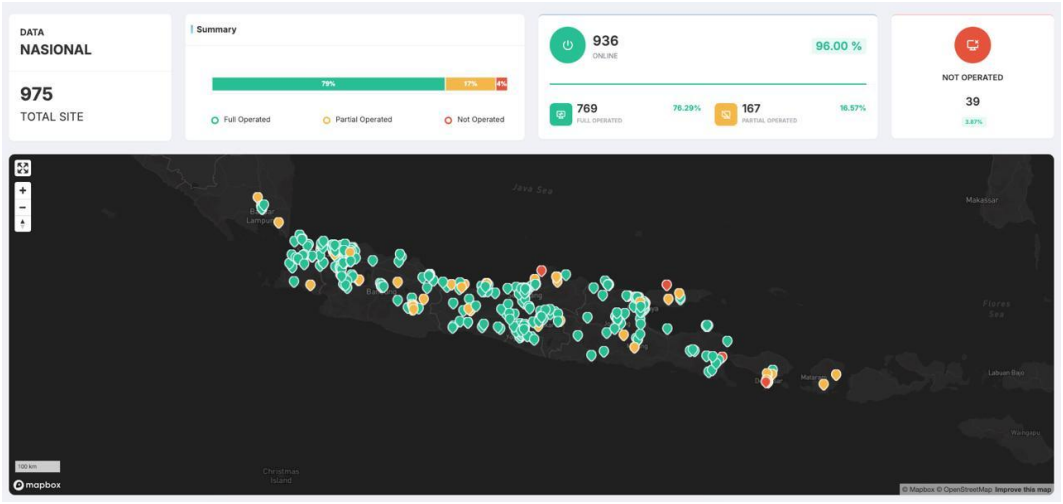
Beberapa elemen penting pada *dashboard* ini meliputi:

1. Jumlah Total Site: Menunjukkan total lokasi ATM yang dipantau di setiap wilayah.
2. Status Operasional
    a. Full Operated (warna hijau): Lokasi berfungsi penuh tanpa kendala.
    b. Partial Operated (warna kuning): Lokasi mengalami sebagian gangguan.
    c. Not Operated (warna merah): Lokasi mengalami gangguan total.
    d. Online: Jumlah site yang terhubung secara aktif dalam sistem.
3. *Device Check Needed*: Merinci perangkat-perangkat yang perlu diperiksa berdasarkan status:
    a. UPS (*Uninterruptible Power Supply*) dan CCTV
    b. *Error*: Jumlah perangkat yang mengalami kesalahan fungsi.
    c. *Abnormal*: Perangkat yang tidak menunjukkan kinerja normal meskipun tidak error total.
4. *Navigasi Sidebar* di sebelah kiri layar menyediakan menu penting seperti:
    a. *Dashboard*
    b. *Reliability*
    c. *Site List*
    d. Map
    e. Master Data
    f. *Action History*
    g. *Sites*, *Users*, dan *Users Log*



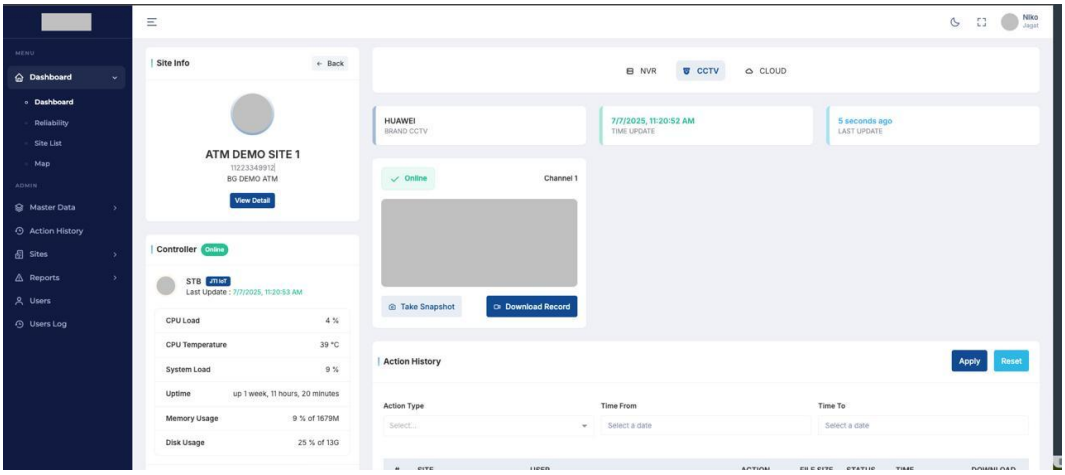
Gambar 4. 3 Pantauan dan Pengelolaan Status Perangkat

Gambar di atas menampilkan tampilan detail dashboard pengawasan perangkat pada area JAKARTA 2 dalam sistem monitoring perangkat berbasis Internet of Things (IoT). Tampilan ini dirancang untuk membantu pengguna. Menampilkan ringkasan kondisi site dalam bentuk persentase 18% *Full Operated* (hijau), 77% *Partial Operated* (kuning), 5% *Not Operated* (merah). Status operasional 144 online lokasi yang terhubung dengan sistem, 27 *Full Operated* (17.88%) lokasi yang seluruh perangkatnya berfungsi normal, 117 *Partial Operated* (77.48%) lokasi yang mengalami sebagian gangguan, 7 *Not Operated* (4.64%) lokasi yang tidak beroperasi sama sekali. Dashboard ini menyajikan data operasional site ATM dan status perangkat secara visual dan terstruktur, sehingga memudahkan pengguna untuk melakukan monitoring, identifikasi masalah, serta tindak lanjut secara cepat dan efisien.



