JOMCOM

Journal of Millimeterwave Communication, Optimization and Modelling

Volume: 4
Issue: 1
Year: 2024
ISSN: 2791-92-93

editor in chief
Assoc. Prof. M. Tahir GUNESER

CONTENT

About the Journal

Journal of Millimeterwave Communication, Optimization and Modelling (JOMCOM) is an international on-line and refereed journal published 2 times a year (June and December) in English. Journal of Millimeterwave Communication, Optimization and Modelling (JOMCOM) published its first issue in 2021 and has been publishing since 2021. Manuscripts in JOMCOM Journal reviewed of at least 2 referees among the referees who have at least doctorate level in their field.

Journal of Millimeterwave Communication, Optimization and Modelling (JOMCOM) is an international online journal that is published 2 times in a year in English.

The purpose of JOMCOM is publishing the scientific research in various fields of communication.

All kinds of transactions and the application about the journal can be made from **https://jomcom.org**

The scientific responsibility of articles belongs to the authors.

ISSN: 2791-9293

Editor in Chief:

Assoc. Prof. Dr. Muhammet Tahir GÜNEŞER

Karabük University

Faculty of Engineering

Department of Electrical and Electronics Engineering

Head of Communication Division

Karabük, TURKEY

jomcomeditor@gmail.com

PUBLISHER

Assoc. Prof. Muhammet Tahir GÜNEŞER

Aims & Scope

Communication Technologies: Journal of Millimeter-wave Communication, Optimization and Modelling (JOMCOM) publishes original research and review articles in Communication Technologies, Innovative Technologies, and Systems in the broad field of Information-Communication Technology. Purpose of JOMCOM; To create value in the field by publishing original studies that will contribute to the literature in wireless communication sciences and be a resource for academia and industrial application whole over the world. Besides, JOMCOM aims to bring the valuable work of researchers working in Communication studies to a broader audience at home and abroad. Readership of JOMCOM; valuable representatives of the wireless communication area, especially those who do academic studies in it, and those who do academic studies about modelling and system design and other interested parties. Since JOMCOM will appeal to a broader audience in article submissions, it prioritizes studies prepared in English.

Optimization and Modelling: Journal of Millimeter-wave Communication, Optimization and Modelling (JOMCOM), within the scope of Wireless Communication Sciences, publishes articles on communication theory and techniques, systems and networks, applications, development and regulatory policies, standards, and management techniques. It also reports experiences and experiments, best practices and solutions, lessons learned, and case studies. Additional studies on System Design, Modelling and Optimization. Subject areas of interest covered in the journal include the following but are not limited to:

5G-6G Technologies

Circuits for Optical Communication Systems

Antenna Design

Communication Design Materials

Fiber Optic Communication

Innovative Designs for Communications

Integrated Circuits for Communications

Optimization Methods on Engineering

Realization of Antenna Systems

Realization of Microwave, Radar, and Sonar Systems

RF Circuits

System Design

Visible Light Communication

Wireless Communication

Criminal Exploitation of Information and Communication Technologies: Riots

Received: 31 February 2023; Accepted: 6 March 2023 *Research Article*

Murad M. Madzhumayev
Department of Criminal Law, Criminal Procedure and Criminalistics of Law Institute
Peoples' Friendship University of Russia (RUDN University)
Moscow, Russian Federation
murad.mad@outlook.com
0000-0003-3332-2850

***Abstract*—The availability, reliability, security of information and telecommunication networks and systems constitute crucial pillars for enhancing standards of living, employment, business and civil society organizations, augmenting their activities and realizing the economic potential of the nation.**

The paper addresses the implications of information and communication technologies (ICTs) in the organization, coordination, and perpetration of violent unrest. With global trends in ICT developments and the digital population of the world in mind, it analyses their significance in certain phases of unrest.

The results and conclusions stated in the article are reached based on philosophical and ideological, general scientific and special scientific methods and approaches of research: dialectical, formal-logical (analysis and synthesis, induction, and deduction), synchronous comparative legal method and others.

An examination of the use of ICTs during a violent riot emphasizes the following variations of their utilization: a) informational interaction, communication, incitement; b) mobilization of crowd; c) organization of riots; d) allocation of roles; e) coordination.

