Vol. 1 No. 1 Tahun 2024

universitas paramadina

Journal of Informatics, IoT and Games

madinaverse

Diterbitkan oleh:
Program Studi Teknik Informatika
Fakultas Ilmu Rekayasa
Universitas Paramadina

Desember 2024

MADINAVERSE: JURNAL INFORMATIKA, IOT DAN GAMES
Volume 1, Nomor 1, Desember 2024

Dikelola dan Dipublikasikan oleh:
Program Studi Teknik Informatika Universitas Paramadina

MADINAVERSE: JURNAL INFORMATIKA, IOT DAN GAMES
Volume 1, Nomor 1, Desember 2024

Editorial Address
Program Studi Teknik Informatika
Universitas Paramadina Kampus Cipayung
Jl. Raya Mabes Hankam Kav. 9 Setu, Cipayung, Jakarta Timur - 13880

Dikelola dan Dipublikasikan oleh:
Program Studi Teknik Informatika Universitas Paramadina

MADINAVERSE: JURNAL INFORMATIKA, IOT DAN GAMES
Volume 1, Nomor 1, Desember 2024

Daftar Isi

Dikelola dan Dipublikasikan oleh:
Program Studi Teknik Informatika Universitas Paramadina

MADINAVERSE: Jurnal Informatika, IoT dan Games
Vol. 1, No. 1, Desember 2024

"Critical Analysis of Technological Intervention in the Humanitarian Crisis of Sudan and the UN Agencies Resistance"

Humaira Surya Rabbani
B.A of American, British, and Canadian Studies, Faculty of Political Science, Philipps Universität Marburg
Email: Suryarab@students.uni-marburg.de

Abstrak - Sudan merupakan negara yang digambarkan oleh PBB sebagai negara dengan krisis kemanusiaan terburuk pada tahun 2024. Teknologi berperan sebagai mesin pelanggaran HAM oleh pihak yang berkonflik, dan menjadi senjata bagi badan PBB yang bekerja di Sudan untuk mengatasi bencana sosial dan ketahanan pangan dengan memberikan tindakan dan solusi jangka pendek dan jangka panjang melingkupi berbagai bidang. Pengumpulan data dalam tulisan ini dilakukan dengan menggunakan sejarah dan analisis data. Keterbatasan makalah penelitian ini adalah tidak adanya kesempatan bagi peneliti untuk terjun langsung ke Sudan dan mendapatkan data langsung. Sebelum melakukan penggolahan data, semua data akan diperiksa validistasnya ke dalam sumber terpercaya. Dari hasil analisis data dalam makalah tersebut, dapat disimpulkan bahwa intervensi teknologi dalam krisis kemanusiaan telah berkontribusi dan berhasil dalam banyak hal positif dengan menjadi harapan terakhir bagi para korban dan sebaliknya, disalahgunakan dan kurang efektif untuk membuka masalah Sudan kepada komunitas internasional.

Kata kunci: Humanitarian Crisis, Sudan, Technological Interventions, UN Agencies

Abstract -Sudan is a country that has been described by the UN as the worst humanitarian crisis in 2024. Technology became the tool for the human rights violations by the conflicting parties and gun for UN agencies working in Sudan to entangle the social disaster and food security by providing short term and long-term actions and solutions in many fields. The data collection in this paper was carried out using history and data analysis. The limitation of this study paper was the absence of a chance for the researcher to go directly to Sudan to get first-hand data. All data will likely be checked into reliable sources. From the results analysis data in the paper, it can be concluded that technological intervention in the human crisis has contributed and succeeded in many positive ways to being the last platform for the victims and on the contrary, being abused, and failed to open the Sudanese issue to the international community.

Keywords— Humanitarian Crisis, Sudan, Technological Interventions, UN Agencies

I. INTRODUCTION

Early thought that started and motivated the wiring process of this paper is hence there was never a real democracy and long-lasting peace in Sudan, a country that was claimed by the UN as having the worst humanitarian crisis in the half of 2024. With its promising geopolitics, and its strategic position on the edge of the Red Sea, the Sahel, and the Horn of Africa, Sudan is also gifted with numerous natural and human resources. However, sadly Sudan is always been the place where the shadow and proxy wars between the stronger states and non-state actors that stronger in terms of military and financial aspects, and this humanitarian crisis got a very limited publication in international news media coverage. The constant rise and fall of authoritarian governments has caused political instability and created a domino effect such as food insecurity and social disasters across the nation as the economy and peace continue to evolve from bad to worse.

In recent studies, various sources have highlighted significant findings relevant to current events. For instance, Center for Strategic & International Studies (2024) provides insight into emerging trends in the field, emphasizing the impact of external factors on recent developments [1]. Additionally, BBC (2023) reported on key issues affecting the global landscape, shedding light on the political implications of current affairs. Meanwhile, Al Jazeera (2024) covered crucial stories that underscore social and economic challenges faced by communities worldwide. Finally, VOA Africa (2023) focused on specific regional issues, offering a depth of analysis that captures the complexities of the situation on the ground. These sources collectively contribute to a comprehensive understanding of the ongoing narrative in today's society.

The problem formulations in this paper are as follows:

1. How has the technology been used as a tool of propaganda, brainwashing, spreading hate, failing democracy and removing human rights in Sudan and how far, deep, and complex is its function to result in food insecurity and social disaster?

2. What specific technological interventions have been employed by the UN agencies to counteract these negative effects and address the humanitarian crisis mainly in the fields of food insecurity and social disaster in the country?

The aims of this paper are as follows:

1. To examine how technology has been used and abused as a tool of propaganda, brainwashing, spreading hate, failing democracy, and removing human rights in Sudan, and to

determine the depth and complexity of its function in resulting food insecurity and social disasters.

2. To identify the specific technological interventions employed by the UN agencies to counteract the negative effects of technology and address the humanitarian crisis, particularly in the fields of food insecurity and social disaster in Sudan.

This paper provides for the advantages for the future such as pinned points on the critical issues of technological intervention in humanitarian crises, specifically focusing on Sudan. By addressing that technology also has a very negative impact on its intervention such as a tool of propaganda, brainwashing, spreading hate, failing democracy, removing human rights in Sudan and raising awareness.

The paper also specifically identified technological interventions by the UN agencies to counter back these negative effects and handle the humanitarian crisis in Sudan, highlighting food insecurity and social disaster. The analysis can provide useful insights for policymakers, humanitarian organizations, and stakeholders taking part in managing similar crises in the future.

This paper also can function as a learning tool for choosing more suitable approaches and strategies in the future. It can facilitate further research and investigation into more effective uses of technology in humanitarian efforts, contributing to developing more creative solutions for addressing global crises.

Overall, this paper has the prospect to inform and influence future policies, interventions, and strategies aimed at the use of technology for humanitarian purposes, eventually contributing to more practical and impactful answers to humanitarian crises worldwide.

II. RESEARCH AIM & METHOD

A. Research Aim

As the exact title of this paper ‘The Invisible Delegation: Critical Analysis of Technological Interventions in the Humanitarian Crisis of Sudan and the UN Agencies Resistance’, this paper aims to find answers by examining how technology has been used and abused as a tool of propaganda, brainwashing, spreading hate, failing democracy, and removing human rights in Sudan, and to determine the depth and complexity of its function in resulting food insecurity and social disasters. Also identify the specific technological interventions, which are analogized as the invisible delegation used by the UN agencies to counteract the negative effects of technology and address the humanitarian crisis, particularly in the fields of food insecurity and social disaster in Sudan.

B. Research Method

The methods that have been used by the author to conduct this research and gather valid information are observation historical and data analysis and document analysis.

1. Historical data analysis will implicate reviewing past events and their impact on the humanitarian crisis in Sudan, with a specific focus on the role of technology.

2. Document analysis will be used for the review and extract of in-depth analysis of reports, articles, and official documents regarding to the use of technology and UN interventions in Sudan.

The data sources for this research will include educational publications such as educational articles, news articles, and international organizations' report papers related to technology, humanitarian crises, and UN interventions. Besides, official reports and publications from UN agencies, and governmental organizations involved in Sudan's humanitarian crisis will be accessed and analyzed.

Qualitative analysis will be conducted to gain a deep understanding of the narratives and perspectives connected to the use of technology and UN interventions in Sudan. The limitation in conducting this paper’s research is the author's inability to get access to firsthand data in Sudan, which may limit the depth of the analysis. The data validity and credibility portrayal will be critical and aimed at safeguarding the academic trustworthiness of the research results by using proper crediting and referencing from all sources.

III. RESULT & DISCUSSION

A. How has the technology been used as a tool of propaganda, brainwashing, spreading hate, failing democracy and removing human rights in Sudan and how far, deep, and complex is its function to result in food insecurity and social disaster?

On 15th April 2023, Omar al Bashir, who had been a longtime military dictator, was forcefully removed from power after three decades through a military coup d’état. This significant event marked a dramatic shift in the political landscape (Center for Preventive Action, 2024) [2]. This military coup d’etat was supported widely by the citizens and paramilitary groups across the country in the hope of ending the authoritarian rule in Sudan. However, instead of establishing a democratic government for its people, the military won’t let go of its control over the full power in government and just change it with another authoritarian ruler. The transfer of power triggered the rebellion from a powerful paramilitary group named Rapid Support Force versus the Sudanese Armed Forces. Both have various backing from powerful countries such as the United Arab Emirates and Russia. In a recent study, Kurtz (2024) describes the rebellion as leading to a year filled with misery and a humanitarian catastrophe that severely affected its citizens. This situation highlights the profound impact of the conflict on the population, underscoring the urgent need for humanitarian assistance and intervention in times of crisis [3].

Technology is playing a powerful role in scrambling the support from the citizens to take control and power by the RFS and SAF, as Reporters Without Borders noted in its 2024 latest report. Both conflicting parties used television to constantly show propaganda about their image brand their coalition with Uni Arab Emirate and Russia and brainwash

the citizens to justify their actions of human rights violations. The finances for the use of technology for propaganda purposes came from the UAE and Russia [4].

Aa citated from Gallopin, the UAE, a country that served the world as the financial hub, mutually benefit the RSF. UAE need RSF to secure their ownership of Sudanese gold mining to their state's gold global trade and economic reserve. The RSF is also being benefited by the UAE as they can collect their gold revenue safely in haven UAE and supply the weapons for their military activities that some described as genocide [5].

In study by Doxsee and Mahdi and Hiebert (2023) Russia, which is also profitable by the gold like UAE, need the RSF and Sudan completely to fund their own war in Ukraine. Especially after being sanctioned by the EU and other nations [6]. In exchange, the Russian buzzer will continue to work to divide and create chaos in Sudan and the Wagner group, Putin's right-handed paramilitary group, trained and served the RSF willingness if they still want Sudan's gold. Russia's buzzer was tasked to help spread hate speech and propaganda to divide and provoke heat tension between different groups of citizens. This including by the successful use of AI voice cloning to impersonate former president Omar al Bashir, which reported missing since the latest coup, in late 2023.

Another technological abuse by both conflicting parties was their monopolized control and totally limited internet access all over the country [7]. When a demonstration is likely to happen, they shut off the internet access and connection completely and leave the country and its citizens in a total blackout. In study by Nnamani (2023), the internet blackout in political instability has collapsed the economy of the nation [8]. The online services and business completely stopped. The social disaster happened everywhere as many citizens suddenly found themselves as a refugee and were displaced from their own homes with no economic strength and ability to communicate with the outside world [9].

Technology was also responsible for taking part in this food security crisis. In the report by WFP (2024), the food insecurity problem that already existed at the beginning of the civil war now has become very intense and remarked that Sudan is facing the worst hunger crisis and 18 million people are found in the scale of acute hunger and 5 million people in the scale of emergency and malnutrition [10]. The international media coverage just simplified the humanitarian crisis to the international world as just a 'civil war between two generals' and forgot the multilayered and complex foreign roles and circumstances behind it. It was disappointing to compare the case with the news coverage of Ukraine and Palestine. Again, the *realpolitik* played hard to determine the direction and narrative brought and spread to the international community. During the humanitarian crises, Ukraine and Palestine were considered to be more politically important to intervene for major power holders in the world than Sudan. Study conducted by Donelly and Dhingra (2024) showed the shallow simplified narratives made the many international donors cut their funding for UN agencies' humanitarian missions in Sudan. Especially after the RSF also closed the port and airport of Sudan, and donors cut the funding of international aid agencies for Sudan, leaving its people off from the outside world in the intense and stressful humanitarian crisis. The war also disturbed the agricultural productivity across the country, along with the global climate change that brought the drought and resulted in failed harvests. This also correlated tightly with Sudan's economy as the economy mostly relied on agriculture [11].

The children and women are the most victimized in Sudan's humanitarian crisis. Using the latest UN Women statement (2024), gender-based violence became more intense as part of the to continue. In the mass displacement, many women and girls bore the horrifying consequences of the social disaster and food insecurity. Desperate for quick money to provide basic needs such as food and clothes, many women and girls have been raped, experienced domestic violence from their families as the stress and unstable emotional condition in the disaster to were being sold to human traffickers that often organized group to send these women to overseas per request on social media. Technology, which was previously hoped to be the last platform for victims to speak up, seek justice and try to bring this issue up to the international community in the hope they will seek accountability for what the government and the RSF had already done to them, failed its task [12].

B. What specific technological interventions have been used by the UN agencies to counteract these negative effects and address the humanitarian crisis mainly in the fields of food insecurity and social disaster in the country?

To counter back the government and the conflicting parties' use of technology in this humanitarian crisis, the agencies of the United Nations such as the United Nations Refugee Agency (UNHCR), the United Nations Children's Fund (UNICEF), and the World Food Programme (WFP) in 2024 to overcome all of the humanitarian crisis's social disaster and food insecurity in Sudan step by step aimed to reach Sustainable Development Goals by continuing this programme from 2019, even before the civil war, to currently. This project sought the well of the citizens in poverty, gender equality, solving climate change and building peace.

Mass displacement was one of the main results of the social disaster, in Sudan's case, it the political instability. However, the huge amount of displaced people refugees in Sudan was not only internally displaced Sudanese after the civil war between the Sudanese Armed Forces and RFS. As data obtained from UNHCR Sudan also hosted refugees from neighbouring countries with fragile economic and political instability, even though their level of humanitarian crisis was not as severe as can be seen in Sudan. Including Chad, Yemen, Central Africa Republic, Ethiopia, South Sudan, Syria, and Eritrea.

Another resistance and effort from UNHCR (2024), the UN agencies using the technology intervention is launching a programme named 'Empowering Refugees Through Technology' to provide internet to refugees aimed at the betterment of the refugees as the bridge to the aspect of communicating with the outside world. The technology was viewed and used to be an important platform to raise the issue of a humanitarian crisis to the international community through transparent and direct communication [13]. This will likely make the donors give back their humanitarian aid to fuel the transformation progress of the refugee life. This program also enables the refugee of the mass displacement to

put an update and keep learning in this digital era remotely from their shelter. Especially women and girls in Sudan, a country that is still likely to believe that women and girls should not be outside the home too often. The program also makes the identification and data collection process to be easier. The access to electronic cash assistance and financial services to support the refugees in the transformation process including the electric coupon for food rations for each family of refugee. This effort was conducted through the UN agencies' cooperation with various tech companies and businesses with the same humanitarian aim, and the national government.