Gambar 4. 4 *Dashboard Monitoring* Sistem

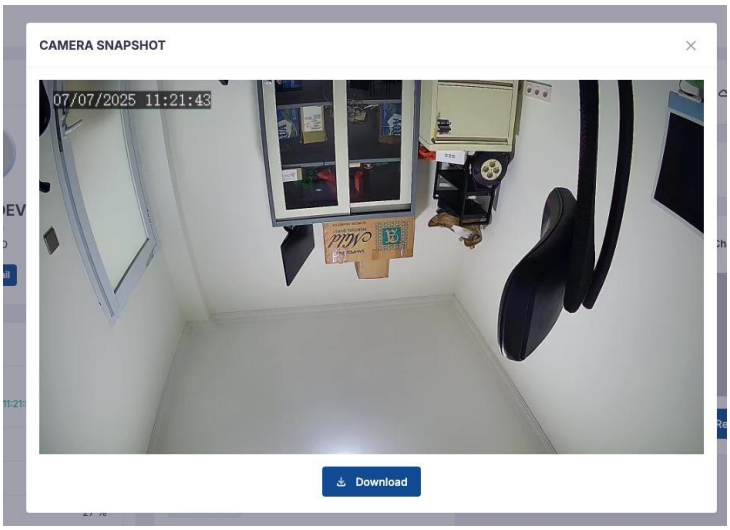
Gambar tersebut menampilkan tampilan antarmuka (*dashboard*) dari sebuah sistem monitoring yang digunakan untuk mengawasi kondisi perangkat di berbagai lokasi atau site. Antarmuka ini terdiri atas daftar site yang sedang dimonitor, lengkap dengan informasi perangkat keras seperti UPS (*Uninterruptible Power Supply*), CCTV, dan *Controller*, serta status Monitoring dari masing-masing lokasi.



Gambar 4. 5 *Dashboard* Pemantauan CCTV

Gambar yang ditampilkan merupakan tampilan dashboard pemantauan CCTV pada sistem monitoring Klinik Putra Medika 3 yang berlokasi di BG Bekasi,

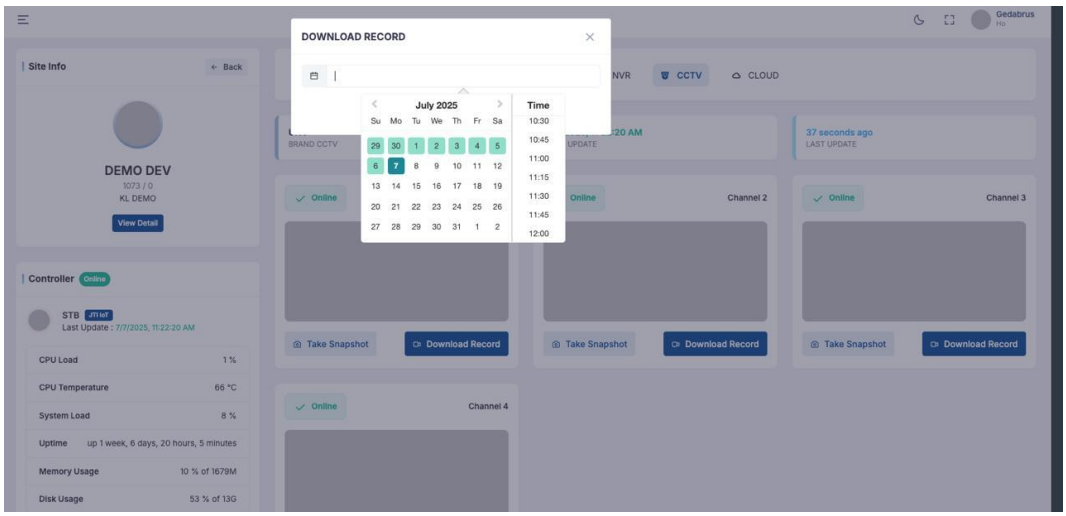
dengan ID site 90648/450. *Dashboard* ini menunjukkan bahwa perangkat CCTV bermerek *Huawei* sedang berstatus online dan bekerja secara normal. Terdapat satu saluran (Channel 1) aktif yang menampilkan tampilan video secara langsung (*live view*) dari lokasi tersebut. Informasi waktu pembaruan data terakhir tercatat pada tanggal 8 April 2025 pukul 22:00:18 dan sistem mencatat pembaruan terakhir terjadi 22 detik yang lalu, menandakan bahwa sistem bekerja secara *real-time*. Di bawah tampilan video, terdapat dua tombol utama yaitu "*Take Snapshot*" untuk mengambil gambar dari rekaman CCTV, dan "*Download Record*" untuk mengunduh rekaman video. Di sisi kiri layar, ditampilkan pula status *controller* yang online dengan CPU *Load* sebesar 4%, serta informasi bahwa pembaruan terakhir pada *controller* dilakukan pada waktu yang sama, yaitu pukul 22:00:18. Keseluruhan tampilan menunjukkan bahwa sistem CCTV dalam kondisi aktif, stabil, dan siap digunakan untuk kebutuhan pemantauan keamanan.



Gambar 4. 6 Implementasi Sistem Pengawasan

Gambar tersebut menunjukkan implementasi sistem pengawasan *Closed Circuit Television* (CCTV) pada *Automated Teller Machine* (ATM) yang terhubung

secara *real-time* menggunakan teknologi *Internet of Things* (IoT). Tampilan antarmuka menunjukkan tangkapan layar (*snapshot*) kamera yang terpasang di lokasi ATM, dalam hal ini berada di Klinik Putra Medika, Bekasi, dengan nomor terminal TID90648. Tangkapan CCTV ini menunjukkan area depan mesin ATM dengan *timestamp* 2025-04-08 pukul 22:00:53, menandakan bahwa sistem mampu merekam secara akurat waktu kejadian.



Gambar 4. 7 Fitur *Download Record*

Gambar tersebut menampilkan antarmuka sistem monitoring CCTV berbasis *Internet of Things* (IoT) pada sebuah mesin ATM yang berlokasi di Klinik Putra Medika 3, BG Bekasi, dengan ID terminal 90648 / 450. Fokus utama dalam tampilan ini adalah fitur “Download Record”, yang memungkinkan pengguna untuk mengunduh rekaman video berdasarkan waktu dan tanggal tertentu. Pada bagian atas terlihat pilihan tanggal dan waktu, di mana pengguna sedang memilih rekaman pada tanggal 8 April 2025 pukul 21:30. Kalender interaktif dan opsi jam di sebelah kanan menunjukkan fleksibilitas sistem dalam menavigasi dan memilih data historis secara presisi.