As of today, an imminently significant challenge arises out from the criminal liability of internet service providers. The dissemination of information on the Internet involves, in addition to the author himself, other entities, in particular the owner of the network information resource, the owner of the server, etc.

Accordingly, the liability of ISPs for failure to restrict access to information containing advocacy, incitement, recruitment or other involvement in the commission of acts of mass unrest on the part of Internet users arises only if they are aware of the social danger of not restricting access to such information, anticipate the dangerous consequences of mass unrest as a direct consequence of such failure and, in so doing, knowingly direct their intellectual and physical efforts towards it.

Keywords—information and communication technologies, riots, organization of riots, incitement to riot, intermediary liability, internet service providers, mob assembly.

I. INTRODUCTION

Security is essential in all aspects of everyday life: technical, biological, political, economic, social, territorial, and so on. It is critical not only to accurately describe this idea, concept, and its derivatives, but also to appropriately use them for their intended purpose.

From this perspective, the state of security can be defined as the defense capability from internal and external threats targeted at national interests, i.e. ensuring the rights and legal interests of individuals, society, the state, and the sustainable development of urban and human settlements.

All communication networks, databases, and information sources have so far been integrated to form cyberspace [1].

Under the context of cybersecurity, it is feasible to identify both the vulnerability posed by this new place/space and the behaviors or processes aimed to make it (more) safe [1]. It is a combination of actions and methods, both technological and non-technical, aimed at safeguarding the bioelectrical environment and the data it stores and conveys from all potential dangers [1]. This very desirable outcome has yet to be realized.

This paper reveals precisely the non-technical measures of cyber security.

Delinquency, crime are de facto objective phenomena in the course of which human behavior unfolds in the spatial and temporal aspects of the interaction of the individual (motor and mental activity) with the environment. It affects the combination of subjective and objective factors (phenomena and processes) of that reality [2]. The offender, the victim of a crime (the object of assault); the circumstances of its commission; as well as the real-life situation of a crime comprise a crime mechanism, the essence of which is expressed in the functional-activity qualities of the system of these elements and the regularity of their interaction [2].

Often criminals exploit objects and realities in the course of their criminal acts. Rationale behind this may be the desire of the offender to simplify the commission of the crime, or rather to gain a mechanical/machine advantage in the commission of the crime.

II. THE INFORMATION SOCIETY

The information society is an environment that generates publicly available information and/or knowledge that individuals can use and/or share with the aim of pursuing their own sustainable enhancement potential to improve their standard of living within legal limits.

There are several definitions of the information society in the specialist literature, based on its key features. The most important three of them will be given here.

Y. Masuda, a Japanese sociologist, who is credited as one of the founders of the concept in question, argues that in the information society the central function will be digital values, while material values will remain in the periphery [3]. The fundamental nature of the infrastructure of "computopia", as he called the information society, applies to the main source

of information production. Information utility illustrates the predominance of knowledge capital over material capitals [3].

On the contrary, D. Bell, the American sociologist referred to the information society as the "post-industrial society". He described theoretical knowledge as its fundamental nucleus. The codification of theoretical knowledge, he argued, was a source of innovation and social change [4].

An alternative approach was adopted by F. Webster, who defined the information society by classifying it into groups: the technological aspect; the economic aspect; the work-related aspect; the spatial aspect; and the cultural aspect.

The scale of technological innovation is considered an indicator of the formation of the information society, which should lead to social transformation because of the significant impact on society [5].

The economic dimension represents the intensification of the value of information activity in the economy. A positive index in the gross national product of the information business will determine the logical conclusion of the achievement of the information economy [5]. In the employment-related parameter, the information society indicator is the predominant number of people working in the information field. The emergence of white-collar workers to replace manual work, the growth of employment in the service sector and the decline in production are clear evidence of this [5]. In the spatial criterion, the fundamental emphasis is on information networks, and they can subsequently influence the organization of time and space. Tools functioning on the national, transnational, and global level, equipping the "ring of information highway" in the presence of appropriate techniques allows us to imagine a "conductive society" [5].