Aware that the children suffered the most in the Sudan humanitarian crisis, the UN agencies emphasized its care to the acute and emergency malnutrition conditions caused by the food insecurity that was experienced by many children and their delayed occasion to fulfil their human rights to get a proper and good education. Data collected show by UNICEF (2024) that 4 million children have registered in the refugee camp, and almost all of them are malnourished. The humanitarian crisis also impacted Sudanese education to evolve as the worst in the world. So the 'Digital Strategy' programme launched by UNICEF to boost the digital interventions in many positive aspects of the refugee children's lives, including health, education, social and child protection, environment and water, and sanitation as the aim of SDGs (Sustainable Development Goals). This action was also launched in Sudan and hoped to encourage the children of refugees to heal from the trauma and set up a better future [14].

In efforts to end food insecurity and improve a lower middle-income country, the economy relies heavily on the agricultural industry, UNEP reported the UN uses and provides 'Technology Needs Assistance' in Sudan. It acted to improve the variety of crop breeding, conservation agriculture, automatic water level monitoring systems, rainwater-harvesting techniques, biogas-improved stoves, compact fluorescent lamps, and efficient boilers with dual fuels to ensure long-term food security solutions [15].

IV. CONCLUSION & CLOSING

a. In conclusion, the technological intervention really played a very crucial role both in positive and negative ways along with their impacts on the Sudan humanitarian crisis. In the hands of wrong parties like the SDF and RSF, the technology can be a very dangerous weapon in provoking hate, constant propaganda, brainwashing, stripping human rights and failing democracy. But in the UN agencies' hand, technology can be a positive tool to counteract all the negative effects, especially in the aspects of solving social disasters and ensuring food security, even though it still needs further exploration and improvement hence the complex nature behind the humanitarian crisis itself.

b. The analysis in this paper correlates the use of technology and the failed democracy in the authoritarian government as domino effects with other bad consequences such as economic catastrophe, social disaster, mass displacement, and food insecurity at an acute level. And can be concluded that the climate change influence is also significant to food security, but not as much as the social disaster did.

c. by evaluating the previous efforts, failures, challenges, and complex nature using a more strategic approach, the author is positively optimistic that UN agencies will reach more success in doing positive technological intervention. The collaboration with civil society from the grassroots level and the local community to connect with the international community to ensure transparency and accountability was crucial for the successful positive technological interventions in adapting to the dynamic of humanitarian crises itself.

d. May it be the opening way towards stability, peace, democracy and giving back people their rights as human. Especially for the women and children. May the victim get justice and somehow the worst humanitarian crisis will end.

REFERENCES

[1] C. Doxsee, "How Does the Conflict in Sudan Affect Russia and the Wagner Group?," Center for Strategic & International Studies. Accessed: Jun. 19, 2024. [Online]. Available: https://www.csis.org/analysis/how-does-conflict-sudan-affect-russia-and-wagner-group

[2] Center for Preventive Action, "Civil War in Sudan," Global Conflict Tracker.

[3] G. Kurtz, "How (Not) to Talk About the War in Sudan, Stiftung Wissenshcaft Und Politik," Germany: Deutsches Institut fur Internationale Politik und Sicherheit.

[4] Reporter Beyond Borders, "Sudan: Reporter Beyond Borders," Reporter Beyond Borders.

[5] J.-B. Gallopin, "The Great Game of the UAE and Saudi Arabia in Sudan," Middle East Political Science. Accessed: Jun. 20, 2024. [Online]. Available: https://pomeps.org/the-great-game-of-the-uae-and-saudi-arabia-in-sudan

[6] M. Mahdi and K. Hiebert, "Sudan's conflict is being fuelled by a digital propaganda war," Middle East Eye. Accessed: Jun. 19, 2024. [Online]. Available: https://www.middleeasteye.net/opinion/sudan-civil-war-digital-propaganda-campaigns-fuelling

[7] Aljazeera, "Network blackout cuts communications for millions in war-torn Sudan," Aljazeera.

[8] C. Nnamani, "Sudan's war is crippling its budding tech ecosystem," Techcabal. Accessed: Jun. 20, 2024. [Online]. Available: https://techcabal.com/2023/06/08/sudan-war-is-crippling-its-budding-tech-ecosystem/

[9] C. Mitchell, "Internet blackouts: The rise of government-imposed shutdowns," Aljazeera. Accessed: Jun. 19, 2024. [Online]. Available: https://www.aljazeera.com/features/2019/6/16/internet-blackouts-the-rise-of-government-imposed-shutdowns

[10] World Food Programme, "The Sudan country strategic plan (2019 - 2024)," Rome, 2023.

[11] C. Donnelly and R. Dhingra, "Sudan's Crisis Requires a New Approach to International Aid," Lawfare. Accessed: Jun. 19, 2024. [Online]. Available: https://www.lawfaremedia.org/article/sudan-s-crisis-requires-a-new-approach-to-international-aid

[12] UN Woman, "A year of suffering for Sudanese women and girls," UN Woman.

[13] The UN Refugee Agency, "Empowering refugees through technology," 2024. [Online]. Available: https://www.unhcr.org/media/empowering-refugees-through-technology

[14] UNICEF, "One year of the brutal war in Sudan," UNICEF. Accessed: Jun. 19, 2024. [Online]. Available: https://www.unicef.org/sudan/one-year-brutal-war-sudan

[15] Technology Need Assesment, “Sudan is currently in the process of working on its TNA. It has completed its Technology Action Plans and Project Ideas.,” Technology Need Assesment.

State of the Art: Tantangan dan Pentingnya Standarisasi Keamanan IoT dalam Berbagai Implementasi

Sutan Muhammad Sadam Awal[1*)] , Muhammad Darwis[2]
[1]Graduate School of Bioresource and Bioenvironmental Sciences, Faculty of Agriculture, Kyushu University
[2]Program Studi Desain Komunikasi Visual, Fakultas Ilmu Rekayasa, Universitas Paramadina
Email: [1]awal.muhamad.sadam.578@s.kyushu-u.ac.jp, [2]muhammad.darwis@paramadina.ac.id

Abstrak - Standarisasi keamanan data di lingkungan IoT telah menjadi isu utama dengan adopsi teknologi IoT yang cepat. Penelitian ini memberikan gambaran tentang pentingnya standarisasi keamanan informasi untuk melindungi perangkat dan data IoT. Dengan standar keamanan yang jelas dan teruji, pengembang dapat merancang perangkat IoT dengan langkah keamanan yang konsisten. Perusahaan mendapatkan benefit dari investasi keamanan. Selain itu, standardisasi juga memungkinkan interoperabilitas perangkat IoT dari vendor yang berbeda, mengurangi risiko serangan, melindungi privasi pengguna, dan meningkatkan kepercayaan pengguna terhadap teknologi IoT. Penelitian ini juga menyatakan bahwa meskipun standar keamanan IoT sudah ada, penelitian dan pengembangan masih diperlukan untuk mengatasi ancaman keamanan baru yang hadir seiring dengan kemajuan teknologi IoT.

Kata kunci: Keamanan IoT, Keamanan Siber, Perusahaan IoT, Standarisasi IoT

Abstract - Security standardization in the IoT environment has become a major issue with the rapid adoption of IoT technology. This study provides an overview of the importance of information security standardization to protect IoT devices and data. With clear and tested security standards, developers can design IoT devices with consistent security measures. Companies benefit from security investments. In addition, standardization also enables interoperability of IoT devices from different vendors, reduces the risk of attacks, protects user privacy, and increases user trust in IoT technology. The study also states that although IoT security standards exist, research and development are still needed to address new security threats that arise along with the advancement of IoT technology.

Keywords— IoT Security, Cyber Security, IoT Enterprise, IoT Standardization

I. PENDAHULUAN

Perkembangan bisnis teknologi berbasis internet of things (atau selanjutnya disebut IoT) begitu cepat sehingga dapat menimbulkan potensi kejahatan baru menggunakan dunia digital. Industri yang bergerak di bidang teknologi informasi menghadapi tantangan dalam keamanan siber berbasis IoT. Sektor ini memiliki peran vital sebagai target dalam penyerangan siber, sehingga perlu menginvestasikan keamanan infrastruktur. Di samping membawa kemudahan bagi kehidupan manusia, perangkat-perangkat ini rentan terhadap berbagai ancaman dan tantangan keamanan yang tidak hanya membuat khawatir para pengguna untuk mengadopsinya di lingkungan sensitif seperti *e-health* dan *smart home* dan lain-lain, tetapi juga menimbulkan bahaya bagi perkembangan IoT di masa mendatang [1].

Investasi keamanan merupakan sebuah kunci dalam mengupayakan kenyamanan dalam menggunakan IoT. Dengan memperkuat keamanan IoT akan mendapatkan keuntungan berupa pencegahan dari serangan siber secara masif, menghindarkan dari biaya pemulihan terdampak sangat besar, memberikan jaminan kepada pelanggan untuk terus menggunakan sistem IoT. Tentunya, untuk mencapai target keamanan IoT diperlukan standarisasi yang jelas sehingga perusahaan dapat mencapai kualifikasi keamanan siber tertentu, agar supaya dapat menjamin bahwa ini sudah aman digunakan. Berdasarkan penelitian yang dilakukan oleh Karie dkk, diketahui bahwa selama ini terdapat ketidaksesuaian standar keamanan yang diimplementasikan dalam berbagai proyek IoT, meskipun memang standar tersebut memiliki potensi untuk diterapkan [2].

Penelitian ini akan menyoroti standarisasi protokol keamanan IoT yang mengacu kepada jurnal penelitian terkait keamanan IoT. Data umumnya ditelaah melalui studi literatur agar dapat mengorientasikan informasi yang lebih akurat dan efisien. Studi literatur adalah kegiatan yang berkaitan dengan metode pengumpulan data perpustakaan, membaca dan menyimpan bahan penelitian, serta mengolahnya. Selanjutnya, hasil dari penelitian ini berupa pengumpulan data dengan konteks standarisasi keamanan IoT yang bisa dihubungkan dengan dunia pekerjaan secara nyata, agar menjadi acuan perusahaan menerapkan standar keamanan berbasis IoT.

Penelitian ini penting untuk dilaksanakan mengingat saat ini pengembangan teknologi berbasis IoT sedang ramai digalakkan dan diprediksi akan terus menjadi trend teknologi dalam beberapa dekade kedepan. Perkembangan teknologi IoT perlu untuk diperhatikan keamanannya karena dampaknya dapat bersinggungan langsung dengan

keberadaan manusia sebagai penggunanya. Standarisasi keamanan IoT pada akhirnya akan menjadi salah satu poin penting untuk mengurangi resiko dan kesalahan. Dengan demikian, langka untuk memajukan peradaban dengan berbagai solusi canggih berbasis IoT dapat tercapai dan sangat berguna bagi kehidupan.

II. LITERATURE STUDY

A. Keamanan IoT

Keamanan merupakan salah satu bagian terpenting sekaligus tantangan dalam sebuah penerapan IoT. IoT adalah sistem yang kompleks. Iot tidak hanya terlibat sebagai entitas data, mesin, RFID, sensor dan lain-lain, tetapi juga mencakup berbagai perangkat dengan kemampuan komunikasi dan pemrosesan data. Karena banyaknya entitas dan data yang terlibat, IoT menghadirkan risiko keamanan yang dapat mengancam dan merugikan konsumen. Risiko keamanan dapat mempengaruhi kualitas dari IoT itu sendiri. Menurut Roman, dkk. [3] bentuk kejahatan siber terdiri dari:

1. *Eavesdropping*, serangan pasif yang dilakukan di berbagai saluran komunikasi dengan tujuan mengekstraksi data dari arus informasi.
2. *Node Capture*, penyerang mengekstrak data dari node atau infrastruktur lain dengan kemampuan penyimpanan data.
3. Perusakan objek-objek IoT dalam bentuk fisik.
4. *Denial of Service*, serangan yang mengakibatkan pihak yang resmi tidak bisa mengakses layanan.

B. Keamanan Siber

Keamanan siber adalah perlindungan komputer, jaringan, perangkat lunak, sistem kritis, dan data terhadap potensi ancaman digital. Perusahaan memiliki tanggung jawab untuk melindungi data untuk menjaga kepercayaan pelanggan dan mematuhi peraturan. Berdasarkan laporan *National Cyber Security Index* (NCSI) terbaru, tingkat keamanan siber Indonesia menempati peringkat ke-84 dengan skor 38,96. NCSI menggunakan 12 indikator dalam laporannya, mulai dari pengembangan kebijakan keamanan siber atas perlindungan data pribadi hingga memerangi kejahatan siber [4]. Laporan NCSI menunjukkan bahwa tingkat keamanan siber Indonesia masih relatif rendah dibandingkan negara lain. [5] Langkah-langkah keamanan siber memberikan pertahanan dari serangan siber dan memberikan manfaat sebagai berikut, antara lain:

1. Mencegah atau mengurangi biaya pelanggaran
2. Memelihara kepatuhan terhadap peraturan
3. Mengurangi ancaman siber yang terus berkembang.

C. Standarisasi Keamanan IoT

Standar keamanan untuk perangkat IoT yang dikeluarkan oleh organisasi terkemuka dan diakui secara luas untuk melindungi perangkat IoT, data pengguna, dan masalah terkait. Saat ini jumlahnya sedikit dan tidak tersedia secara luas, hanya diatur di wilayah tertentu. Di negara bagian California, Amerika Serikat misalnya, memberlakukan undang-undang perdata California, yang memiliki bagian terpisah tentang keamanan wajib perangkat IoT. Hukum California adalah salah satu dari sedikit hukum di dunia yang secara hukum mengatur privasi dan keamanan perangkat IoT. Salah satu standar yang digunakan misalnya adalah Institut Nasional Standar dan Teknologi (NIST), yang merilis buku putih berjudul Kriteria Keamanan Dasar untuk Perangkat IoT Konsumen. NIST memiliki kerangka kerja untuk memudahkan perusahaan dalam mencapai target standarisasi keamanan. Metode NIST dapat digunakan untuk mengidentifikasi lalu lintas serangan pada jaringan IoT dan menggunakan hasilnya sebagai bukti digital yang resmi dalam bentuk laporan. Selain itu, masih terdapat beberapa standar yang mengatur mengenai jaringan dan teknologi IoT, meskipun terbatas di negara dan wilayah tertentu saja [6].