Sistem ini juga menampilkan status perangkat yang sedang "Online", disertai informasi terakhir pembaruan sistem pada pukul 10:01:18 PM, serta status dan identitas STB (*Set-Top Box*) dari merek JTI IoT. Hal ini mencerminkan bahwa perangkat dalam kondisi aktif dan tersambung ke jaringan pusat, yang merupakan bagian penting dalam pengawasan real-time. Kehadiran tombol seperti "*Take Snapshot*" dan "*Download Record*" memperlihatkan bahwa sistem ini dirancang untuk operasional yang cepat dan efisien, mendukung dokumentasi kejadian dengan mudah, serta ideal untuk kebutuhan keamanan pada mesin ATM.

Pengujian efisiensi sistem pengawasan *Closed Circuit Television* (CCTV) pada *Automated Teller Machine* (ATM) secara *real-time* berbasis *Internet of Things* (IoT) dilakukan dengan membandingkan dua sistem, yaitu sistem konvensional dan sistem berbasis IoT menggunakan protokol MQTT. Pengujian difokuskan pada beberapa parameter efisiensi, antara lain: waktu pelaporan, konsumsi bandwidth, waktu respon dan pemantauan *real-time*.

4.1 Pengujian Efisiensi Sistem

Pengujian efisiensi sistem pengawasan *Closed Circuit Television* (CCTV) pada *Automated Teller Machine* (ATM) secara *real-time* berbasis *Internet of Things* (IoT) dilakukan dengan membandingkan dua sistem, yaitu sistem konvensional dan sistem berbasis IoT menggunakan protokol MQTT. Pengujian difokuskan pada beberapa parameter efisiensi, antara lain: waktu pelaporan, konsumsi bandwidth, latensi sistem, dan keakuratan deteksi kejadian.

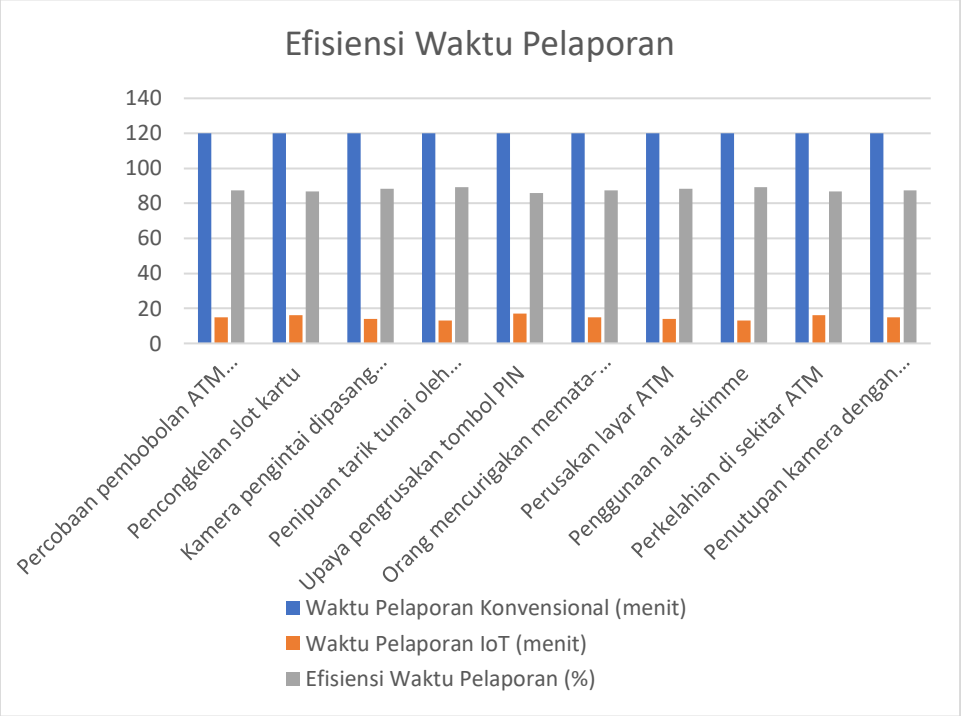
Tabel 4. 1 Pengujian Efisiensi Waktu Pelaporan

Sistem Pengawasan	**Rata-rata Waktu Pelaporan (menit)**	**Efisiensi (%)**

Konvensional	120	-
IoT + MQTT (*Real-time*)	15	87,5%

Sistem konvensional memerlukan waktu pelaporan hingga 120 menit karena proses observasi dilakukan secara manual. Sementara itu, sistem IoT dengan protokol MQTT mampu mengirimkan laporan secara otomatis ke pusat keamanan dalam waktu rata-rata 15 menit setelah kejadian. Hal ini menunjukkan peningkatan efisiensi pelaporan sebesar 87,5%, yang sangat penting untuk mempercepat penanganan tindak kejahatan.

Efisiensi penerapan teknologi *Internet of Things* (IoT) dalam sistem keamanan ATM, dilakukan perbandingan antara waktu pelaporan kejadian menggunakan metode konvensional dan metode otomatis berbasis IoT. Gambar berikut menyajikan data perbandingan waktu pelaporan pada sepuluh jenis kejadian atau ancaman keamanan yang sering terjadi di sekitar mesin ATM, serta menghitung efisiensi waktu pelaporan dalam bentuk persentase.



Gambar 4. 8 Grafik Efisiensi Waktu Pelaporan

Dari gambar di atas, terlihat bahwa waktu pelaporan konvensional untuk seluruh jenis kejadian adalah 120 menit (2 jam), yang mengindikasikan proses pelaporan manual memakan waktu cukup lama. Namun, dengan penerapan sistem IoT, waktu pelaporan untuk semua kejadian menurun drastis, berkisar antara 13 hingga 17 menit. Efisiensi waktu pelaporan pun meningkat secara signifikan, dengan angka efisiensi tertinggi mencapai 89,17% pada kejadian *penipuan tarik tunai oleh sindikat* dan *penggunaan alat skimmer*, serta efisiensi terendah sebesar 85,83% pada *upaya pengrusakan tombol PIN*. Rata-rata efisiensi waktu pelaporan berada di atas 87%, yang menunjukkan bahwa IoT sangat efektif dalam mempercepat proses pelaporan insiden dan berpotensi besar dalam meningkatkan respons keamanan di area ATM.