Television, radio stations, cinematography, books, magazines, posters, billboards, shop window signs, personal computers, audio accessories, Internet access and hand-held computers demonstrate the uninterrupted spread of this field, which allows us to speak of information in a cultural dimension. At the same time, these factors can be considered as tools of the information society. The presented points to the media-loaded society in which we live, and the new media all surrounds us [5]. Throughout the Age of Enlightenment, the public sphere was linked to the development of bourgeois literature. While by the twentieth century the media had taken the place of bourgeois literature [6]. In the 21st century, the autonomous citizenry was conceived as the ideal of an enlightened citizen, digitally networked and discussing issues of collective interest [7]. It can be assumed that the traditional public sphere tends to move to the Internet, evidence of which is the plurality and opposition of the digital arena to the "central public sphere" dominated by state, corporate and establishment power. This inclination towards an alternative public sphere can be explained by the open and free communicative nature of the digital public sphere, which is represented or supported online from websites to social networking sites, weblogs, and microblogs [8].

III. The Public Legal Sphere (Digital Population)

Staying inseparable from the public sphere since its early conceptualization, the media play a central role in public debates, both in more traditional forms and in new forms enhanced by digital technologies. The transformation of the media paradigm introduces clear changes both in media practices and in the role of citizens/consumers/producers. New media, in particular the Internet, pose new theoretical, methodological, and practical challenges to the shaping of the digital public sphere. Traditional spaces dedicated to public debate are confronted with different forms of socialization, with networked organizations and new channels of information dissemination and exchange that actualize "old" issues in terms of power, control, and citizen participation in public life [9]. The theoretical literature defines 'herding instinct' as referring to situations where people with private, incomplete information consistently make public decisions. Consequently, the first few decision-makers disclose their information and subsequent decision-makers may follow a set pattern, even if their private information suggests that they should deviate from it [10]. This 'information cascade' can occur in perfectly rational people when the information implied by early decisions outweighs the private information of any individual. Anderson and Holt conducted a laboratory study in 1997 in which they calculated the possibility of one person's signals and predictions influencing the decisions of another [11]. An information cascade is a sequence of decisions in which individuals optimally ignore their own preferences and mimic the choices of others ahead of them [12, 13]. The evolution of social media platforms such as Twitter, Facebook, WhatsApp has changed the information cascade process. Due to easy accessibility, especially via smartphones, a large number of people have joined these social media platforms. Moreover, these platforms have become the main source of information dissemination or cascade. Important news about disasters, riots, epidemics, political issues are often spread through these platforms and thus, within a short time, specific information reaches a large number of people.

Accessibility, operational security of information telecommunication networks and systems is crucial to the sustainable improvement of standards of living, working, business organization and civil society. The objects of digital legal relations under law include information in the form of digital data and information objects with digital data (information and communication technologies) [14]. Figure 1 illustrates that the development of ICT, especially mobile phones, has been more dynamic and faster than the introduction of other communication technologies. There has been a rapid preference for mobile networks and devices as the primary means of communication, including access to the World Wide Web. Today, mobile networks cover almost 95% of the planet. Meanwhile, mobile broadband networks with higher quality Internet connectivity cover about 80%.

Mobile networks now cover more than 95% of the Earth's land area, and mobile broadband networks, which provide much better Internet connectivity, cover about 94% [15]. By the end of 2022, more than half of the world's population (65%) was using the Internet, with the proportion of young people (aged 15-24) increasing to more than 75% (Internet users in 2005-2022 shown in Figure 2) [15]. The global progressive trend in ICT diffusion and growth of Internet users allows us to speak of a digital population of planet Earth and/or individual countries.

Today's realities involve both positive and negative aspects of the use of ICTs. On the negative side, there is an increasing trend of crimes involving the use of such tools. Their use is increasingly popular with terrorist, organized crime, and extremist groups as a means to influence government policy and/or decisions.

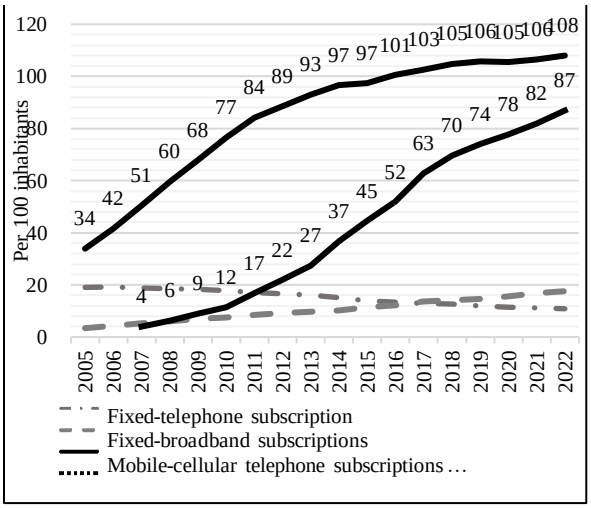


Fig. 1. Global trends in ICTs in 2005–2022 (Per 100 inhabitants)