III. METODE PENELITIAN

Penelitian ini menggunakan pendekatan studi literatur, yang dilakukan dengan mengumpulkan dan menganalisis berbagai referensi dari penelitian-penelitian sebelumnya. Data yang diperoleh kemudian diintegrasikan untuk menghasilkan kesimpulan yang komprehensif. Dalam penelitian ini, teknik analisis data yang digunakan adalah metode analisis isi, yang memungkinkan penarikan kesimpulan yang valid dan pengecekan kembali terhadap konteksnya. Proses analisis dimulai dengan mengidentifikasi hasil penelitian yang paling penting, esensial, dan relevan. Selanjutnya, penelitian diurutkan berdasarkan tahun publikasi, dimulai dari yang paling terbaru, kemudian bergerak mundur ke tahun-tahun sebelumnya. Peneliti kemudian membaca ringkasan dari setiap penelitian yang relevan untuk menilai kesesuaian topik yang dibahas dengan fokus penelitian ini. Pada tahap finalisasi, perhatian diberikan pada bagian-bagian yang penting dan relevan dengan masalah penelitian.

IV. HASIL DAN DISKUSI

Seperti yang telah dijelaskan, bahwa penelitian ini dengan mengemukakan studi literatur. Oleh karena itu, langkah selanjutnya yang penulis lakukan setelah mengidentifikasi kebutuhan pada penelitian ini adalah mulai melakukan literature studi. Berbagai penelitian yang memiliki topik kajian sama sebelumnya, penulis kumpulkan dan telaah kemudian penulis rangkum satu sama lain. Rangkuman hasil studi tersebut seperti pada TABEL 1.

TABEL 1. Studi Literatur

Penelitian	***Permasalahan***	***Topik Keamanan***	***Tantangan***	***Kesimpulan***
A Review of Security Standards and Frameworks for IoT-Based Smart Environments	Menemukan standar keamanan dan kerangka kerja penilaian yang paling memenuhi persyaratan keamanan serta menilai secara komprehensif dan memaparkan postur keamanan lingkungan pintar berbasis IoT	Menggunakan metode taksonomi untuk mendaftarkan langkah-langkah standarisasi keamanan IoT	Banyaknya produsen perangkat IoT tidak memasukkan desain keamanan dan menggunakan berbagai protokol terbaik sehingga membuat konfigurasi kompleks di lingkungan cerdas berbasis IoT.	Keamanan lingkungan pintar berbasis IoT sulit dikembangkan dan diterapkan karena kombinasi tantangan yang ada. Untuk mengatasi ini, makalah ini membahas berbagai standar keamanan, termasuk 80 standar ISO/IEC, 32 standar ETSI, dan 37 kerangka kerja keamanan konvensional yang mencakup 7 publikasi khusus NIST dalam teknik keamanan.
ANT-Centric IoT Security Reference Architecture—Security-by-Design for Satellite-Enabled Smart Cities	Memahami masalah keamanan sistem IoT yang kompleks, dan mengusulkan arsitektur referensi keamanan untuk menilai risiko keamanan dan menangani persyaratan keamanan	Keamanan *ANT Centric* bertujuan melindungi aktivitas kritis dan menerapkan keamanan end-to-end dengan menggunakan konsep mikro-perimeter untuk menghindari asumsi keamanan pada jaringan fisik yang mendasarinya.	1. Kompleksitas sistem IoT dalam hal jumlah perangkat yang terhubung dan persyaratan komunikasi dan pemrosesan yang luas. 2. Peningkatan paparan serangan fisik karena penempatan di lapangan.	IoV meningkatkan navigasi, keselamatan, dan manajemen lalu lintas. SAGIN menjadi infrastruktur ideal untuk menghubungkan IoV dan mendukung kota pintar.
Reviewing IoT Security via Logic Bugs in IoT Platforms and Systems	Kompleksitas (*platform* dan sistem IoT) justru meningkat dalam hal interaksi antara dunia fisik dan dunia maya. Kompleksitas yang meningkat dapat menghasilkan kerentanan baru.	Sistem model, dan skenario serangan perangkat IoT secara umum (*Hardware, Cloud)*	Lebih Banyak Entitas yang Terlibat. Dibandingkan dengan sistem komputasi tradisional, ada lebih banyak entitas yang terlibat	Pabrikan perangkat IoT harus menyadari bahwa perangkat IoT tidak lagi beroperasi sebagai sistem individual. Mereka harus lebih memperhatikan bahaya logika yang terlibat dalam komunikasi perpustakaan.
Arm PSA-Certified IoT Chip Security: A Case Study	Menganalisis keamanan chip IoT yang telah memperoleh sertifikasi *Arm Platform Security Architecture* (PSA) Level 2.	Sertifikasi *Arm Platform Security Architecture* (PSA) Level 2.	Mengevaluasi kebocoran fisik pada chip target dan menganalisis kebisingan dalam jejak elektromagnetik yang dikumpulkan. Mereka juga melakukan simulasi serangan saluran samping EM dengan skenario yang sesuai dengan dunia nyata sebanyak mungkin.	Menganalisis chip keamanan yang telah lulus sertifikasi *Arm's PSA Level 2.* Penulis berhasil memulihkan setengah dari byte kunci enkripsi AES di chip keamanan dengan menggunakan analisis saluran samping EM.
A Network-Aware Internet-Wide Scan for Security Maximization of IPv6-Enabled WLAN IoT Devices	WLAN IoT, seperti IEEE 802.11ah (*WiFi-HaLow*), rentan terhadap ancaman keamanan karena sumber daya yang terbatas, membatasi penggunaan perlindungan dan protokol keamanan.	Aktivasi IPv6 WLAN di Perangkat IoT	Dampak pemindaian tingkat pada skor temporal melibatkan perbaikan, kepercayaan laporan, dan kematangan kode. Metrik lingkungan mencerminkan pengaruh pada keamanan perangkat melalui modifikasi lingkungan keamanan seperti CONF, INT, AVA, dan persyaratan terkait.	Peneliti mengamati bahwa kecepatan pemindaian yang optimal memberikan keamanan yang tinggi sambil memastikan QoS. Namun, pendekatan ini mempertimbangkan perspektif admin detik, yang tidak dapat mengontrol parameter jaringan.
A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security	Sifat lintas sektoral dan multidisiplin sistem IoT menyebabkan tantangan keamanan baru. Langkah-langkah keamanan tradisional tidak efektif untuk melindungi perangkat IoT dan mengatasi kerentanan yang ada.	Taksonomi ML/DL Metode untuk keamanan IoT	Tantangan utama dalam ML dan DL adalah memperoleh set data pelatihan berkualitas tinggi yang mencakup berbagai jenis serangan.	ML dan DL untuk keamanan IoT saling terkait dan saling berinteraksi. Integrasi sinergis ML, DL, dan *blockchain* meningkatkan keamanan dalam sistem IoT.
Blockchain mechanisms for IoT security	Penelitian ini menyoroti beberapa lingkungan IoT di mana BCM memainkan peran penting, sementara pada saat yang sama	Mekanisme *Blockhain*	Teknologi IoT/CPS relatif baru dan belum sepenuhnya dipahami seperti sistem TI tradisional. Belum ada standar komprehensif untuk	Keuntungan menggunakan blockchain adalah bahwa mereka dapat bekerja di lapisan bawah model komunikasi serta di lapisan

	menunjukkan bahwa BCM hanyalah bagian dari solusi Keamanan IoT (IoTSec).		arsitektur, jaringan, dan keamanan yang telah dikembangkan, distabilkan, diadopsi, atau diterapkan. Standarisasi akan memfasilitasi kesederhanaan dan integrasi sistem (termasuk keamanan) dari berbagai vendor terbaik.	aplikasi, sehingga memungkinkan penggunaan sinergis mekanisme lintas lapisan dan domain ekosistem IoT.
Security of IoT Systems: Design Challenges and Opportunities	Memberikan dorongan untuk pengembangan teknik keamanan IoT *Computer-aided design* (CAD). Kita mulai dengan menyajikan survei singkat tentang tantangan dan peluang IoT dengan penekanan pada masalah keamanan	*IoT Security Desiderata* dan *Public physical unclonable function* (PUF)	Dua kendala utama untuk perangkat IoT adalah energi dan keamanan. Kedua kendala tersebut dapat diatasi dengan baik menggunakan teknik CAD	Teknik CAD intensif pengoptimalan ditambah dengan pemodelan akurat tradisional mereka secara alami cocok untuk mengaktifkan desain yang sangat optimal perangkat IoT
IoT Security : ZWave and Thread	Penelitian ini membahas tantangan keamanan untuk sistem IoT. Fitur keamanan sistem IoT tersebar di banyakZ bagian protokol IoT dan membahas berbagai jenis serangan pada sistem IoT dan cara protokol menanganinya	*Zwave* dan *Thread*	- Autentikasi: Verifikasi kredensial perangkat sebelum akses sumber daya PAN. - Kerahasiaan: Enkripsi data untuk melindungi isi pesan. - Otorisasi: Perangkat yang telah dikonfirmasi memiliki izin dan hak akses untuk mengakses sumber daya PAN.	*Z-Wave* dapat beradaptasi dan bertahan dari perubahan teknologi. *Thread* masih baru, sehingga sulit menemukan produk dengan logo *Thread* di pasaran. Waktu akan menentukan bagaimana *Thread* berkembang seiring berjalannya waktu.
Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures	IoT biasanya memiliki arsitektur tiga lapisan yang terdiri dari lapisan Persepsi, Jaringan, dan Aplikasi. Sejumlah prinsip keamanan harus diterapkan pada setiap lapisan untuk mencapai realisasi IoT yang aman.	3 Layar arsitektur IoT: Aplikasi, Jaringan dan Persepsi	Tantangan teknologi biasanya terkait dengan teknologi nirkabel, skalabilitas, energi, dan sifat terdistribusi, sedangkan tantangan keamanan memerlukan kemampuan untuk memastikan keamanan dengan otentikasi, kerahasiaan, keamanan *end-to-end*, integritas, dll.	Kerangka IoT rentan terhadap serangan di semua lapisan, dan banyak tantangan dan persyaratan keamanan perlu diatasi. otentikasi dan protokol kontrol akses, tetapi dengan kemajuan teknologi seperti IPv6 dan 5G, integrasi protokol jaringan baru menjadi penting untuk mencapai topologi IoT yang dinamis.

Berdasarkan TABEL 1, selanjutnya penulis mulai menganalisis topik standar keamanan IoT yang terdapat pada masing-masing penelitian. Langkah ini dilakukan untuk melihat kesamaan dan inti dari masing-masing objektif penelitian tersebut. Kompleksitas *platform* dan sistem IoT semakin meningkat di dunia siber dan nyata maka akan semakin menghasilkan kerentanan yang baru. Kendala utama untuk perangkat IoT adalah energi dan keamanan [7]. Kerangka IoT rentan terhadap serangan di setiap lapisan jaringan dan sistem [8], karenanya ada banyak tantangan dan persyaratan keamanan yang perlu ditangani. Persyaratan untuk mengamankan perangkat IoT sangat kompleks, karena berbagai teknologi, mulai dari perangkat fisik dan komunikasi nirkabel hingga arsitektur seluler dan komputasi awan, harus diamankan dan diintegrasikan dengan teknologi lainnya. Karena standar keamanan dan kerangka kerja dapat diterapkan di domain IoT sangat berbeda dari yang digunakan di domain non-IoT, diperlukan standar keamanan yang efektif dan dengan kerangka kerja berbasis IoT. Semua tantangan ini membuat pengembangan, penerapan, pemantauan, dan pemeliharaan keamanan lingkungan cerdas berbasis IoT menjadi jauh lebih sulit [2].

Lebih jauh, dari 80 standar keamanan ISO/IEC, 32 standar ETSI, dan 37 kerangka kerja keamanan konvensional yang berbeda, termasuk 7 publikasi desain keamanan khusus NIST. Proses peninjauan menemukan bahwa standar keamanan dan kerangka kerja evaluasi akan secara langsung menangani persyaratan keamanan berbasis IoT [2]. Taksonomi mencakup kemungkinan solusi untuk tantangan yang teridentifikasi. Arsitektur referensi keamanan *ANT-centric* sebagai salah satu fokus pada tiga perspektif arsitektur dalam mempelajari sistem IoT yaitu perangkat, internet dan semantik [9]. *ANT-centric* bisa direkomendasikan untuk perangkat IoT dan sudah diterapkan di penelitian kendaraan internet (IoV). Sedangkan untuk spesifik perangkat *chip* IoT, *sertifikasi Arm's PSA Level 2* termasuk aman dibandingkan chip keamanan lain yang beredar di pasar. Meskipun, tetap memiliki risiko kebocoran informasi kunci yang sudah dienkripsi karena sertifikasi PSA level 2 hanya persyaratan dasar. Sertifikasi PSA Level 3 lebih baik karena memungkinkan jaminan keamanan yang lebih ketat. Namun, hanya dua chip yang memperoleh sertifikasi Level 3, dan sebagian besar *chip* yang ada belum mendapatkan sertifikasi tersebut [10].

Kemajuan dalam *machine learning* dan *data mining* telah memungkinkan pengembangan berbagai metode analitik yang kuat yang dapat digunakan untuk meningkatkan keamanan IoT [11]. *Blockchain* tidak terbatas peruntukkannya untuk uang digital, namun bisa diterapkan di integrasi aplikasi data IoT yang ditransasikan ruang lingkup jaringan *multi-tier* yang besar maupun arsip sistem [12]. Teknik *computer-aided design* (CAD) intensif dan optimal yang digabungkan dengan pemodelan akurat tradisional, secara alami cocok untuk memungkinkan desain perangkat IoT yang sangat aman. *Z-wave* lebih aman karena *Z-wave* mendapatkan kerangka keamanan S2 [13]. Kerangka kerja keamanan S2, didasarkan pada AES-128 untuk tautan data dan ECDH untuk pertukaran kunci [14]. Thread masih sangat baru sehingga sulit untuk menemukan produk apa pun di pasaran [15].

V. KESIMPULAN

Berdasarkan identifikasi dari literatur yang relevansi, 9 (sembilan) dari 10 (sepuluh) jurnal membahas tujuan utama dari standarisasi keamanan IoT. Pengumpulan data terfokus kepada beragam standarisasi dan kerangka kerja keamanan yang digunakan. Standarisasi keamanan data IoT sangat penting untuk melindungi data yang dikirimkan oleh perangkat IoT dan jaringan IoT. Standarisasi keamanan yang jelas memungkinkan pengembang merancang perangkat IoT dengan tindakan keamanan yang konsisten dan teruji. Membantu mengurangi risiko serangan dan melindungi privasi pengguna. Hal ini berbanding lurus dengan perusahaan meningkatkan kepercayaan pengguna menggunakan sistem IoT. Investasi keamanan sesuai standar menghasilkan biaya yang lebih layak dihabiskan dibanding biaya pemulihan. Meskipun standar keamanan data IoT sudah ada, melibatkan berbagai pihak dalam proses standarisasi penelitian dan pengembangan harus terus dilakukan untuk memerangi ancaman keamanan baru yang hadir dengan perkembangan teknologi IoT.