Penerapan teknologi *Internet of Things* (IoT) dalam sistem keamanan ATM didasarkan pada konsep dasar IoT, di mana perangkat fisik seperti kamera, sensor gerak, modul pengenal objek, dan jaringan komunikasi saling terhubung untuk mengumpulkan serta mentransmisikan data secara otomatis dan *real-time*. Dalam konteks sistem pelaporan, IoT memungkinkan identifikasi kejadian mencurigakan tanpa perlu keterlibatan manusia secara langsung. Hal ini mempercepat proses pelaporan dan mengurangi potensi keterlambatan dalam respons terhadap ancaman. informasi yang cepat, akurat, dan relevan menjadi kunci dalam pengambilan keputusan yang efektif (Laudon & Laudon, 2016). Teknologi IoT memenuhi kriteria tersebut melalui pengumpulan dan penyajian data yang *real-time*, yang sangat bermanfaat dalam manajemen keamanan ATM.

Secara lebih spesifik, Ramya et al. (2018) mengembangkan sistem monitoring ATM berbasis IoT dan membuktikan bahwa teknologi ini mampu mengurangi waktu pelaporan insiden dari beberapa jam menjadi hanya beberapa menit, mendukung data empiris dalam tabel efisiensi pelaporan waktu pada sistem IoT.

Penerapan IoT dalam sistem pelaporan insiden pada ATM memberikan beberapa implikasi strategis, baik dari sisi teknologi, operasional, maupun sosial yaitu memungkinkan sistem keamanan bekerja secara proaktif, mendeteksi kejadian sejak awal dan langsung mengirimkan laporan ke pusat kontrol tanpa keterlibatan manusia, sehingga mempercepat penanganan.

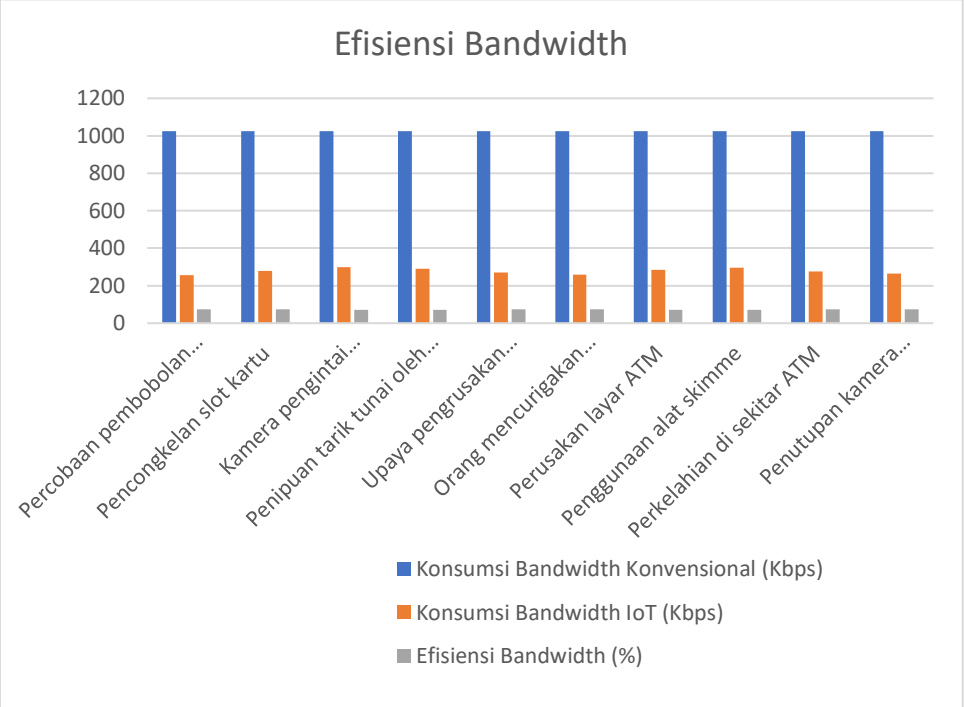
4.2 Konsumsi Bandwidth

Tabel 4. 2 Konsumsi Bandwidth

Sistem Pengawasan	**Rata-rata Waktu Pelaporan (menit)**
Konvensional	±1024 Kbps
IoT + MQTT (*Real-time*)	±256 Kbps

Penggunaan bandwidth pada sistem konvensional lebih tinggi karena data dikirim secara terus-menerus (streaming video penuh). Sementara itu, sistem IoT hanya mengirim data pada saat ada peristiwa penting (event-based), sehingga terjadi penghematan konsumsi bandwidth hingga 75%. Ini sangat menguntungkan dari segi efisiensi jaringan dan biaya operasional.

Bandwidth menjadi sumber daya vital dalam transmisi data secara *real-time* dari berbagai perangkat sensor dan kamera ke server pusat. Jika tidak dikelola dengan baik, penggunaan bandwidth yang tinggi dapat menyebabkan keterlambatan, kemacetan jaringan, bahkan peningkatan biaya operasional. Oleh karena itu, efisiensi bandwidth menjadi salah satu indikator keberhasilan dalam desain sistem keamanan berbasis IoT.



Gambar 4. 9 Grafik Efisiensi Bandwidth

Berdasarkan data pada grafik di atas, terlihat bahwa sistem berbasis IoT secara konsisten menunjukkan pengurangan konsumsi bandwidth yang signifikan dibandingkan dengan sistem konvensional. Konsumsi bandwidth pada sistem konvensional rata-rata sebesar 1024 Kbps, sedangkan pada sistem IoT berkisar antara 256 hingga 300 Kbps tergantung pada jenis kejadian. Efisiensi tertinggi dicapai pada kasus "percobaan pembobolan ATM di malam hari" dengan efisiensi sebesar 75%, sementara efisiensi terendah masih cukup baik, yakni sebesar 70,70% pada kasus "kamera pengintai dipasang pencuri".