Source: Measuring digital development Facts and Figures 2022. United Nations International Telecommunication Union (ITU)

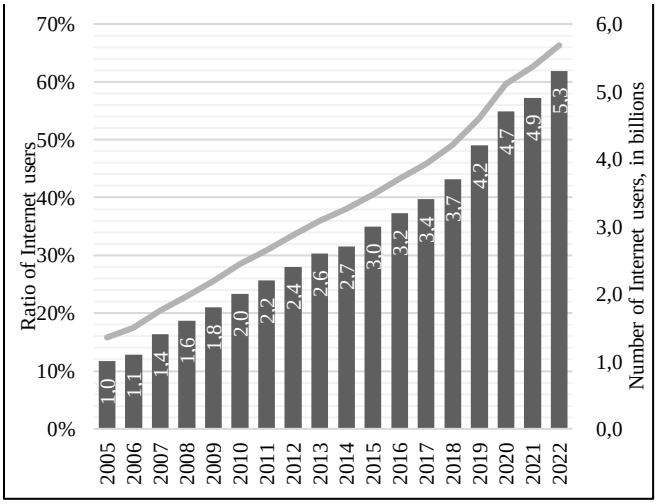


Fig. 2. Individuals using the Internet in 2005–2022 (%)

Source: Measuring digital development Facts and Figures 2022. United Nations International Telecommunication Union (ITU)

IV. The Criminal Utilization Of The Attributes Of The Information Society (ICTs): Riots

The events of the last decade in various countries around the world demonstrate the high efficiency of the impact of information and communication technologies on the consciousness of the general public in order to aggravate mass disturbances. The events of the "Arab Spring", the "colour revolutions" (e.g. in former Eastern Bloc countries), the riots in Minneapolis with subsequent spread to other US cities, etc., are illustrative in this regard. Among other things, one should also note the tactical methods used by the non-systemic opposition in a number of countries, in which public calls for "peaceful" rallies are posted online, with the initial intention to inflame and aggravate the situation.

In assessing the perspectives for exploiting ICTs during a riot, the following areas of use can be identified:

a) Information interaction, communication, appeals;

b) Mobilising people (rioters);

c) Organising the riots;

d) Allocation of roles;

e) Coordination in confrontation with law enforcement agencies;

f) Coordination in achieving the final objective.

When public discontent with certain social problems arises, ICTs facilitate the exchange of information, communication and even calls for specific (not always legal) actions.

A wide range of circumstances can serve as catalysts for social unrest. For example, inappropriate or otherwise lawful police action; unemployment; poor housing conditions; inadequate education; inadequate recreation facilities and programs; ineffective political power structures and recourse/appeal mechanisms; discrimination against people of another race; unfair administration of justice; inadequate federal programs; unacceptable municipal services; and low levels of social protection [16].

Traditional media often do not capture the essence of citizens' collective activism. Moreover, the respective structures restrict access to some websites and communication resources [17]. As an alternative, ICT provides an opportunity to overcome such media structures, ensuring the dissemination of information without 'filters' and censorship.

Mass mobilizations can take hours, days, weeks to months and involve large numbers of citizens. A popular mobilization mechanism involves individuals becoming involved in collective wrongdoing [17, 18, 19,]. In addition to the latter, both social movements and informal structures (such as activist associations) may be involved. At the same time, mass mobilization has a certain impact on public opinion through the concentration of attention and the involvement of the population [20]. A characteristic feature of this phenomenon is its disruptive component.

ICTs reduce the cost of publicizing necessary information about social movements in a short period of time, thereby increasing the number of active participants [21]. There is no doubt that these properties of ICT contribute to the organization of mass disturbances [22]. Decentralized, non-hierarchical organizational structures can be modelled using these technologies.