1. REFERENSI

[1] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," IEEE Internet Things J, vol. 7, no. 10, pp. 10250–10276, 2020, doi: 10.1109/JIOT.2020.2997651.

[2] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," IEEE Access, vol. 9, pp. 121975–121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[3] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2019, doi: 10.1016/j.comnet.2012.12.018.

[4] Zen Munawar and Novianti Indah Putri, "Keamanan IoT Dengan Deep Learning dan Teknologi Big Data," Tematik, vol. 7, no. 2, pp. 161–185, 2020, doi: 10.38204/tematik.v7i2.479.

[5] A. Haryanto and S. M. Sutra, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," Global Political Studies Journal, vol. 7, no. 1, pp. 56–69, 2023, doi: 10.34010/gpsjournal.v7i1.8141.

[6] L. Arsada and H. Pembahasan, "Penerapan Metode NIST untuk Analisis Serangan Denial of Service (DOS) pada Perangkat Internet of Things (IoT)," Jurnal Ilmiah Komputasi, vol. 20, no. 2, pp. 275–281, 2021, doi: 10.32409/jikstik.20.2.2724.

[7] W. Zhou et al., "Reviewing IoT Security via Logic Bugs in IoT Platforms and Systems," IEEE Internet Things J, vol. 8, no. 14, pp. 11621–11639, 2021, doi: 10.1109/JIOT.2021.3059457.

[8] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015, pp. 336–341, 2016, doi: 10.1109/ICITST.2015.7412116.

[9] D. Lammert, "The connection between the sustainability impacts of software products and the role of software engineers," ACM International Conference Proceeding Series, pp. 294–299, 2021, doi: 10.1145/3463274.3463346.

[10] F. Chen, D. Luo, J. Li, V. C. M. Leung, S. Li, and J. Fan, "Arm PSA-Certified IoT Chip Security: A Case Study," Tsinghua Sci Technol, vol. 28, no. 2, pp. 244–257, 2023, doi: 10.26599/TST.2021.9010094.

[11] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," IEEE Communications Surveys

and Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.
[12] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," Internet of Things (Netherlands), vol. 1–2, pp. 1–13, 2018, doi: 10.1016/j.iot.2018.05.002.
[13] J. Shepard, "New Security Requirements for All Z-Wave Certified IoT Devices," eepower.com.
[14] Silicon Lab, "Introduction to Z-Wave SmartStart," 2017.
[15] I. Unwala, Z. Taqvi, and J. Lu, "IoT security: ZWave and thread," IEEE Green Technologies Conference, vol. 2018-April, pp. 176–182, 2018, doi: 10.1109/GreenTech.2018.00040.

Optimasi Pengelolaan Data Pencarian Fasilitas Ekspedisi Berbasis Otomasi dengan Pendekatan *Framework Waterfall*

Eva Yulyanti[1*)], Shindy Yuliyatini[2] , Imelda Imelda[3]
[1,2,3]Program Studi Magister Ilmu Komputer, Fakultas Teknologi Informasi, Universitas Budi Luhur
Email: [1]2311601369@student.budiluhur.ac.id, [2]2311601302@student.budiluhur.ac.id, [3]imelda@budiluhur.ac.id

Abstrak - Teknologi informasi (TI) telah menjadi bagian integral dari kehidupan sehari-hari dan berperan penting dalam berbagai aspek masyarakat modern. Dengan pesatnya perkembangan teknologi, TI telah mengubah cara individu dan organisasi berkomunikasi, bekerja, dan berinteraksi. PT. XYZ, sebagai perusahaan yang bergerak di bidang logistik menghadapi sebuah tantangan dalam mengelola data pencarian fasilitas ekspedisi. Studi ini bertujuan untuk melakukan otomatisasi pengelolaan data pencarian fasilitas ekspedisi dengan menggunakan metode *Waterfall*. Adapun tahap tahap dalam *Waterfall* mencakup tahap-tahap seperti analisis kebutuhan, perancangan, implementasi, pengujian dan pemeliharaan. Metode *waterfall* sangat membantu karena menyediakan proses yang terstruktur, jelas, dan terorganisasi dalam penyelesaian proyek.

Kata kunci: Waterfall, Otomatisasi Sistem, Analisis Kebutuhan

Abstract - Information technology (IT) has become an integral part of everyday life and plays an important role in various aspects of modern society. With the rapid development of technology, IT has changed the way individuals and organizations communicate, work, and interact. PT XYZ, as a company engaged in logistics, faces a challenge in managing expedition facility search data. This study aims to automate the management of expedition facility search data using the Waterfall framework. The stages in Waterfall include stages such as needs analysis, design, implementation, testing and maintenance. The waterfall method is helpful because it provides a structured, clear, and organized process for project completion.

Keywords— Waterfall, Automatization System, Requirements Analysis

I. PENDAHULUAN

Dalam era digital saat ini, TI telah menjadi komponen penting yang mendukung berbagai sektor, mulai dari bisnis, pendidikan, kesehatan, hingga pemerintahan. Transformasi yang dipicu oleh kemajuan teknologi telah mengubah cara individu dan organisasi berinteraksi, berkomunikasi, dan mengambil keputusan. Seiring dengan meningkatnya volume data dan kompleksitas informasi, TI menawarkan solusi inovatif yang memungkinkan pengolahan dan analisis data secara efisien. Hal ini tidak hanya meningkatkan produktivitas, tetapi juga memberikan keunggulan kompetitif bagi organisasi. Dengan adanya pemanfaatan TI tentu akan lebih dimudahkan dibandingkan dengan tidak adanya pemanfaatan TI. Salah satunya yang terjadi pada PT. XYZ. PT. XYZ adalah sebuah perusahaan logistik yang disediakan untuk memberikan pelayanan pengiriman salah satu platform *e-commerce* yang cukup terkenal. Layanan ini merupakan bagian dari upaya PT. XYZ untuk memberikan pengalaman belanja online yang lebih mudah dan nyaman bagi para pengguna di seluruh Indonesia. Dengan adanya layanan pengiriman khusus pengguna dapat memesan produk dari berbagai toko online dapat memilih opsi pengiriman yang disediakan. PT. XYZ menawarkan layanan pengiriman yang cepat, terpercaya, dan terintegrasi dengan sistem pembayaran digital, sehingga pengguna dapat membayar dan melacak pengiriman produk dengan mudah. Saat ini PT. XYZ sudah memiliki 2.065 fasilitas.

Pesatnya kegiatan belanja online yang dilakukan oleh masyarakat di seluruh Indonesia, PT. XYZ berusaha untuk menyediakan pengiriman di seluruh indonesia, baik di wilayah terpencil sekalipun. Dengan demikian PT. XYZ memperluas ekspansi dengan membuka fasilitas baru atau gudang yang dapat menampung paket dan mengcover semua area. PT. XYZ menciptakan target untuk membuka fasilitas di tiap kecamatan di indonesia. Untuk memperluas cakupan bisnis nya divisi yang berperan penting adalah expansion. Divisi *expansion* adalah bagian dalam sebuah perusahaan yang bertanggung jawab untuk merencanakan, mengelola, dan melaksanakan strategi pertumbuhan dan perluasan bisnis.

Expansion bertanggung jawab dalam melakukan pencarian fasilitas hingga fasilitas tersebut bisa beroperasi (*Go-live*). Dalam prosesnya scouting lokasi biasanya dilakukan langsung oleh *ES* (*Expansion Specialist*) dengan cara datang secara langsung ke lokasi yang di *scouting*. *Expansion* mampu membuka sekitar 70 fasilitas setiap bulannya.

Pada bulan November 2024 ini, *expansion* menciptakan proyek baru yang dinamakan proyek Roro jonggrang. Seperti namanya yaitu Roro Jonggrang, adalah proyek kilat yang dilakukan dengan tujuan dapat membuka sekitar 340 an fasilitas di waktu yang sama, yaitu *go-live* di tgl 28 November 2024. Tentu hal tersebut menjadi tantangan baru untuk expansion karena keterbatasan *ES* (*Expansion Specialist*) yang hanya ada 20 orang. Untuk mengatasi keterbatasan tersebut expansion meminta bantuan dari *City Lead* (bagian

operasional) masing-masing kota untuk bisa memberikan rekomendasi lokasi yang sesuai target pencarian. Caranya yaitu dengan memberikan *google form* yang bisa di isi oleh ops, kemudian dilakukan *review* apakah lokasi yang direkomendasikan sesuai dengan target atau tidak, baik dari segi harga, Luas Bangunan dan titik episentrumnya.

Cara tersebut dinilai efektif untuk bisa memenuhi target pencarian fasilitas dalam proyek roro jonggrang, namun ada beberapa kendala yang dialami oleh *expansion* yaitu 1. kemungkinan terjadi double proses untuk kebutuhan fasilitas yang sama karena ops mengisi *google form* lebih dari sekali. 2. Ketika fasilitas yang sudah di rekomendasikan sudah naik proses atau sudah *approval expansion*, maka harus dilakukan penghapusan agar menghindari double proses. 3. Ketika terjadinya *rescout* atau gagal sewa maka harus ditambahkan lagi ke dalam list *google form.* Selama ini dari sisi *expansion* masih melakukan penghapusan dan penambahan list fasilitas di *google form* secara manual yaitu satu persatu. Hal ini tentu rentan terjadi kesalahan dan berimpact terhadap beberapa hal, salah satunya yaitu waktu dan juga biaya. Karena jika terjadi kesalahan, maka akan terjadi keterlambatan dalam pengoperasian dan jika terjadi *double* proses akan menyebabkan kerugian biaya. Untuk mengatasi masalah-masalah yang ada, penulis membuat sebuah otomatisasi dengan metode *Waterfall*, supaya penghapusan dan penambahan list fasilitas tidak lagi dilakukan secara manual. Kerangka kerja *Waterfall* dipilih karena kemampuannya dalam menjelaskan kebutuhan bisnis dan strategi teknologi melalui desain tahapan yang terstruktur yaitu requirements *analysis* (analisis kebutuhan), *design* (perancangan), *implementation* (implementasi), *testing* (pengujian), dan *deployment* & *maintenance* (deploy dan pemeliharaan) [1], [2], [3].

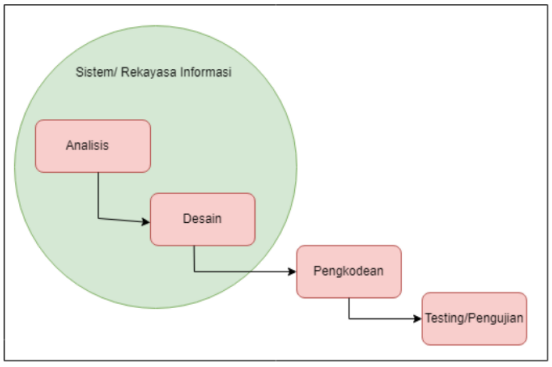
Berdasarkan latar belakang yang kebutuhan PT. XYZ dalam pengelolaan data lokasi fasilitas untuk proyek Roro Jonggrang. Adapun rumusan masalah yang diangkat adalah sebagai berikut:

1. Kendala apa saja yang dihadapi PT. XYZ dalam pengelolaan data lokasi fasilitas untuk proyek Roro Jonggrang?
2. Bagaimana implementasi metode *waterfall* terhadap akurasi dan kecepatan proses pencarian lokasi fasilitas?
3. Apa saja tantangan dalam proses implementasi metode *waterfall* di PT. XYZ?

II. METODE PENELITIAN

Metodologi penelitian adalah suatu sistematis dan terstruktur yang digunakan untuk merancang, melaksanakan, dan menganalisis penelitian. Ini mencakup berbagai langkah dan teknik yang dipilih oleh peneliti untuk mencapai tujuan penelitian.

Model SDLC air terjun (*waterfall*) sering juga disebut model sekuensial linier (*Sequential linear*) atau alur hidup klasik (*classic life cycle*). Model air terjun (*waterfall*) menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau urut dimulai dari analisis, desain, pengkodean, pengujian dan tahap pendukung (*support*). Disebut dengan waterfall karena tahap demi tahap yang dilalui harus menunggu selesainya tahap sebelumnya dan berjalan berurutan [4]. Sebagai contoh tahap coding harus menunggu tahap design selesai. Secara umum tahapan pada model *waterfall* bisa dilihat pada gambar berikut:



Gambar 1. Metode Waterfall

1. Analisis: Menganalisis Masalah dan kebutuhan terkait perancangan sistem informasi pencarian fasilitas ekspedisi.
2. Desain: membuat gambaran sistem seperti apa yang akan dibuat.
3. Melakukan pengkodean (memasukkan koding).
4. Melakukan pengujian terhadap keberhasilan aplikasi yang dirancang.

A. *Desain Penelitian*

Penelitian atau *Research* dilakukan untuk mencari solusi dan mencapai suatu tujuan dengan cara yang sistematis. Tujuan dari suatu penelitian adalah menemukan hal baru, mengembangkan, memperluas ilmu, atau pun menguji kebenaran yang sudah ada. Dalam arti yang lebih spesifik penelitian ilmiah adalah serangkaian pengamatan yang dilakukan secara terus menerus dan berkesinambungan, terakumulasi dan akhirnya akan menghasilkan teori-teori yang dapat menjelaskan fenomena yang ada. Dalam melakukan penelitian diperlukan landasan teori dan arah/tujuan yang jelas yang harus bisa diuji melalui pengamatan untuk menjawab masalah-masalah yang ada. Untuk itu penelitian harus dilakukan secara kompleks dan sistematis untuk mencapai tujuan yang ingin dicapai [3].

Berikut langkah-langkah yang dilakukan untuk melakukan penelitian :

1. Mencari dan membaca literatur mengenai penerapan *waterfall* dalam mengotomatisasi data.
2. Melakukan pengambilan data kepada pihak PT. XYZ.
3. Mempelajari proses dan mengidentifikasi permasalahan yang ada untuk mendapat gambaran tentang permasalahan dalam melakukan pencarian fasilitas untuk proyek roro jonggrang.
4. Memberikan solusi agar proses pencarian fasilitas berjalan lebih mudah dan efektif sehingga target proyek bisa direalisasikan oleh *expansion* PT. XYZ.

B. Prosedur Penelitian

Data dikumpulkan melalui wawancara dengan pihak terkait di divisi expansion, observasi proses yang ada, dan analisis dokumen terkait pengelolaan data.

a. Metode Observasi

Merupakan teknik atau pendekatan untuk mendapatkan data primer dengan cara mengamati langsung objek. Penulis melakukan observasi di PT. XYZ untuk melakukan pengamatan dan mengetahui kendala apa yang dihadapi, mengetahui apa saja informasi yang dibutuhkan disana. Kemudian dari kebutuhan yang telah didapat bisa di analisa sistem seperti apa yang akan dibuat.

b. Metode Wawancara

Metode wawancara dilakukan untuk melengkapi hasil pengamatan yang diperoleh melalui metode observasi. Penulis menggunakan wawancara dengan melakukan tanya jawab salah kepada satu karyawan dari divisi *expansion* dan mengajukan beberapa pertanyaan yang berhubungan dengan penelitian. Pertanyaan yang diajukan tentunya harus berkaitan erat dengan sistem yang akan dibuat agar bisa menghasilkan sistem yang sesuai dengan kebutuhan [5].

c. Metode Studi Pustaka

Dalam penelitian ini, studi pustaka dilakukan dengan mencari jurnal-jurnal literatur yang berkaitan dengan masalah yang akan diteliti sebagai referensi bagi penulis untuk menganalisis pemecahan masalah dalam penelitian ini [6], [7].