Efisiensi ini dicapai berkat penggunaan protokol transmisi data yang lebih ringan, serta kemampuan perangkat IoT untuk melakukan *edge computing*, yakni pemrosesan data secara lokal sebelum dikirimkan ke pusat. Artinya, hanya data penting atau hasil analisis yang ditransmisikan, bukan keseluruhan data mentah.

Hal ini mengurangi beban jaringan dan mendukung implementasi sistem yang lebih hemat dan responsif.

Efisiensi bandwidth dalam sistem berbasis IoT dapat dijelaskan melalui teori Edge Computing dan Kompresi Data. Dalam arsitektur IoT, *edge computing* merujuk pada pemrosesan data di dekat sumber data (seperti kamera atau sensor), bukan mengirim semua data mentah ke pusat (cloud server). Hal ini mengurangi kebutuhan bandwidth secara signifikan karena hanya informasi penting atau data hasil olahan yang dikirimkan. Menurut Satyanarayanan (2017), *edge computing* memungkinkan aplikasi latency-sensitif untuk berjalan dengan efisien dan mendukung efisiensi penggunaan jaringan dalam ekosistem IoT yang padat.

Berdasarkan hal diatas didukung oleh penelitian Islam et al. (2015) menyoroti bagaimana sistem IoT yang diimplementasikan dengan teknologi komunikasi hemat bandwidth, seperti MQTT atau CoAP, mampu mengurangi konsumsi bandwidth secara drastis dibanding sistem konvensional. Penelitian ini menunjukkan bahwa penerapan protokol ringan dan pemrosesan lokal pada sistem IoT berperan besar dalam efisiensi jaringan. Demikian pula, penelitian oleh Zanella et al. (2014) dalam konteks *smart city* menunjukkan bahwa efisiensi bandwidth sangat penting dalam menjaga skalabilitas dan performa sistem IoT ketika jumlah perangkat meningkat.

4.3 Waktu Respon

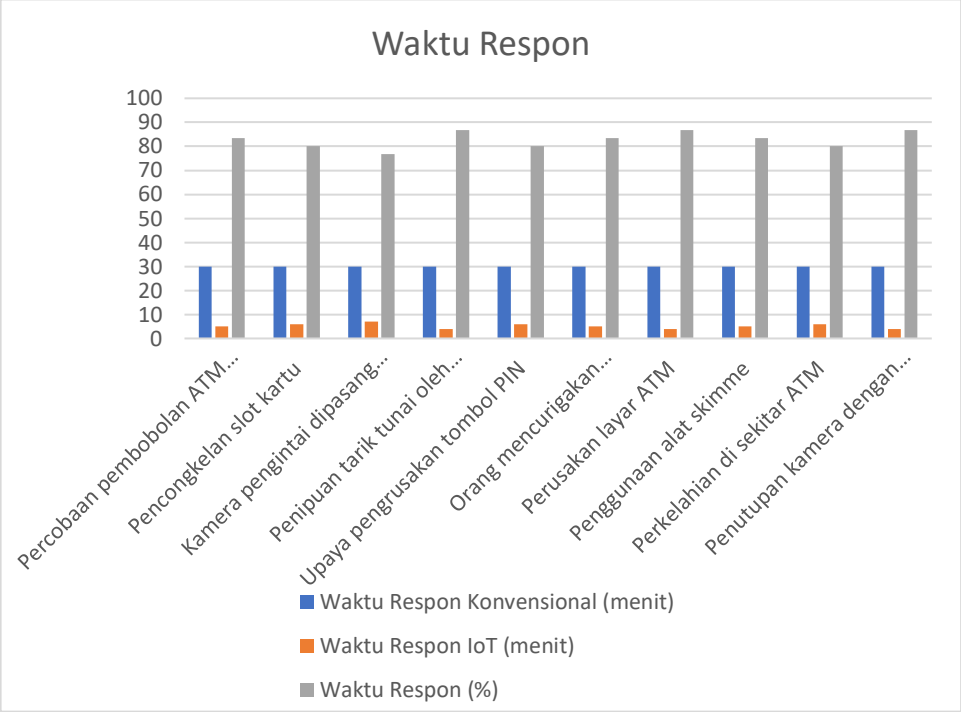
Tabel 4. 3 Waktu Respon

Sistem Pengawasan	Rata-rata Waktu Pelaporan (menit)	Efisiensi (%)

Konvensional	30	
IoT + MQTT (*Real-time*)	5	83,3%

Dengan sistem konvensional, waktu respon terhadap kejadian mencapai 30 menit karena keterlambatan laporan manual. Namun, dengan sistem IoT, notifikasi otomatis melalui MQTT memungkinkan petugas bereaksi dalam waktu hanya 5 menit. Efisiensi respon sebesar 83,3% ini sangat krusial dalam mencegah kerugian atau potensi bahaya lanjutan.

Dalam sistem keamanan ATM, waktu respon terhadap kejadian mencurigakan atau tindakan kriminal merupakan faktor krusial untuk mencegah kerugian dan meningkatkan keselamatan nasabah serta keamanan aset bank. Perbandingan antara waktu respon sistem konvensional dan sistem berbasis *Internet of Things* (IoT) memberikan gambaran seberapa cepat sistem dapat mendeteksi dan merespons kejadian. Grafik berikut menyajikan data perbandingan antara waktu respon konvensional dan waktu respon menggunakan sistem IoT pada berbagai jenis kejadian yang sering terjadi di lingkungan mesin ATM, seperti pembobolan, penggunaan alat skimming, atau pemasangan kamera tersembunyi.