With the use of ICT tools, organizers can outline tactical plans for determining the form of implementation of collective action and the allocation of roles to participants in a mobilized crowd. The allocation of functional roles among the participants in a crowd takes place at the stage of preparation for the commission and/or implementation of acts of mass disorder as part of the criminal intent. Moreover, this may be accompanied by conditional discipline, active organizing activities, and an elaborate (if necessary) system of supplying the means and implements for the commission of the crime.

In order to ensure public order and public security at all public events, regardless of whether they are authorized or unauthorized, they are usually accompanied by representatives of law enforcement agencies. There is a high risk of confrontation between participants in unauthorized assemblies and law enforcement officials. Depending on the

objectives of such actions, the organizers may follow several scenarios:

a) They are not interested in a violent confrontation with representatives of law enforcement agencies and therefore urge participants in an unsanctioned assembly to stop it immediately on the first request of the police;

b) They a priori aim to escalate the confrontation and by their provocative actions (appeals, orders, etc.) promote an early and violent confrontation with the forces of law and order;

c) They choose not to comply with the legitimate demands of the authorities and proceed "on the spot" to coordinate the actions of the crowd against the forces of law and order.

ICTs can be used to transmit alerts in all of the above cases: of impending National Guard units, police (riot control units); of coordination within 'small groups'; and of command for further mass violent action.

In a mobilized crowd, participants need to be aware of specific plans for unlawful activity, as a lack of coordination among participants can reduce the effectiveness of the action as a whole. The dissemination of such plans can also be accomplished through the use of ICTs.

When assessing the possible impact of ICT use on the course of a mass riot, it is necessary to identify the perpetrators to be held criminally liable. ICTs and associated devices appear to function effectively as tools and instruments of crime. At the very least, incitement, organization and instigation to mass disorder do not seem possible in the current circumstances without the use of ICTs.

A topical issue today is the criminal liability of Internet service providers. The fact is that in the process of dissemination of information on the network, along with the author himself, other entities are involved, in particular, the owner of the network information resource, the owner of the server, etc. [23]. In other words, this process involves, in parallel, entities providing communication services, in particular, operations of receiving, processing, storage, transmission, delivery of telecommunications, etc. These are usually legal entities or self-employed individuals (entrepreneurship & self-employment) providing the above services on the basis of a proper license obtained.

Among ISPs, access providers, hosting providers, caching providers, backbone providers and last-mile providers can be distinguished. In defining legal responsibilities, ISPs should be differentiated according to the functions they perform [24], which are described below.

The functions of access providers include providing access to third-party content by moving, routing data without permanently storing it [25]. For example, through such a provider a user connects to the Internet or an information system from his location to the underlying network of the Internet [25]. Hosting providers store, make available, third-party content both on their own and on a rented technical base (server) [25, 26]. As a consequence, content is permanently online. Most often, users are given direct access to upload content to the network, bypassing the mechanism of manual control by the hosting provider [25].

The mechanism of automatic temporary storage and transfer of data, in order to optimise the technological process of information transfer, is carried out by the caching service provider [27, 28]. Being a technological process, caching in order to reduce the intensity of the flow, accelerate the loading of Web sites and improve the transfer of information provides intermediate storage in the server cache memory [27].

The provision of data and communication services is usually provided by the transport telecommunications infrastructure. Backbone providers lay data links, namely connecting strategic parts of the Internet to backbone lines [29, 30].

The communication line directly from the backbone networks to the user/consumer is laid by last mile providers [31, 32, 33].

The right to freedom of expression is clearly applicable to all citizens, provided that they follow the established rules for the organization and conduct of events, meetings, protests, marches or pickets [34]. However, when there is a conflict between the right to freedom of expression and association and the need to maintain public order and safety, it is crucial to strike a balance. In a democratic state governed by the rule of law, a citizen has the right to freedom of expression and association [34]. Equally important is the security of civilians, who face imminent risks due to potential escalation in the exercise of these rights.

In this context, bans on the dissemination of information aimed at propaganda for war, inciting national, racial, or religious hatred and enmity, as well as other information for the dissemination of which criminal liability is prescribed, are justified [35, 36].

The owner (moderators) of websites, pages on the Internet and/or information system and/or software for electronic data processing shall be guided by the established regulations when disseminating information on social networks in order to attract persons to participate in the mass disorder. That is, they must not allow their resources to be used to commit crimes or to disseminate information that promotes a cult of violence and cruelty.