III. HASIL DAN DISKUSI

Waterfall adalah model pengembangan perangkat lunak yang bersifat linier dan berurutan, di mana setiap tahap atau fase dalam proses pengembangan dilakukan secara bertahap dan tidak bisa kembali ke tahap sebelumnya. Model ini menggambarkan proses pengembangan perangkat lunak seperti aliran air terjun yang mengalir turun dari atas, sehingga setiap fase harus diselesaikan terlebih dahulu sebelum melanjutkan ke fase berikutnya [8].

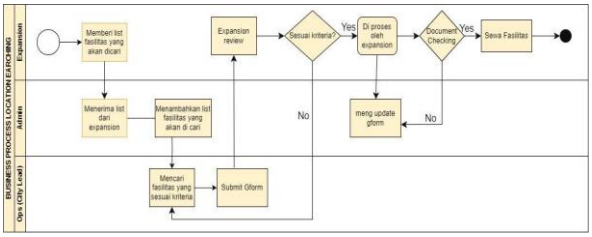
A. Kebutuhan (*Requirements*)

Pada fase ini, Perusahaan akan menetapkan konteks dan tujuan arsitektur yang diinginkan. PT. XYZ perlu mengidentifikasi tantangan yang dihadapi, seperti pengelolaan data yang manual dan potensi duplikasi. Di sini, *stakeholder* dapat dilibatkan untuk merumuskan kebutuhan dan ekspektasi mereka. Fase ini juga melibatkan pengembangan visi yang jelas mengenai bagaimana sistem baru akan berfungsi [9]. PT. XYZ dapat merumuskan tujuan otomatisasi yang meliputi:

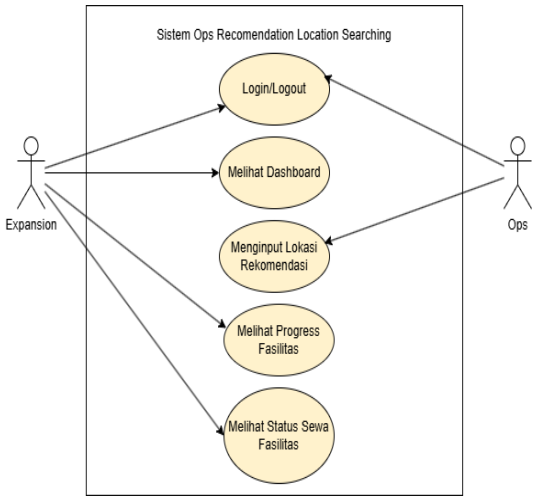
a. Meningkatkan efisiensi dalam pencarian dan pengelolaan lokasi fasilitas.
b. Mengurangi kesalahan dalam proses pengumpulan data.
c. Menciptakan sistem yang lebih responsif dan adaptif terhadap perubahan kebutuhan bisnis.

B. Desain (Design)

Mendesain arsitektur dan komponen-komponen perangkat lunak. Desain yang dibuat mampu menginterpretasikan apa yang akan dibuat di sistem [10], [11].



Gambar 2. Proses Bisnis Pencarian Fasilitas [12]



Gambar 3. *Use Case Diagram* Sistem yang diusulkan [13]

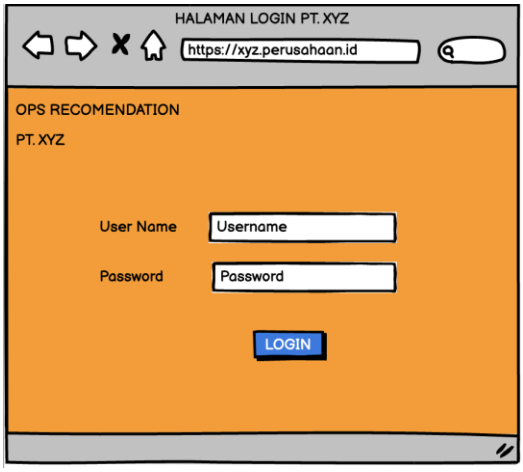
C. Implementasi (Implementation)

Pengujian (*Testing*): Menguji perangkat lunak untuk memastikan bahwa ia berfungsi sesuai dengan yang diinginkan [14]. Proses pengkodean atau pengembangan perangkat lunak berdasarkan desain yang telah dibuat [15].

1. Halaman Login

TABEL 1. *Blackbox* Halaman *Login*

Input	Hasil yang diharapkan	Hasil
Input username & Password	Login ke menu selanjutnya	*Valid*

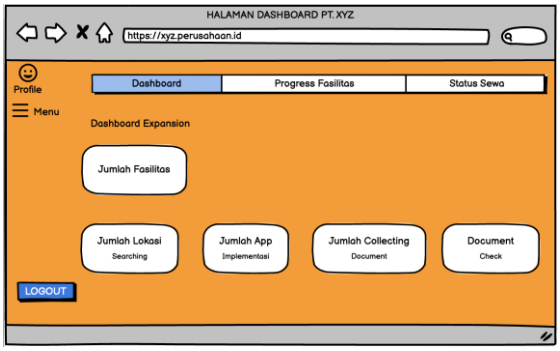


Gambar 4. Halaman *Login*

2. Halaman *Dashboard*

TABEL 2. *Blackbox Dashboard*

Input	Hasil yang diharapkan	Hasil
Memilih menu yang ada di *dashboard*	Masuk ke menu selanjutnya	*Valid*

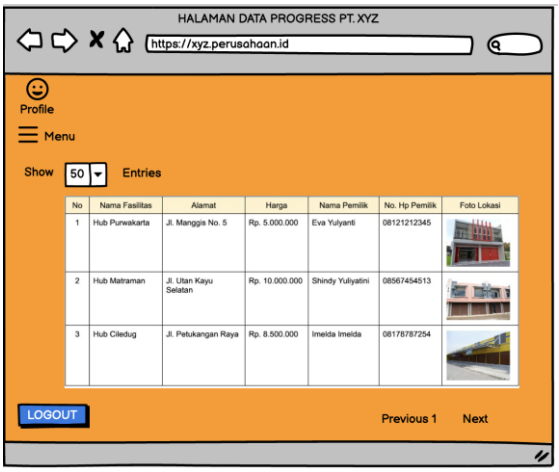


Gambar 5. Halaman *Dashboard*

3. Halaman Data Progress

TABEL 3. *Blackbox* Data *Progress*

Input	Hasil yang diharapkan	Hasil
Memilih menu data progress	masuk ke menu data progress & dapat melihat progress tiap facility	*Valid*



Gambar 6. Halaman Data *Progress*

4. Halaman Status Sewa

TABEL. 4 Blackbox Status Sewa

Input	Hasil yang diharapkan	Hasil
Memilih menu status sewa	masuk ke menu status sewa & dapat melihat status tiap facility	*Valid*

Gambar 7. Halaman Status Sewa

IV. KESIMPULAN

Penelitian ini menegaskan bahwa otomatisasi berbasis teknologi dapat memberikan solusi yang signifikan terhadap permasalahan operasional yang kompleks. PT. XYZ, sebagai perusahaan logistik, menghadapi tantangan dalam mengelola data pencarian fasilitas ekspedisi secara manual, yang rentan terhadap kesalahan seperti duplikasi data, keterlambatan, dan biaya tambahan. Dengan menggunakan metode pengembangan perangkat lunak *Waterfall*, penelitian ini berhasil mengotomatisasi proses pengelolaan data, mulai dari analisis kebutuhan, desain, implementasi, hingga pengujian sistem. Metode ini memberikan struktur yang terorganisasi dan jelas dalam menyelesaikan proyek. Sistem baru yang dikembangkan meningkatkan efisiensi operasional, mengurangi kesalahan manusia, dan mempermudah pengelolaan data. Hasil pengujian menunjukkan bahwa fitur-fitur utama seperti *login*, *dashboard*, dan pelacakan progres fasilitas berjalan sesuai harapan. Solusi ini memberikan dampak positif terhadap kecepatan dan akurasi proses bisnis, memungkinkan PT. XYZ untuk mencapai target ekspansi fasilitas lebih efektif dan efisien.

REFERENSI

[1] B. Setiadi, "Aplikasi Monitoring Keuangan Bagian Operasional Di Starindo Berbasis Web," *Journal of Industrial Engineering and Operation Management*, vol. 4, no. 1, 2021, doi: 10.31602/jieom.v4i1.5437.

[2] S. Alviana and B. Kurniawan, "Penerapan Sistem Informasi Iuran Warga Griya Pataruman Asri Berbasis Website," *Jurnal Pengabdian Masyarakat Indonesia*, vol. 1, no. 6, pp. 343–350, 2021, doi: 10.52436/1.jpmi.41.

[3] Z. Sharfina and H. B. Santoso, "An Indonesian adaptation of the System Usability Scale (SUS)," *2016 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2016*, pp. 145–148, 2017, doi: 10.1109/ICACSIS.2016.7872776.

[4] D. Susanti, "PERANCANGAN APLIKASI ABSENSI DAN CATATAN PEGAWAI DI DESA CIHAUR BERBASIS WEB MENGGUNAKAN CODEIGNITER Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)," *Universitas Majalengka*, vol. 6, no. 1, 2017.

[5] M. Arifin and T. Sagirani, "Pendekatan Double Diamond Untuk Meningkatkan Ketertarikan Pengguna Pada Portal Akademik," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 10, no. 2, pp. 228–240, 2023.

[6] M. J. Sousa, R. Cruz, and J. M. Martins, "Digital Learning Methodologies and Tools – a Literature Review," *EDULEARN17 Proceedings*, vol. 1, no. July, pp. 5185–5192, 2017, doi: 10.21125/edulearn.2017.2158.

[7] H. K. Andreassen *et al.*, "European citizens' use of E-health services: A study of seven countries," *BMC Public Health*, vol. 7, pp. 1–7, 2007, doi: 10.1186/1471-2458-7-53.

[8] D. Gunawan, D. Puji, R. Andriani, and Susafa'ati, "Sistem Informasi Penjualan Berbasis Web Pada Restoran Caki Cake Karawang," *Jurnal AKRAB JUARA*, vol. 3, no. 1, pp. 1–16, 2018.

[9] A. C. Leal, "Methodological proposal of requirements engineering aligning IS/IT to the business strategy," *Proceedings - International Conference of the Chilean Computer Science Society, SCCC*, pp. 245–246, 2012, doi: 10.1109/SCCC.2012.35.

[10] A. Shaikh and U. K. Wiil, "Overview of Slicing and Feedback Techniques for Efficient Verification of UML/OCL Class Diagrams," *IEEE Access*, vol. 6, no. c, pp. 23864–23882, 2018, doi: 10.1109/ACCESS.2018.2797695.

[11] R. A. Maulana, M. A. Fatih, L. A. Suto, and M. Darwis, "Development of Paramadina Roomhub Application As Room Booking System Using Waterfall Method," vol. 07, no. 02, pp. 176–185, 2024.

[12] W. A. Rahman and L. Ariyani, "Rancang Bangun Sistem Informasi Pembayaran Iuran Warga RT 05 RW 002 Berbasis Java," *Jurnal Riset dan Aplikasi Mahasiswa Informatika (JRAMI)*, vol. 2, no. 04, pp. 657–662, 2021, doi: 10.30998/jrami.v2i04.1637.

[13] R. S. Pressman, *Software Engineering: A Practitioner's Approach 8e.*, 8th ed. New York: McGraw-Hill, 2015.

[14] T. S. Jaya, "Pengujian Aplikasi dengan Metode Blackbox Testing Boundary Value Analysis (Studi Kasus: Kantor Digital Politeknik Negeri Lampung)," *Jurnal Informatika Pengembangan IT (JPIT)*, vol. 3, no. 2, pp. 45–46, 2018, doi: 10.30591/jpit.v3i1.647.

[15] A. Hadi, "Analisis Dan Perancangan Sistem Informasi Penjualan Pulsa Pada Toko Lumbung Buana Cellular," *PENA TEKNIK: Jurnal Ilmiah Ilmu-Ilmu Teknik*, vol. 5, no. 1, p. 19, 2020, doi: 10.51557/pt_jiit.v5i1.600.

MADINAVERSE: Jurnal Informatika, IoT dan Games
Vol. 1, No. 1, Desember 2024

Keamanan Data dalam Penggunaan IoT untuk Menghimpun dan Mengelola Big Data

Syahla Nadya Putri Syabrina
Program Studi Teknik Informatika, Fakultas Ilmu Rekayasa, Universitas Paramadina
Email: syahla.putri@students.paramadina.ac

Abstrak - Dalam era pertumbuhan sistem informasi yang pesat, pemanfaatan Internet of Things (IoT) dan Big Data telah menjadi fokus utama perusahaan modern. Perangkat IoT, yang terhubung ke internet, memainkan peran penting dalam mengumpulkan, mentransmisikan, dan mengolah data dari berbagai sumber. Sementara itu, Big Data adalah istilah yang menggambarkan jumlah data yang besar dan beragam, jika dimanfaatkan dengan baik, dapat memberikan berbagai keuntungan. Namun, dengan meningkatnya penggunaan IoT dan Big Data, perlindungan keamanan informasi menjadi semakin penting. Tujuan dari penelitian ini adalah untuk menganalisis tantangan utama dalam keamanan data terkait penggunaan IoT untuk mengelola Big Data. Metode penelitian menggunakan kajian literatur dari berbagai artikel jurnal nasional dan internasional yang relevan. Hasil analisis menunjukkan bahwa tantangan utama meliputi pengumpulan data yang luas, keamanan data, identifikasi individu, kontrol pengguna, dan akses data oleh pihak ketiga. Oleh karena itu, integrasi yang seimbang antara teknologi IoT, Big Data, dan praktik keamanan data menjadi kunci untuk memastikan keberhasilan dan keberlanjutan bisnis di era digital ini.

Kata kunci: Keamanan Data, IoT, Big Data, Pengumpulan Data, Perlindungan Informasi

Abstrak - In the era of rapid information system growth, the utilization of the Internet of Things (IoT) and Big Data has become a primary focus for modern companies. IoT devices, which are connected to the internet, play a crucial role in collecting, transmitting, and processing data from various sources. Meanwhile, Big Data describes large and diverse datasets that, if properly leveraged, can provide numerous benefits. However, with the increasing use of IoT and Big Data, the protection of information security becomes increasingly important. The aim of this study is to analyze the main challenges in data security related to the use of IoT for managing Big Data. The research method involves a literature review of various relevant national and international journal articles. The results indicate that the main challenges include extensive data collection, data security, individual identification, user control, and third-party data access. Therefore, a balanced integration of IoT technology, Big Data, and data security practices is key to ensuring business success and sustainability in this digital era.