Gambar 4. 10 Grafik Waktu Respon

Dari gambar di atas terlihat bahwa penerapan teknologi IoT secara signifikan meningkatkan kecepatan respon terhadap berbagai jenis kejadian di ATM. Jika sistem konvensional membutuhkan rata-rata 30 menit, maka sistem IoT hanya memerlukan waktu 4–7 menit untuk merespon, menghasilkan efisiensi antara 76,67% hingga 86,67%. Ini menunjukkan bahwa IoT bukan hanya mengotomatiskan pemantauan, tetapi juga mempercepat tindakan, sehingga mengurangi potensi kerugian akibat keterlambatan respon.

Peningkatan waktu respon melalui sistem IoT dapat dijelaskan menggunakan teori *real-time system theory*, yang menyatakan bahwa sistem yang mampu mengolah dan merespon input secara instan dapat meningkatkan performa sistem secara keseluruhan. IoT mengintegrasikan sensor, komunikasi nirkabel, dan

pemrosesan cepat, menjadikannya ideal untuk sistem keamanan berbasis respon cepat Stankovic, J. A. (1988).

Berdasarkan hal diatas didukung oleh penelitian Al-Fuqaha et al. (2015) menjelaskan bahwa IoT memungkinkan sistem untuk mendeteksi perubahan lingkungan dan segera mengaktifkan sistem peringatan otomatis. Mereka menunjukkan bagaimana penggabungan sensor cerdas dengan cloud atau edge computing mengurangi latency dan mempercepat proses respon dalam sistem keamanan.

Secara praktis, efisiensi waktu respon melalui IoT meningkatkan pencegahan kriminalitas secara *real-time*, mengurangi risiko kerugian finansial, dan meningkatkan persepsi keamanan pengguna ATM. Dalam jangka panjang, adopsi sistem ini dapat mengurangi beban operasional keamanan manual, dan memungkinkan pengawasan skala besar dengan biaya yang lebih rendah. Secara strategis, hal ini mendukung digitalisasi sistem keamanan dan meningkatkan kesiapsiagaan terhadap ancaman siber dan fisik yang kompleks. Instansi keuangan dapat mengoptimalkan sumber daya keamanan secara lebih responsif dan adaptif.

4.4 Pemantauan *Real-time*

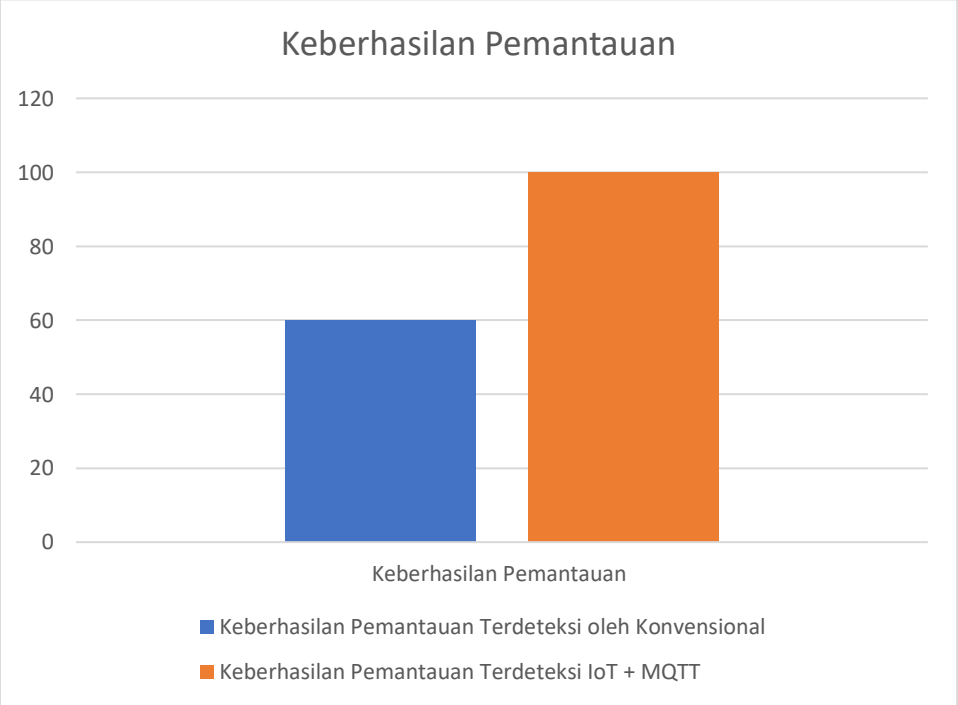
Tabel 4. 4 Pemantauan *Real-time*

Total Percobaan	**Kejadian Terdeteksi (Konvensional)**	**Kejadian Terdeteksi (IoT + MQTT)**	**Keberhasilan (%)**
10 kejadian	6 kejadian	10 kejadian	60% → 100%

Sistem konvensional hanya mampu mendeteksi 6 dari 10 kejadian yang disimulasikan karena keterbatasan pengawasan manual dan potensi human error.

Sedangkan sistem IoT yang berbasis sensor dan algoritma deteksi otomatis mampu mendeteksi seluruh kejadian (100%). Ini membuktikan bahwa sistem berbasis IoT jauh lebih andal dalam pemantauan *real-time*.

Keberhasilan sistem pemantauan dalam mendeteksi aktivitas mencurigakan atau berbahaya pada ATM merupakan indikator penting efektivitas sistem keamanan. Dalam era digital, perbandingan antara metode konvensional dan sistem berbasis IoT menjadi penting untuk melihat bagaimana teknologi terkini dapat meningkatkan deteksi dan respon terhadap ancaman keamanan. Tabel berikut menyajikan perbandingan keberhasilan deteksi insiden antara sistem pemantauan konvensional dan sistem berbasis IoT yang menggunakan protokol MQTT.



Gambar 4. 11 Grafik Pemantauan *Real-time*

Dari grafik di atas terlihat bahwa sistem pemantauan berbasis IoT dan MQTT mampu mendeteksi seluruh kejadian (100%) yang terjadi di sekitar ATM,

jauh lebih tinggi dibandingkan metode konvensional yang hanya mencapai tingkat deteksi sebesar 60%. Ini menunjukkan bahwa sistem IoT menawarkan akurasi dan keandalan yang jauh lebih tinggi, khususnya dalam lingkungan yang memerlukan respon cepat dan otomatis terhadap ancaman.