Channel-specific policies for information systems and programs that enable end-to-end encryption for the transmission and reception of messages are also important. Cryptographic algorithms in such ICT tools are designed to be encrypted in such a way that messages sent and received are intended for two parties only, excluding third parties, including state agencies, from receiving the information [37, 38]. Such systems and programs include Telegram, SafeSMS, None of your business (NOYB), FlyByNight, Pretty Good Privacy (PGP), Off-the-record (OTR), Signal, etc. Obviously, riot masterminds can take advantage of such technologies.

This raises two questions: the possibility of blocking specific individuals using ICT for illegal purposes by these networks, and the permissibility of the state authorities monitoring the communications of citizens with the help of such technologies. On the first issue, there are already known examples of the blocking of the accounts of the 45th President of the United States, Donald Trump, as well as other accounts relaying his messages. However, there are many accounts that incite, urge, recruit and engage people in violent acts without being detected or blocked. Regarding the second question, it seems that monitoring and surveillance of correspondence is permissible in cases of threats to the security of individuals, society and the state.

V. LIABILITY OF ICTS

When qualifying acts of incitement, inducement, recruitment, or other involvement of a person in the commission of acts of mass disorder on the Internet, it is necessary to unambiguously clarify the function performed by each particular person (Internet service providers) in committing the crime. The existence of guilt and, accordingly, the incidence of criminal responsibility for these acts depends on the cognitive elements in a person's psyche, i.e. the intellectual (the ability to understand the wrongfulness of his behavior, foresee consequences) and the orientation of mental and physical efforts to make a decision, i.e. the volitional (the desire for these consequences to occur) elements of guilt [31].

On this issue, we must agree with the position of researchers who argue that ISPs providing technological support in the communications of subjects, i.e. providing only technical support/connecting network access, should not be criminally liable [24]. The criminal liability of ISPs arises if they have the organizational and technical capacity to influence the informational social relations of their users at any time.

Access providers, caching service providers, backbone providers and last-mile providers are therefore not liable because their activities consist only of technological support for the connection of users to the network [24]. In the case of a hosting provider there is a special approach to liability depending on the specific functions performed. If the hosting provider only provides disk space for the physical hosting of information permanently on the network, no liability should be imposed on it. However, if the competent authorities are notified of the illegal content of the uploaded information, and if it is technically possible to restrict access to such information, the hosting provider should be liable for not fulfilling his obligation to restrict access to such information [24].

In view of the above, it may be argued that the liability of Internet service providers for failure to take measures to restrict Internet users' access to information containing appeals, incitement, recruitment or other involvement of persons in the commission of acts of mass unrest arises only if they are aware of the social danger of not restricting access to such information, anticipate dangerous consequences in the form of mass unrest which are a direct consequence of such failure, and in doing so consciously fail to take action.

The guilt of the provider is based on an assessment of the factual circumstances of a particular case, the presence or absence of a mental attitude in the person's actions towards the omission (not restricting access to the information in question) which subsequently contributed to the mass disorder.

CONCLUSION

To summarize the above, the following conclusions are relevant in relation to the exploitation of information and communication technologies as a high-tech means of committing riots:

(1) Attributes of the information society, being ancillary and peripheral factors, are not a direct determinant of riots. Stepping aside from the techno-determinist model, the views of Professor C. Fuchs are convincing, because the triggers of conflict atmosphere in society are exclusively social relations (problems).

2. The use of information and communications technologies by organizers and instigators enables them to be included among the sources of threats in the event of social unrest. Potentially dangerous areas of illicit use of ICTs can be distinguished as follows:

a) Information interaction, communication, appeals;

b) Mobilising people (rioters);

c) Organising mass unrest;

d) Role allocation;

e) Coordination in confrontation with law enforcement agencies;

f) Coordination in achieving the final objective.

3. The criminal liability of ISPs for failing to take measures to restrict Internet users' access to information containing appeals, incitement, recruitment, or other involvement of persons in the commission of acts of riots shall only occur where they are aware of the social danger of not restricting access to such information, foresee dangerous consequences in the form of mass disorder that are a direct result of such restrictions and yet consciously fail to act.