Keywords: Data Security, IoT, Big Data, Data Collection, Information Protection

I. PENDAHULUAN

Di era perkembangan pesat sistem informasi, penggunaan Internet of Things (IoT) dan big data telah menjadi perhatian utama bagi perusahaan-perusahaan modern.Perangkat IoT, yang merupakan perangkat fisik terhubung ke internet, memainkan peran penting dalam mengumpulkan, mentransmisikan, dan mengolah data dari berbagai sumber, termasuk sensor, transaksi, dan aktivitas digital lainnya. Di sisi lain operasional, inovasi produk dan layanan, strategi pemasaran yang efektif, serta deteksi penipuan dan keamanan.

Namun, dengan meningkatnya penggunaan IoT dan big data, perlindungan keamanan informasi menjadi semakin penting. Informasi yang tidak dilindungi
dengan baik dapat jatuh ke tangan yang tidak bertanggung jawab, menyebabkan ketidakakuratan data dan bahkan bisa menjadi sumber informasi yang menyesatkan. Oleh karena itu, system keamanan data harus mampu mengidentifikasi, mengotentifikasi, dan memberikan izin dengan tepat kepada pengguna. Berbagai serangan atau peretasan, seperti gangguan sistem, penolakan layanan, vandalisme dan lainnya, dapat mengancam integritas data dan keamanan sistem [1].

Tujuan dari keamanan data dalam penggunaan IoT untuk menghimpun dan mengelola big data adalah untuk melindungi sistem dari berbagai ancaman dan untuk mendeteksi serta memperbaiki kerusakan yang mungkin terjadi. Pendekatan yang efektif dalam mengelola data dan komunikasi antar objek IoT harus mencakup penggunaan algoritma pemograman yang tepat, yang tidak harus mengoptimalkan kinerja sistem tetapi juga menjaga keamanan data yang dikirim dan diterima. Dengan demikian, integrasi yang seimbang antara penggunaan IoT, Big data, dan keamanan data menjadi kunci dalam memastikan keberhasilan dan keberlanjutan bisnis modern di era digital ini [2].

Dalam konteks tersebut, tujuan dari penelitian ini adalah untuk menganalisis dan memahami tantangan utama yang

dihadapi dalam menjaga keamanan data pada penggunaan IoT untuk mengelola big data.

II. METODE PENELITIAN

Penulis menggunakan kajian literatur dengan mencari berbagai artikel dari jurnal nasional dan internasional melalui Google Scholar yang relevan dengan topik yang dibahas. Langkah-langkah dalam menggunakan kajian literatur ini mencakup pemilihan topik, pengumpulan sumber literatur yang mendukung topik tersebut, pengkajian literatur yang relevan untuk menyusun pembahasan tentang kemampuan berpikir kreatif matematis, serta menyimpulkan dan memberikan saran berdasarkan hasil dari kajian [3].

III. ANALISIS DATA

Dalam revolusi industri, interkoneksi antara IoT dan Big Data memiliki dampak yang signifikan dalam upaya meningkatkan efisiensi operasional perusahaan. Gabungan teknologi ini memungkinkan penggunaan data yang dikumpulkan dari berbagai sumber, seperti sensor, perangkat mobile, media sosial, dan transaksi bisnis, untuk mengoptimalkan proses operasional. Melalui IoT, perusahaan dapat memantau dan mengendalikan proses produksi secara real time, sementara Big Data digunakan untuk menganalisis data tersebut guna mengidentifikasi potensi peningkatan efisiensi produk serta untuk menyempurnakan jadwal produksi. Pemanfaatan Big Data dan IoT membawa manfaat signifikan dalam meningkatkan efisiensi, mengurangi biaya operasional dan meningkatkan kualitas produk yang dihasilkan [4].

Di era digital yang semakin berkembang, berbagai aktivitas juga semakin meluas jangkauannya, maka itu akan memberikan ancaman baru terhadap keamanan data diri, data perusahaan dan potensi pelanggaran privasi. Diperlukannya pemahaman yang lebih mendalam mengenai praktik aman dalam penggunaan teknologi digital Keamanan data mengacu pada tindakan perlindungan yang diambil untuk mengamankan data dari akses yang tidak disetujui dan untuk menjaga kerahasiaan, integritas dan ketersediaan data. Praktik perlindungan data yang efektif mencakup teknik perlindungan data seperti enkripsi data, manajemen kunci, redaksi data, subsetting data dan penyembunyiaan data, serta control akses khusus dan hak pemantauan [5].

A. Keamanan Pengguna IoT dalam mengelola Big Data

Penggunaan Internet of Things (IoT) untuk mengumpulkan dan mengelola Big Data semakin umum digunakan di berbagai sektor industri seperti kesehatan, manufaktur, transportasi, energi, dan lainnya. IoT memfasilitasi koneksi perangkat dan sensor ke internet, menghasilkan data besar dan beragam yang kemudian dianalisis menggunakan teknologi Big Data. Keamanan dalam IoT adalah praktik yang menjaga sistem IoT agar aman, melindungi dari ancaman dan pelanggaran, serta mengidentifikasi dan mengurangi risiko. Hal ini penting untuk memastikan ketersediaan, kerahasiaan, dan integritas solusi IoT. Perhatian terhadap keamanan privasi dalam IoT juga penting karena harus diintegrasikan dengan baik.

Berikut ini adalah konsep-konsep keamanan yang penting dalam Internet of Things (IoT) yang perlu dipahami:

1. Identifikasi dan otentikasi di mana setiap perangkat harus diidentifikasi dan diautentikasi sebelum diizinkan berinteraksi dengan perangkat lain.
2. Data yang dikirim harus dienkripsi untuk menjaga kerahasiaan, sementara jaringan IoT harus dilindungi dengan firewall dan deteksi intrusi.
3. Pengelolaan akses dan otorisasi penting untuk memastikan peran yang tepat bagi pengguna dan perangkat, sementara pemantauan keamanan dan pembaruan perangkat lunak secara teratur juga krusial.
4. Perlindungan fisik perangkat keras IoT dan pengujian keamanan yang komprehensif juga diperlukan untuk mengidentifikasi dan mengatasi potensi kerentanan.

Dengan menerapkan konsep-konsep ini, keamanan IoT dapat ditingkatkan secara signifikan [6].

IV. HASIL ANALISIS DATA

Keamanan dan kerahasiaan data merupakan perhatian utama dalam era big data yang semakin berkembang. Sebagian besar pemilik dan penyedia layanan big data saat ini seringkali tidak memiliki kapasitas untuk mengelola dan menganalisis volume data yang besar tersebut. Oleh karena itu, mereka cenderung mengirimkan data tersebut ke pihak ketiga untuk diproses, namun hal ini juga dapat menimbulkan potensi masalah keamanan data sensitif tersebut. Masalah keamanan dan privasi menjadi semakin penting seiring dengan kemajuan teknologi, terutama dalam bidang seperti perbankan dan telekomunikasi yang seringkali memiliki akses langsung terhadap data pribadi pelanggan mereka. Untuk melindungi data individu, pemerintah biasanya membentuk regulasi seperti Undang-Undang Perlindungan Data dan Informasi Pribadi serta regulasi lainnya yang mengatur penggunaan dan perlindungan data secara lebih tepat. Kendati demikian, tantangan privasi data juga muncul dari pemanfaatan teknologi big data yang kurang bijaksana, yang dapat mengancam stabilitas negara dan keamanan warga negara [7] [8]. Oleh karena itu, keamanan dalam pengelolaan big data harus diperhatikan secara serius.

Berikut tantangan yang perlu diperhatikan dalam menggunakan Internet of Things (IoT) untuk mengumpulkan dan mengelola Big Data :

1. Pengumpulan data yang luas, Setiap perangkat IoT dapat mengumpulkan data tentang aktivitas pengguna, preferensi, lokasi, dan lainnya. Tantangan privasi terkait dengan bagaimana data ini dikumpulkan, digunakan, dan disimpan dengan aman.

2. Keamanan Data: Karena perangkat IoT terhubung ke internet, mereka rentan terhadap serangan siber. Jika tidak ada langkah-langkah keamanan yang memadai, data pribadi yang dikumpulkan oleh perangkat IoT bisa diakses oleh pihak yang tidak berwenang. Perlindungan data harus menjadi prioritas untuk menjaga privasi pengguna [9], [10].

3. Identifikasi Individu: Data yang dikumpulkan oleh perangkat IoT bisa mengungkap identitas individu secara langsung atau tidak langsung. Pola aktivitas sehari-hari atau informasi geografis yang dikumpulkan oleh perangkat pintar dapat mengidentifikasi kebiasaan dan rutinitas individu dengan mudah. Hal ini dapat mengancam privasi dan keamanan individu [11], [12].

4. Kontrol Pengguna: Penggunaan perangkat IoT bisa mengurangi kontrol pengguna atas data pribadi mereka. Pengguna harus dapat memahami dan mengendalikan penggunaan data mereka oleh perangkat IoT serta pihak lain dalam ekosistem IoT. Kejelasan dan transparansi dalam kebijakan privasi serta opsi untuk mengontrol pengumpulan dan penggunaan data sangat penting [13].

5. Akses Data oleh Pihak Ketiga, Data yang dikumpulkan oleh perangkat IoT dapat dibagikan dengan pihak ketiga seperti penyedia layanan atau mitra bisnis. Pembagian data ini meningkatkan risiko privasi. Diperlukan kebijakan dan persyaratan yang jelas tentang penggunaan dan pembagian data untuk menjaga privasi pengguna [14], [15].

V. KESIMPULAN

Dalam era pertumbuhan sistem informasi yang pesat, pemanfaatan Internet of Things (IoT) dan Big Data menjadi fokus utama perusahaan modern. Meskipun menawarkan manfaat yang besar, tantangan keamanan data menjadi perhatian utama dalam penggunaan IoT untuk menghimpun dan mengelola Big Data. Perlindungan data yang luas, keamanan data selama transit dan penyimpanan, identifikasi individu, kontrol pengguna, dan akses data oleh pihak ketiga adalah aspek-aspek yang perlu diperhatikan dengan serius. Integrasi yang seimbang antara teknologi IoT, Big Data, dan praktik keamanan data menjadi kunci untuk menghadapi risiko serangan siber, pelanggaran privasi, dan kerentanan sistem. Hasil analisis menjelaskan bahwa tantangan keamanan data yang terkait dengan penggunaan IoT untuk mengelola Big Data ialah pengumpulan data yang luas, keamanan data, identifikasi individu, kontrol pengguna, akses data oleh pihak ketiga. Oleh karena itu, upaya perlindungan data yang efektif melalui teknik-teknik keamanan seperti enkripsi, manajemen akses, dan pemantauan secara teratur menjadi sangat penting dalam memastikan keberhasilan dan keberlanjutan bisnis di era digital ini.

REFERENSI

[1] Eka Mayasari and Agussalim Agussalim, “Literature Review: Big Data dan Data Analys pada Perusahaan,” *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 3, pp. 171–187, 2023, doi: 10.55606/juisik.v3i3.680.

[2] Edy Soesanto, Nova Astia Ningsih, Lili Khoerunisa, and Muhammad Ilham Faturrahman, “Keamanan Informasi Data Dalam Pemanfaatan Teknologi Informasi Pada PT Bank Central Asia (BCA),” *Student Res. J.*, vol. 1, no. 3, pp. 227–238, 2023, doi: 10.55606/srjyappi.v1i3.334.

[3] D. J. Sengkey, P. Deniyanti Sampoerno, and T. A. Aziz, “Kemampuan Pemahaman Konsep Matematis: Sebuah Kajian Literatur,” *Griya J. Math. Educ. Appl.*, vol. 3, no. 1, pp. 67–75, 2023, doi: 10.29303/griya.v3i1.265.

[4] S. A. Putri, Y. Nabela, M. Arifan, R. Hidayat, and M. Ikaningtyas, “Optimalisasi Proses Operasional dengan Menggabungkan Teknologi IoT dan Big Data : Studi Kasus pada PT Pertamina dalam Industri Minyak dan Gas Operational Process Optimization by Combining IoT and Big Data Technology : A Case Study on PT Pertamina in the O,” vol. 3, no. 1, pp. 1–10, 2024.

[5] S. Ceri, “Data-Centric Systems and Applications Series editors”.

[6] F. Prasetyo Eka Putra, S. Mellyana Dewi, and A. Hamzah, “Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi,” vol. 5, no. 2, pp. 26–32, 2023, doi: 10.37034/jsisfotek.v5i1.232.

[7] N. S. Nainggolan and I. P. Nasution, “Pentingnya Keamanan Big Data Dalam Lembaga Pemerintahan Di Era Digital,” *J. Sains dan Teknol.*, vol. 3, no. 2, pp. 253–257, 2023, doi: 10.47233/jsit.v3i2.883.

[8] Y. Daeng, J. Levin, M. Razzaq Prayudha, N. Putri Ramadhani, S. Imanuel, and A. Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng, “Analisis Penerapan Sistem Keamanan Siber TerhadapKejahatan Siber Di Indonesia,” *J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 1135–1145, 2023.

[9] R. Rizal, N. Widiyasono, and S. Yuliyanti, “Kecerdasan Buatan untuk Klasifikasi Serangan Siber pada Internet of Things Network Traffic,” *Jumanji*, vol. 7, no. 2, pp. 2598–8069, 2023.

[10] R. Pratama Putra *et al.*, “Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi,” *Innov. J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 2898–2905, 2023, [Online]. Available: https://j-innovative.org/index.php/Innovative/article/view/6662

[11] J. Manurung, A. P. E. Sihombing, and B. Pandiangan, “Sosialisasi Dan Edukasi Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat,” *J. Pengabdi. Masy. Nauli*, vol. 2, no. 1, pp. 1–7, 2023, [Online]. Available:

https://ejournal.marqchainstitute.or.id/index.php/Nauli/article/view/103

[12] Khoiri Gusnanda, Nur Ulfadillah, and Titin Sumarni, "Struktur Basis Data Di Era Digital (Implementasi Pengamanan Basis Data Di Era Global)," *J. Sains dan Teknol.*, vol. 3, no. 7, pp. 100–111, 2024, [Online]. Available: https://ejournal.warunayama.org/kohesi

[13] H. W. Saputra and I. Komputer, "Penerapan kecerdasan buatan dalam pengujian perangkat lunak," vol. 1, no. 2, pp. 1–16, 2024.

[14] D. Natalia and A. A. Sudiro, "Anak yang Menjadi Korban/Pelaku/Saksi; Pelindungan anak; Hak-Hak anak," vol. 5, no. 1, 2024.

[15] T. G. Laksana and S. Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *J. Ilm. Multidisiplin*, vol. 3, no. 01, pp. 109–122, 2024, doi: 10.56127/jukim.v3i01.1143.