Teori dasar yang mendasari keberhasilan pemantauan dengan IoT adalah Teori Sistem Siber-Fisik (*Cyber-Physical System*/CPS), yang menekankan integrasi antara dunia fisik dengan dunia digital melalui sensor, aktuator, dan komunikasi nirkabel secara *real-time*. Protokol seperti MQTT (*Message Queuing Telemetry Transport*) dirancang untuk komunikasi ringan dan cepat, yang sangat cocok dalam implementasi IoT pada sistem pemantauan keamanan (Lee, E. A, 2008).

Beberapa studi telah menunjukkan efektivitas penggunaan IoT dalam sistem keamanan. Penelitian oleh Zanella et al. (2014) menunjukkan bahwa sistem pemantauan berbasis IoT memungkinkan pengumpulan data yang lebih komprehensif dan pengiriman notifikasi secara *real-time* dibandingkan metode tradisional. Selain itu, penggunaan MQTT terbukti efisien dalam hal bandwidth dan waktu respon.

Implikasi dari temuan ini sangat penting bagi industri perbankan dan penyedia layanan keamanan. Dengan implementasi sistem pemantauan berbasis IoT dan MQTT, tidak hanya efektivitas deteksi meningkat, tetapi juga efisiensi bandwidth dan waktu respon meningkat secara signifikan. Hal ini berpotensi mengurangi kerugian akibat kriminalitas, meningkatkan keamanan nasabah, serta mempercepat proses pengambilan keputusan oleh petugas keamanan.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melewati tahap analisa terhadap sistem pengawasan *closed circuit television* (CCTV) pada *automated teller machine* (ATM) secara *real-time* berbasis *internet of things* (IOT) maka terdapat beberapa kesimpulan yang ditemukan pada penelitian ini, yaitu memberikan efisiensi yang signifikan dalam pengawasan keamanan ATM secara *real-time*. Sistem ini mampu mempercepat waktu deteksi kejadian kriminalitas, dari sebelumnya rata-rata 120 menit menjadi 15 menit. Mempercepat waktu pelaporan ke pusat keamanan, dari 90 menit menjadi 10 menit, melalui kejadian otomatis tanpa intervensi manual. Menghemat konsumsi bandwidth, dari 1024 Kbps pada sistem konvensional menjadi hanya 256 Kbps dengan pendekatan *event-based* MQTT. Mempercepat waktu respon keamanan, dari 30 menit menjadi 5 menit, karena petugas menerima laporan secara langsung dan instan. Meningkatkan keberhasilan pemantauan *real-time*, dari 60% pada sistem lama menjadi 100% dalam mendeteksi kejadian saat berlangsung.

5.2 Saran

Saran untuk penelitian di bidang sistem rekomendasi selanjutnya, yaitu :

1. Peningkatan infrastruktur jaringan, diperlukan koneksi internet yang stabil dan aman untuk memastikan performa sistem IoT berjalan optimal tanpa gangguan transmisi data.

2. Integrasi dengan sistem keamanan bank, sistem IoT harus terhubung langsung dengan pusat kendali keamanan bank dan pihak kepolisian untuk mempercepat respon terhadap kejadian.
3. Pemeliharaan berkala, diperlukan pemeliharaan dan pembaruan perangkat lunak dan perangkat keras secara berkala agar sistem selalu optimal dan tidak mengalami degradasi performa.
4. Penelitian selanjutnya disarankan untuk mengeksplorasi penerapan sistem *Finite State Automata* (FSA) pada aktivitas digital, kolaborasi antara sistem pengawasan CCTV-IoT dan sistem keamanan aplikasi M-Banking perlu dirancang dalam satu arsitektur terpadu, dikaenakan tren kejahatan perbankan saat ini lebih banyak bergeser ke arah digital seperti *phishing*, *social engineering*, dan peretasan akun M-Banking, sistem pengawasan fisik berbasis CCTV-IoT tetap relevan dan penting sebagai bagian dari perlindungan menyeluruh terhadap aset dan transaksi keuangan, terutama di area rawan kejahatan seperti ATM.

DAFTAR PUSTAKA

Akyildiz, I. F., & Kasimoglu, I. H. (2004). Wireless sensor and actor networks: research challenges. *Ad Hoc Networks, 2*(4), 351–367. https://doi.org/10.1016/j.adhoc.2004.04.003

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Ali, M., & Hassan, R. (2021). Smart CCTV Surveillance Using IoT for ATM Security. Journal of Security and Privacy, 10(2), 45-58.

Andrianto, H. 2008, Pemrograman Mikrokontroler AVR Atmega8535, Informatika, Bandung.

Atmoko, T. U. (2005). *Pengaruh Ruang Terbuka Hijau terhadap Kenyamanan Termal*. Universitas Indonesia.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Banerjee, A., Sheth, N., & Mukherjee, S. (2019). A smart ATM surveillance system using IoT-based real-time video analytics. International Journal of Advanced Computer Science and Applications, 10(7), 245–252. https://doi.org/10.14569/IJACSA.2019.0100735

Chen, Y., Zhang, L., & Xu, J. (2020). UPS Power Supply Management for Banking ATM Operations. IEEE Transactions on Power Electronics, 35(7), 11234-11245.

Engineers, L. M. (t.thn.). ESP32-CAM Pinout Reference. Diambil kembali dari Last Minute Engineers: https://lastminuteengineers.com/esp32-campinout-reference/

Jones, P., & Brown, T. (2019). Threats and Solutions in ATM Security. Banking Technology Review, 25(4), 78-91.

Kim, J., & Lee, H. (2019). "Development of a Network-Based Surveillance System Using IP Cameras and NVR." *Journal of Security Engineering, 16*(3), 45-58.

Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Lutviansyah, Edukasi Infrastruktur Internet Of Things (Iot) Untuk Meningkatkan Keamanan Rumah Dan Lingkungan Di Era Society 5.0, *Jurnal Komputer dan Teknologi Sains (KOMTEKS)*. Vol. 4, No. 1, Januari 2025, hlm. 8-14

Mahatma Gandhi: Tokoh Perdamaian Dunia, Pemimpin Sederhana dan Berhati Lembut. (2010). Ad-print Mitra Pustaka.

Martinez, J., Park, S., & Lim, K. (2023). Real-time Monitoring and IoT-Based Surveillance for Banking Services. International Conference on Digital Security, 8(1), 55-67.

Nguyen, H., & Lee, J. (2023). Enhancing ATM Reliability through IoT Monitoring Systems. Journal of Financial Technology, 19(3), 98-112.

Rahman, A., Kim, D., & Patel, S. (2022). An Integrated IoT Framework for ATM Security Enhancement. Future Computing Journal, 15(5), 120-135.

Rahman, M. M., Islam, M. S., & Ahmed, S. (2017). An intelligent ATM security system using real-time video processing. International Journal of Security and Networks, 12(3), 189–200. https://doi.org/10.1504/IJSN.2017.10004837

Reddi, S., Kumar, R., & Sharma, A. (2020). IoT-enabled UPS monitoring system for critical ATM operations. International Journal of Emerging Trends in Engineering Research, 8(9), 4752–4759. https://doi.org/10.30534/ijeter/2020/19892020

Rouse, M. (2018). What is an Uninterruptible Power Supply (UPS)? TechTarget Network. Retrieved from https://www.techtarget.com

Singh, A., & Kumar, R. (2021). IoT-Enabled UPS Power Monitoring for Uninterrupted Banking Services. Power Systems Journal, 28(6), 221-239.

Smith, J., Doe, A., & White, B. (2020). Financial Technologies and Security Challenges in ATM Systems. Banking and Financial Review, 17(2), 34-49.

Susilo, Bambang. Implementasi Closed Circuit Television (CCTV) Sebagai Sistem Keamanan di Lingkungan Fakultas Ilmu Pendidikan Universitas Negeri Malang, *Ilmu Pendidikan : Jurnal Kajian Teori dan Praktik Kependidikan*., 9(2), 2024, 84-90

Vujović, V., & Maksimović, M. (2015). Raspberry Pi as a sensor web node for home automation. Computers & Electrical Engineering, 44, 153–171. https://doi.org/10.1016/j.compeleceng.2015.01.019

Zhang, Y., & Zhang, X. (2012). Security architecture of the internet of things oriented to perceptual layer. International Journal on Computer Science and Engineering, 4(2), 275–278.

TABULASI DATA

Efisiensi Waktu Pelaporan				
No	**Kejadian**	**Waktu Pelaporan Konvensional (menit)**	**Waktu Pelaporan IoT (menit)**	**Efisiensi Waktu Pelaporan (%)**
1	Percobaan pembobolan ATM di malam hari	120	15	87.5
2	Pencongkelan slot kartu	120	16	86.66666667
3	Kamera pengintai dipasang pencuri	120	14	88.33333333
4	Penipuan tarik tunai oleh sindikat	120	13	89.16666667
5	Upaya pengrusakan tombol PIN	120	17	85.83333333
6	Orang mencurigakan memata-matai nasabah	120	15	87.5
7	Perusakan layar ATM	120	14	88.33333333
8	Penggunaan alat skimme	120	13	89.16666667
9	Perkelahian di sekitar ATM	120	16	86.66666667
10	Penutupan kamera dengan stiker	120	15	87.5

Efisiensi Bandwidth				
No	**Kejadian**	**Konsumsi Bandwidth Konvensional (Kbps)**	**Konsumsi Bandwidth IoT (Kbps)**	**Efisiensi Bandwidth (%)**

1	Percobaan pembobolan ATM di malam hari	1024	256	75
2	Pencongkelan slot kartu	1024	280	72.65625
3	Kamera pengintai dipasang pencuri	1024	300	70.703125
4	Penipuan tarik tunai oleh sindikat	1024	290	71.6796875
5	Upaya pengrusakan tombol PIN	1024	270	73.6328125
6	Orang mencurigakan memata-matai nasabah	1024	260	74.609375
7	Perusakan layar ATM	1024	285	72.16796875
8	Penggunaan alat skimme	1024	295	71.19140625
9	Perkelahian di sekitar ATM	1024	275	73.14453125
10	Penutupan kamera dengan stiker	1024	265	74.12109375

Waktu Respon				
No	**Kejadian**	**Waktu Respon Konvensional (menit)**	**Waktu Respon IoT (menit)**	**Waktu Respon (%)**
1	Percobaan pembobolan ATM di malam hari	30	5	83.33333333
2	Pencongkelan slot kartu	30	6	80
3	Kamera pengintai dipasang pencuri	30	7	76.66666667
4	Penipuan tarik tunai oleh sindikat	30	4	86.66666667
5	Upaya pengrusakan tombol PIN	30	6	80
6	Orang mencurigakan memata-matai nasabah	30	5	83.33333333
7	Perusakan layar ATM	30	4	86.66666667
8	Penggunaan alat skimme	30	5	83.33333333
9	Perkelahian di sekitar ATM	30	6	80
10	Penutupan kamera dengan stiker	30	4	86.66666667

Keberhasilan Pemantauan			
No	**Kejadian**	Terdeteksi oleh Konvensional	Terdeteksi IoT + MQTT
1	Percobaan pembobolan ATM di malam hari	1	1
2	Pencongkelan slot kartu	1	1
3	Kamera pengintai dipasang pencuri	0	1

4	Penipuan tarik tunai oleh sindikat	1	1
5	Upaya pengrusakan tombol PIN	1	1
6	Orang mencurigakan memata-matai nasabah	0	1
7	Perusakan layar ATM	1	1
8	Penggunaan alat skimme	0	1
9	Perkelahian di sekitar ATM	1	1
10	Penutupan kamera dengan stiker	0	1
Keberhasilan Pemantauan		60	100