REFERENCES

[1] Collins, A. (Ed.). (2016). Contemporary security studies. Fourth edition. Oxford university press. P. 401

[2] Ignatov, A. N. O kategoriyax «mexanizm prestupnogo povedeniya», «mexanizm prestupleniya» i «mexanizm sovershеniya prestupleniya» // Gumanitarny`e, social`no-e`konomicheskie i obshhestvenny`e nauki. № 6–7. 2017. S. 126–132. (Игнатов, А. Н. О категориях «механизм преступного поведения», «механизм преступления» и «механизм совершения преступления» // Гуманитарные, социально-экономические и общественные науки. № 6–7. 2017. С. 126–132.)

[3] Masuda Y., The Information Society as Post-industrial Society, World Future Society, 1981, p. 147

[4] Bell D. The Coming of the Post-Industrial Society // The Educational Forum, (1976) No 40:4, p. 576

[5] Webster F., Theories of the information society, Third edition, Routledge, London, 2006, p. 9-19

[6] Translated by Thomas Burger, Habermas, J., The structural transformation of the public sphere, MA: MIT Press, Cambridge, 1989, pp. 328

[7] Iosifidis P., Wheeler M. The public sphere and network democracy: Social movements and political change? // Global Media Journal, 13 (25), 2015. pp. 1–17

[8] Schäfer M.S., Digital Public Sphere // In The International Encyclopedia of Political Communication, G. Mazzoleni (Ed.). (2015). London: Wiley Blackwell. p. 322

[9] Sousa H., Pinto M., Silva E. C. e. Digital public sphere: weaknesses and challenges // Comunicação E Sociedade, 2013, vol. 23, p. 9

[10] Anderson L, Holt C.A., Information cascade experiments. In: Durlauf S.N., Blume L.E. (eds) Behavioural and Experimental Economics. The New Palgrave Economics Collection. Palgrave Macmillan, London. 2010. pp. 166-167

[11] Anderson L, Holt C.A., Information Cascades in the Laboratory // The American Economic Review, American Economic Association, Dec., 1997, Vol. 87, No. 5, pp. 847- 862

[12] De Vany A., Lee C., Information Cascades in Multi-Agent Models. Papers 99-00-05, California Irvine - School of Social Sciences. 1999, p. 2

[13] Bikhchandani S., Hirshleifer D., Welch I. Information Cascades. In: Palgrave Macmillan (eds) The New Palgrave Dictionary of Economics. Palgrave Macmillan, London. 2008, p. 1.

[14] Blazheev V. V. Cifrovoe pravo: uchebnik / pod obshh. red. V. V. Blazheeva, M. A. Egorovoj. Moskva: Prospekt, 2020. S. 71 (Блажеев В. В. Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. Москва: Проспект, 2020. С. 71.)

[15] Measuring digital development Facts and Figures 2022. United Nations International Telecommunication Union (ITU), Development Sector. 2022. Official text [Electronic resource]. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (Access date: 14.02.2023).

[16] United States. National Advisory Commission on Civil Disorders, & United States. Kerner Commission. Report of the national advisory commission on civil disorders. pp. 8–20.

[17] Mancini F., O'Reilly M. New Technology and the Prevention of Violence and Conflict. Stability: International Journal of Security & Development. Volume 2. Issue 3. Art. 55. 2013. P. 3. URL: https://ssrn.com/abstract=2902494 (22.02.2022)

[18] Smith, L. G., Blackwood, L., & Thomas, E. F. The need to refocus on the group as the site of radicalization. Perspectives on psychological science, 2020. 15(2), P. 335 DOI: https://doi.org/10.1177/1745691619885870

[19] Mancini F., O'Reilly M. New Technology and the Prevention of Violence and Conflict. Stability: International Journal of Security & Development. Volume 2. Issue 3. Art. 55. 2013. P. 3.

[20] Della Porta, D., Diani, M. Social movements: An introduction. Third edition. John Wiley & Sons. 2020. pp. 21–22.

[21] Shultziner D., Goldberg S. The stages of mass mobilization: separate phenomena and distinct causal mechanisms. Journal for the theory of social behaviour. Volume 49, Issue 1. 2019. P. 12. DOI: https://doi.org/10.1111/jtsb.12187.

[22] Leizerov S. Privacy Advocacy Groups Versus Intel: A Case Study of How Social Movements Are Tactically Using the Internet to Fight Corporations. Social Science Computer Review. Volume 18, Issue 4. 2000. pp. 464–465.