MADINAVERSE: Jurnal Informatika, IoT dan Games
Vol. 1, No. 1, Desember 2024

Sistem Prediksi Kelulusan Ujian Sertifikasi IT Dengan Metode Waterfall

Maulana Firmansyah[1*)], Nuciko Abdul Halim[2] , Imelda Imelda[3]
[1,2,3]Program Studi Magister Ilmu Komputer, Fakultas Teknologi Informasi, Universitas Budi Luhur
Email: [1]2311602060@student.budiluhur.ac.id, [2]2311601021@student.budiluhur.ac.id, [3]imelda@budiluhur.ac.id

Abstrak - Penelitian ini bertujuan mengembangkan sistem prediksi kelulusan ujian sertifikasi IT untuk meningkatkan kepercayaan diri peserta ujian dan mengidentifikasi peserta yang membutuhkan pelatihan tambahan di PT Brainmatics. Masalah muncul karena seringnya peserta yang kurang percaya diri untuk memulai sertifikasi dilain sisi banyak yang tidak lulus karena terlalu percaya diri yang akan mempengaruhi rating dari Brainmatics, dari masalah ini muncul tantangan untuk bagaimana memanfaatkan data historis secara efektif guna menghasilkan prediksi yang akurat dan mendukung peserta kurang percaya diri agar lebih siap menghadapi ujian. Penelitian menggunakan metode Waterfall karena pendekatannya yang sistematis dan terstruktur. Sistem prediksi ini memanfaatkan variabel seperti latar belakang pendidikan, pengalaman kerja, dan hasil tes sebelumnya. Tahapan pengembangan meliputi analisis kebutuhan, desain sistem, implementasi, pengujian, dan pemeliharaan. Hasil menunjukkan sistem mampu memberikan prediksi akurat dengan tingkat keandalan tinggi. Sistem ini membantu institusi pelatihan PT Brainmatics untuk mengidentifikasi peserta yang membutuhkan dukungan tambahan, serta meningkatkan kualitas pelatihan dan ujian sertifikasi IT.

Kata kunci: Sertifikasi IT, Waterfall, Sistem Prediksi

Abstract - This study aims to develop a prediction system for IT certification exam success to boost candidates' confidence and identify participants who require additional training at PT Brainmatics. The main issue is how to effectively utilize historical data to produce accurate predictions and support less confident participants in better preparing for the exam. The study employs the Waterfall method due to its systematic and structured approach. The prediction system utilizes variables such as educational background, work experience, and previous test results. The development stages include needs analysis, system design, implementation, testing, and maintenance. The results show that the system provides accurate predictions with a high degree of reliability. This system assists PT Brainmatics training institutions in identifying participants who need additional support and improving the quality of IT training and certification exams

Keywords: IT Certification, Waterfall, Prediction System

I. PENDAHULUAN

Di era digital yang berkembang pesat, sertifikasi dalam bidang Teknologi Informasi (IT) menjadi kunci untuk meningkatkan kompetensi dan kualifikasi sumber daya manusia. PT. Brainmatics Indonesia Cendekia, sebagai penyelenggara ujian sertifikasi IT, dihadapkan pada tantangan mengelola proses ujian secara efektif dan efisien sehingga meningkatkan rating kelulusan yang tinggi. Proses ini meliputi persiapan, penjadwalan, dan evaluasi peserta ujian yang mempengaruhi keberhasilan mereka dalam meraih kelulusan dalam sertifikasi, sehingga meningkatkan rating Brainmatics. Namun, pengelolaan yang efektif masih menghadapi kendala dalam memprediksi kelulusan peserta ujian berdasarkan faktor-faktor yang memengaruhi, seperti latar belakang pendidikan dan pengalaman kerja [1].

Penelitian ini bertujuan untuk mengembangkan sistem prediksi kelulusan ujian sertifikasi IT menggunakan metode *Waterfall* [2], [3]. Metode *Waterfall* dipilih karena pendekatannya yang terstruktur, memungkinkan pengembangan sistem secara bertahap dari analisis kebutuhan hingga implementasi. Pertanyaan penelitian utama meliputi bagaimana implementasi sistem prediksi dapat meningkatkan efisiensi pengelolaan ujian sertifikasi dan seberapa akurat sistem ini dalam memprediksi kelulusan peserta berdasarkan faktor-faktor yang relevan [4].

Manfaat dari penelitian ini adalah memberikan kontribusi dalam meningkatkan efisiensi dan akurasi proses pengelolaan ujian sertifikasi IT, serta memberikan pedoman bagi penyelenggara ujian untuk mengambil keputusan yang lebih tepat dalam persiapan, penjadwalan, dan evaluasi ujian. Dengan demikian, diharapkan penelitian ini dapat mendukung upaya PT. Brainmatics Indonesia Cendekia dalam meningkatkan kualitas layanan sertifikasi IT di Indonesia.

PT. Brainmatics Indonesia Cendekia, sebagai penyelenggara ujian sertifikasi IT, menghadapi kesulitan dalam memprediksi kelulusan peserta ujian dengan tepat. Tantangan ini muncul dari pengelolaan data yang kompleks terkait faktor-faktor yang mempengaruhi keberhasilan, seperti latar belakang pendidikan, pengalaman kerja, dan hasil tes sebelumnya. Saat ini belum ada sistem yang membantu menganalisis data ini secara efisien untuk memberikan gambaran akurat tentang peluang kelulusan peserta.

Rumusan masalah pada penelitian ini bagaimana sistem prediksi kelulusan ujian sertifikasi IT dapat dikembangkan dengan pendekatan Waterfall untuk meningkatkan efisiensi dan akurasi pengelolaan data peserta. Seberapa efektif sistem yang dikembangkan dalam memberikan prediksi akurat mengenai kelulusan peserta ujian sertifikasi berdasarkan faktor-faktor yang relevan.

Dalam rangka menghadapi kompleksitas dan kedalaman sebuah penelitian, peneliti menggunakan tiga pendekatan metodologis yang berbeda, yaitu studi pustaka, observasi, dan wawancara. Metode studi pustaka dilaksanakan dengan melakukan pengumpulan data dan informasi dari berbagai sumber bacaan terpercaya, termasuk buku referensi dan literatur daring yang relevan, yang bertujuan sebagai fondasi utama dalam menyusun kerangka teoretis dan konseptual dalam penulisan karya ilmiah ini. Sementara itu, metode observasi melibatkan proses sistematis dalam mengumpulkan data primer dengan melakukan pengamatan langsung terhadap objek atau fenomena yang menjadi fokus penelitian. Pendekatan ini memungkinkan peneliti untuk memperoleh pemahaman yang mendalam mengenai perilaku dan karakteristik objek yang diamati, serta memberikan gambaran yang akurat terhadap dinamika yang terjadi di lapangan. Selain itu, metode wawancara diimplementasikan sebagai bentuk komunikasi langsung yang mengutamakan interaksi personal antara peneliti dan subjek penelitian. Melalui pola tanya-jawab yang terstruktur, metode ini memfasilitasi proses pengumpulan data yang lebih mendalam mengenai pengalaman, pandangan, dan persepsi subjek terkait isu yang sedang diselidiki. Dengan memanfaatkan ketiga pendekatan metodologis ini secara terpadu, diharapkan peneliti dapat menghasilkan pemahaman yang lebih holistik dan komprehensif terhadap fenomena yang diteliti, serta mendorong terwujudnya kesimpulan yang lebih kuat dan berbasis bukti dalam penulisan karya ilmiah ini [5].

Untuk mendukung penelitian ini, berikut hasil penelitian yang menjadi acuan. Penelitian oleh Pangestuti dengan judul Rancang Bangun Sistem Pendukung Keputusan Penerimaan Karyawan Baru Menggunakan Metode Naïve Bayes Classifier. Hasil dari penelitian ini adalah Sistem pendukung keputusan sebagai alat bantu dalam mengambil keputusan menggunakan metode Naïve Bayes yang diimplementasikan untuk pengambilan keputusan penerimaan karyawan baru [6]. Penelitian oleh Hastuti dengan judul Sistem Pendukung Keputusan Pemilihan Jurusan Siswa dengan Metode Naïve Bayes pada SMK Negeri 2 Karanganyar. Hasil dari penelitian ini adalah Sistem pendukung keputusan menggunakan metode Naïve Bayes mampu membantu siswa dalam menentukan jurusan siswa yang sesuai dengan kompetensi dan bidang yang dikuasai oleh siswa [7].

II. METODE PENELITIAN

Gap dari penelitian sebelumnya terbagi menjadi beberapa bagian:

A. Pendekatan Metodologi

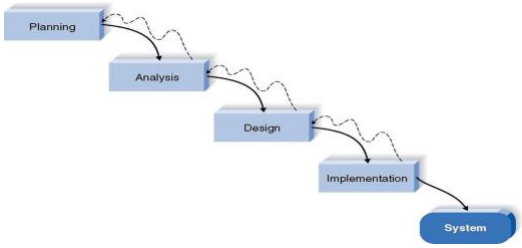
1. Penelitian Sebelumnya: Sebagian besar penelitian sebelumnya, seperti oleh Pangestuti (2020) dan Hastuti (2016), menggunakan metode *Naïve Bayes* untuk sistem pendukung keputusan dalam konteks penerimaan karyawan baru atau pemilihan jurusan siswa. Metode ini berfokus pada klasifikasi probabilistik untuk membantu pengambilan keputusan.
2. Penelitian Saat Ini: Penelitian ini menggunakan metode Waterfall, yang merupakan pendekatan terstruktur dalam pengembangan perangkat lunak. Fokusnya adalah pada proses pengembangan bertahap mulai dari analisis kebutuhan, desain, implementasi, pengujian, hingga pemeliharaan untuk menciptakan sistem prediksi kelulusan ujian sertifikasi IT [8].

B. Tujuan dan Konteks Aplikasi

1. Penelitian Sebelumnya: Penelitian sebelumnya bertujuan untuk mengembangkan sistem pendukung keputusan dalam konteks yang berbeda, seperti membantu proses penerimaan karyawan atau pemilihan jurusan siswa.
2. Penelitian Saat Ini: Fokus penelitian ini adalah pada pengembangan sistem prediksi kelulusan ujian sertifikasi IT untuk membantu PT. Brainmatics Indonesia Cendekia dalam mengelola dan memprediksi kelulusan peserta ujian, dengan tujuan meningkatkan efisiensi dan efektivitas pengelolaan ujian [9].

C. Metode Pengembangan Sistem

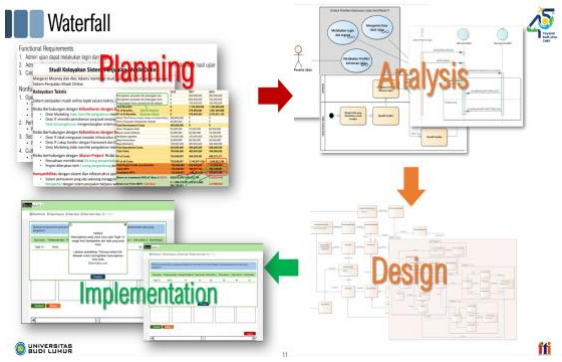
1. Penelitian Sebelumnya: Beberapa penelitian sebelumnya tidak menekankan metode pengembangan sistem secara rinci. Sebagian besar hanya mencakup implementasi algoritma klasifikasi seperti *Naïve Bayes*.
2. Penelitian Saat Ini: Penelitian ini mengadopsi metode Waterfall secara menyeluruh untuk memastikan bahwa setiap tahapan pengembangan dilakukan secara sistematis. Ini memberikan keunggulan dalam dokumentasi yang lengkap dan pemeliharaan sistem yang lebih mudah di masa mendatang.



Gambar 1. Tahapan Metode Waterfall

Waterfall adalah metodologi pengembangan perangkat lunak yang menggunakan pendekatan linear dan berurutan, di mana setiap tahap dalam proses pengembangan harus selesai sebelum melanjutkan ke tahap berikutnya [10]. Tahapan dalam model Waterfall umumnya meliputi:

1. Requirements (Analisis Kebutuhan),
2. Design (Desain),
3. Implementation (Implementasi/Koding),
4. Testing (Pengujian),
5. Deployment (Penerapan),
6. Maintenance (Pemeliharaan).



Gambar 2. Skema Metode Waterfall

Metode Waterfall digunakan karena:

1. Sederhana dan mudah diikuti: Cocok untuk proyek dengan lingkup dan kebutuhan yang jelas.
2. Dokumentasi yang baik: Setiap tahap menghasilkan dokumentasi yang komprehensif, membantu dalam memahami dan mengelola proyek.
3. Cocok untuk proyek kecil atau stabil: Digunakan ketika persyaratan sudah jelas dan jarang berubah selama siklus proyek.
4. Minim risiko: Pendekatan ini meminimalkan ketidakpastian dengan mendefinisikan semuanya di awal.

Metode Waterfall digunakan untuk:

1. Proyek dengan kebutuhan yang jelas dan tetap: Seperti sistem internal perusahaan atau perangkat lunak dengan spesifikasi yang tidak akan berubah.
2. Proyek yang memerlukan kepatuhan ketat: Seperti aplikasi untuk sektor kesehatan, keuangan, atau pemerintahan, yang membutuhkan dokumentasi dan kontrol proses yang ketat.
3. Tim pengembang dengan pengalaman terbatas dalam pengembangan iteratif: Model ini cocok untuk tim yang lebih nyaman dengan pendekatan tradisional dan kurang fleksibel.

D. Fokus Output Penelitian

1. Penelitian Sebelumnya: Output penelitian sebelumnya biasanya berupa sistem atau prototipe yang membantu proses klasifikasi dan pengambilan keputusan untuk kasus tertentu, seperti penentuan penerimaan karyawan atau pemilihan jurusan.
2. Penelitian Saat Ini: Output dari penelitian ini adalah sistem prediksi yang dirancang khusus untuk memprediksi kelulusan ujian sertifikasi IT. Sistem ini tidak hanya memanfaatkan data historis peserta, tetapi juga mengintegrasikan hasil analisis untuk memberikan prediksi dengan akurasi tinggi, yang berbeda dari sekadar alat klasifikasi sederhana [5].

E. Tujuan Penelitian

Tujuan penelitian dalam dokumen ini adalah untuk mengembangkan dan mengimplementasikan sistem prediksi kelulusan ujian sertifikasi IT di PT. Brainmatics Indonesia Cendekia menggunakan metode *Waterfall*. Tujuan ini mencakup:

1. Meningkatkan efisiensi dan efektivitas pengelolaan ujian sertifikasi, termasuk persiapan, penjadwalan, dan evaluasi ujian.
2. Menyediakan sistem prediksi kelulusan yang akurat berdasarkan data historis dan faktor-faktor terkait, seperti latar belakang pendidikan dan pengalaman kerja.
3. Membantu penyelenggara ujian dalam membuat keputusan yang lebih tepat terkait dukungan tambahan yang dibutuhkan peserta untuk meningkatkan peluang kelulusan.
4. Memastikan setiap tahap pengembangan sistem dilakukan secara sistematis dan terdokumentasi dengan baik, sesuai dengan prinsip metode *Waterfall*, untuk mempermudah pemeliharaan dan pengembangan di masa depan [11].

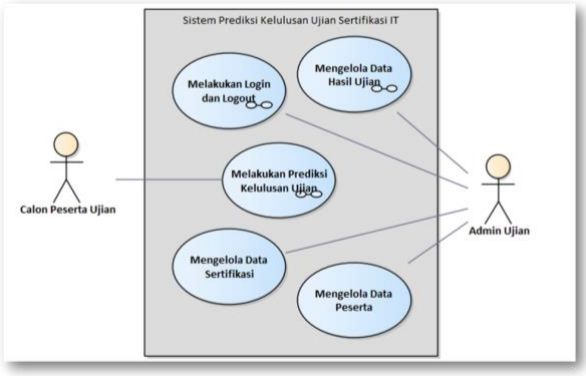
III. HASIL DAN DISKUSI

Penelitian ini terkait dengan rancangan sistem pendukung keputusan untuk manajemen ujian sertifikasi dengan menggunakan metode *waterfall*. Aplikasi ini memiliki potensi yang signifikan untuk meningkatkan efisiensi dan

akurasi dalam proses seleksi, dengan tujuan memperkirakan peluang keberhasilan peserta ujian. Aplikasi ini diharapkan dapat memberikan bantuan berharga bagi PT Brainmatics Indonesia Cendekia dalam mengelola data peserta ujian, sekaligus memprediksi peluang kelulusan peserta tersebut.

Use case Diagram yang Dirancang

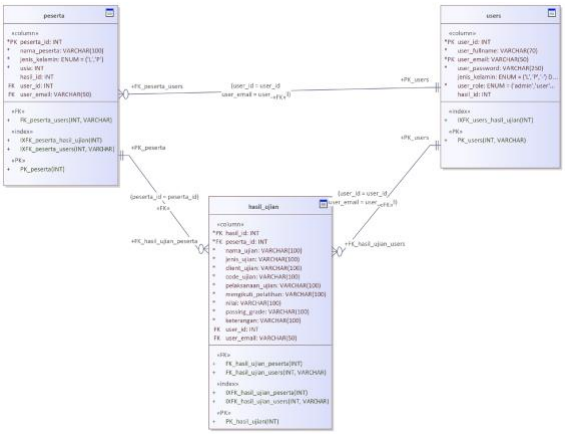
Use Case Diagram digunakan untuk mengilustrasikan sistem dari perspektif pengguna sistem tersebut. Oleh karena itu, pembuatan Diagram Kasus Pengguna lebih menekankan pada fungsionalitas yang terdapat dalam sistem, bukan pada urutan atau alur peristiwa. *Use Case Diagram* memvisualisasikan interaksi antara aktor dan system [12], [13].



Gambar 3. Use case Diagram Sistem Prediksi Kelulusan Ujian Sertifikasi IT

Data Model Diagram* Sistem Pendukung Keputusan Pengelolaan Ujian Sertifikasi Menggunakan Metode *Waterfall

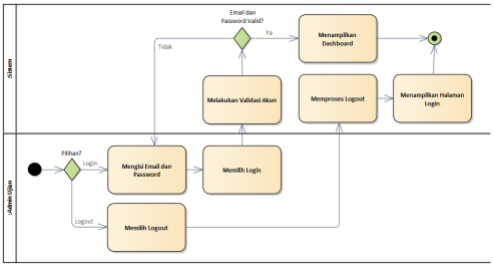
Normalisasi adalah suatu alat yang digunakan untuk mengelompokkan data ke dalam tabel-tabel yang menggambarkan entitas dan relasinya. Ini adalah teknik yang mengadopsi pendekatan bottom-up untuk membantu mengidentifikasi hubungan di antara data. (Indrajani, 2015).



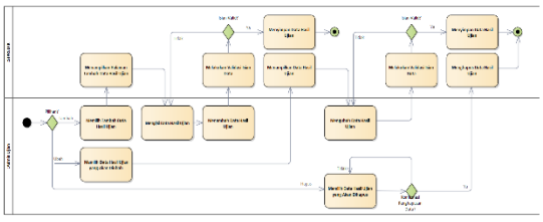
Gambar 4. Data Management Layer Design Sistem Prediksi Kelulusan Ujian Sertifikasi IT

Activity Diagram

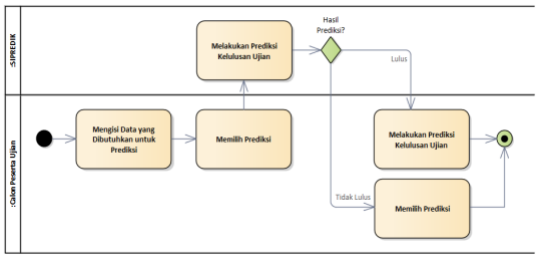
Activity Diagram berguna untuk memaparkan urutan aliran aktivitas, digunakan untuk menjelaskan aktivitas yang terbentuk dalam sebuah operasi, yang pada gilirannya dapat diterapkan juga pada aktivitas lainnya [14]. Diagram ini memiliki kemiripan dengan *flowchart* karena merencanakan alur kerja dari satu aktivitas ke aktivitas atau status lainnya. Membuat *Activity Diagram* pada tahap awal pemodelan proses dapat mendukung pemahaman menyeluruh terhadap proses tersebut. *Activity Diagram* juga berguna untuk menggambarkan interaksi antara beberapa kasus pengguna (*use case*). Contoh pemodelan *Activity Diagram* dapat dilihat pada Gambar 5.



Gambar 5. Activity Diagram Melakukan Login dan Logout



Gambar 6. Activity Diagram Mengelola Data Hasil Ujian

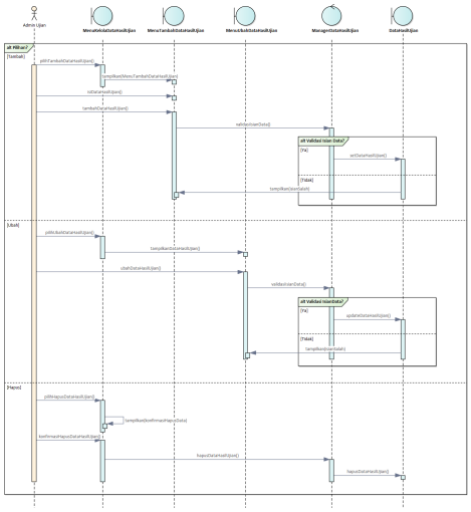


Gambar 7. Activity Diagram Melakukan Prediksi Kelulusan Ujian

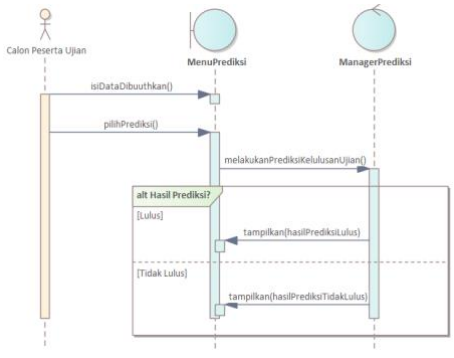
Sequence Diagram

Menggambarkan interaksi antara sejumlah objek dalam urutan waktu [15]. Kegunaannya untuk menunjukkan rangkaian pesan yang dikirim antara objek juga interaksi antar objek yang terjadi pada titik tertentu dalam eksekusi sistem.

Contoh pemodelan *Sequence Diagram* dapat dilihat pada Gambar 8.

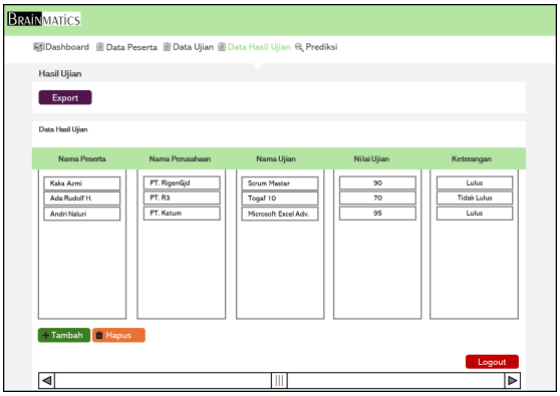


Gambar 8. Sequence Diagram Mengelola Data Hasil Ujian



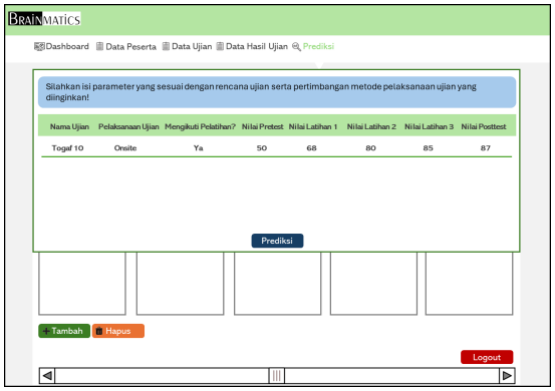
Gambar 9. Sequence Diagram Melakukan Prediksi Kelulusan

Tampilan Layar



Gambar 10. Mengelola Data Hasil Ujian

Pada tampilan Data Hasil Ujian berisi data peserta yang telah atau sudah mendaftar ujian sehingga data peserta dan juga nilai dari peserta dapat dilihat dan diakses oleh Admin.



Gambar 11. Melakukan Prediksi Kelulusan Ujian

Pada Tampilan Prediksi kelulusan berisikan pop up yang dapat diisi oleh peserta ujian untuk dapat melakukan prediksi kemungkinan kelulusan ujian dengan mengisi data yang ada.

Gambar 12. Melakukan Prediksi Kelulusan Ujian – Lulus

Pada Tampilan Lulus menampilkan informasi hasil apabila peserta ujian berkemungkinan untuk lulus dalam ujian yang akan diikuti mendatang.

Gambar 13. Melakukan Prediksi Kelulusan Ujian - Tidak Lulus

Pada tampilan Tidak Lulus menampilkan informasi hasil apabila peserta ujian berkemungkinan tidak lulus dalam ujian yang akan diikuti mendatang.

IV. KESIMPULAN

Sistem prediksi kelulusan ujian sertifikasi IT yang dikembangkan menggunakan metode Waterfall di PT. Brainmatics Indonesia Cendekia telah berhasil merancang tahap awal yang mendukung peningkatan efisiensi dan efektivitas dalam pengelolaan ujian sertifikasi. Analisis kebutuhan dan desain sistem yang telah dilakukan memberikan kerangka kerja yang kokoh untuk fase implementasi dan pengujian yang akan datang. Meskipun sistem belum sepenuhnya diimplementasikan, perencanaan yang sistematis dan terstruktur ini diharapkan akan memfasilitasi pengambilan keputusan yang lebih tepat dalam persiapan, penjadwalan, dan evaluasi ujian, sehingga memperkuat kapabilitas PT. Brainmatics dalam mengelola proses sertifikasi dengan lebih efektif. Keberhasilan dalam tahap pengembangan ini menunjukkan potensi yang signifikan untuk mencapai tujuan utama penelitian.

REFERENSI

[1] Brainmatics, “Brainmatics: The School of Computing,” Brainmatics.id. [Online]. Available: https://brainmatics.id/wp-content/uploads/2025/01/brainmatics-curricula.pdf

[2] F. Febrianto, I. F. N. Aziz, M. A. Kosim, M. Darwis, and R. Hendrowati, “Implementation of The Resident’s Dues Applications (SIUMAS) Using Waterfall Method in RT X Cinere Village,” *JISA(Jurnal Inform. dan Sains)*, vol. 6, no. 2, pp. 137–142, 2023, doi: 10.31326/jisa.v6i2.1766.

[3] R. A. Maulana, M. A. Fatih, L. A. Suto, and M. Darwis, “Development of Paramadina Roomhub Application As Room Booking System Using Waterfall Method,” vol. 07, no. 02, pp. 176–185, 2024.

[4] B. Setiadi, “Aplikasi Monitoring Keuangan Bagian Operasional Di Starindo Berbasis Web,” *J. Ind. Eng. Oper. Manag.*, vol. 4, no. 1, 2021, doi: 10.31602/jieom.v4i1.5437.

[5] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan r&d*. Bandung: Alfabeta, 2018.

[6] T. D. Pangetuti, “RANCANG BANGUN SISTEM PENDUKUNG KEPUTUSAN PENERIMAAN KARYAWAN BARU MENGGUNAKAN METODE NAIVE BAYES CLASSIFIER,” UPN Veteran Jawa Timur, 2020.

[7] D. Hastuti, “SISTEM PENDUKUNG KEPUTUSAN PEMILIHAN JURUSAN SISWA DENGAN METODE NAÏVE BAYES PADA SMK NEGERI 2 KARANGANYAR,” STMIK Sinar Nusantara Surakarta, 2016.

[8] I. Solikin and S. Hardini, “Aplikasi Forecasting Stok Barang Menggunakan Metode Weighted Moving Average (WMA) pada Metrojaya Komputer,” *J. Inform. J. Pengemb. IT*, vol. 4, no. 2, pp. 100–105, 2019, doi: 10.30591/jpit.v4i2.1373.

[9] L. Muflikhah, W. L. Yunita, and M. T. Furqon, “Prediksi Nilai Mata Kuliah Mahasiswa Menggunakan Algoritma K-Apriori,” *Sisfo*, vol. 06, no. 02, pp. 157–172, 2017, doi: 10.24089/j.sisfo.2017.01.001.

[10] R. S. Pressman, *Software Engineering: A Practitioner’s Approach 8e.*, 8th ed. New York: McGraw-Hill, 2015.

[11] A. Solichin, *Pemrograman Web dengan PHP dan MySQL*. Jakarta: Budi Luhur, 2016.

[12] W. Wulandari, “Implementasi Sistem Peramalan Persediaan Barang Menggunakan Metode Moving Average,” *J. Media Inform. Budidarma*, vol. 4, no. 3, p. 707, 2020, doi: 10.30865/mib.v4i3.2199.

[13] C. Djaoui, E. Kerkouche, K. Khalfaoui, and A. Chaoui, “A graph transformation approach to generate analysable maude specifications from UML interaction overview diagrams,” *Proc. - 2018 IEEE 19th Int. Conf. Inf. Reuse Integr. Data Sci. IRI 2018*, pp. 511–517, 2018, doi: 10.1109/IRI.2018.00081.

[14] N. Musthofa and M. A. Adiguna, “Perancangan Aplikasi E-Commerce Spare-Part Komputer Berbasis Web Menggunakan CodeIgniter Pada Dhamar Putra Computer Kota Tangerang,” *OKTAL J. Ilmu Komput. dan Sains*, vol. 1, no. 03, pp. 199–207, 2022.

[15] A. Khalfani *et al.*, “Development of Book Nook Online Bookstore Application With,” vol. 11, no. 1, pp. 50–59, 2024.