[23] Duncan F. Collective Action and Digital information Communication Technologies: The Search for Explanatory Models of Social Movement Organizations' Propensity to Use Dicts in Developed Democracies. Publicly Accessible Penn Dissertations. 2015. 1048. P. 90. (Order No. 3709451). Available from ProQuest Dissertations & Theses Global. (1699101824). URL: https://www.proquest.com/dissertations-theses/collective-action-digital-information/docview/1699101824/se-2?accountid=30408 (23.02.2022).

[24] Rassolov I.M. Pravovy`e problemy` obespecheniya informacionnoj bezopasnosti: yuridicheskaya otvetstvennost` operatorov svyazi. Vestnik Moskovskogo universiteta MVD Rossii. 2013. №12. S. 103. (Рассолов И.М. Правовые проблемы обеспечения информационной безопасности: юридическая ответственность операторов связи. Вестник Московского университета МВД России. 2013. №12. С. 103.)

[25] Perchatkina S. A., Cheremisinova M. E., Cirin A. M., Cirina M. A., Czomartova F. V.. Social`ny`e internet-seti: pravovy`e aspekty`. Zhurnal rossijskogo prava. 2012. №5 (185). S. 20. (Перчаткина С. А., Черемисинова М. Е., Цирин А. М., Цирина М. А., Цомартова Ф. В.. Социальные интернет-сети: правовые аспекты. Журнал российского права. 2012. №5 (185). С. 20.)

[26] Zharova A. K. O neobxodimosti pravovoj klassifikacii operatorov seti Internet // Biznes-informatika. 2011. №3 (17). S. 63. (Жарова А. К. О необходимости правовой классификации операторов сети Интернет // Бизнес-информатика. 2011. №3 (17). С. 63.)

[27] Weber, R. H. Internet Service Provider Liability: The Swiss Perspective. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 1, 2010. P. 148.

[28] Chubukova S.G. Problemy` pravovogo statusa informacionnogo posrednika. Vestnik akademii prava i upravleniya. 2017. № 2 (47). S. 41 (Чубукова С.Г. Проблемы правового статуса информационного посредника. Вестник академии права и управления. 2017. № 2 (47). С. 41)

[29] Pfender, J., Valera, A., & Seah, W. K. Reassessing caching performance in information-centric IoT. Internet of Things, 100479. 2022. P.1 DOI: https://doi.org/10.1016/j.iot.2021.100479.

[30] Ozhiganova E. M. Primenenie sistemy` motivacii vremenny`x sotrudnikov na primere AO «E`R-Telekom xolding» // Biznes-obrazovanie v e`konomike znanij. 2016. №1 (3). S. 44. (Ожиганова Е. М. Применение системы мотивации временных сотрудников на примере АО «ЭР-Телеком холдинг» // Бизнес-образование в экономике знаний. 2016. №1 (3). С. 44.)

[31] Mayr, C., Risso, C., & Grampín, E. Crafting optimal and resilient iBGP-IP/MPLS overlays for transit backbone networks. Optical Switching and Networking, 42, 100635. 2021. P. 2 DOI: https://doi.org/10.1016/j.osn.2021.100635.

[32] Cirina M. A. Rasprostranenie pronarkoticheskoj informacii v Internete: mery` protivodejstviya // Zhurnal rossijskogo prava. 2012. №4 (184). S. 48. (Цирина М. А. Распространение пронаркотической информации в Интернете: меры противодействия // Журнал российского права. 2012. №4 (184). С. 48)

[33] Gevaers, R., Van de Voorde, E., & Vanelslander, T. Cost modelling and simulation of last-mile characteristics in an innovative B2C supply chain environment with implications on urban areas and cities. Procedia-Social and Behavioral Sciences. 2014. 125, P. 400. DOI: https://doi.org/10.1016/j.sbspro.2014.01.1483

[34] Boysen, N., Fedtke, S., & Schwerdfeger, S. Last-mile delivery concepts: a survey from an operational research perspective. Or Spectrum. 2021. 43(1), P. 4. DOI: https://doi.org/10.1007/s00291-020-00607-8.

[35] Pukovodyashhie principy` po svobode mirny`x sobranij, Izdanie 2-e. BDIPCh OBSE. 2011. 192 C. URL: https://www.osce.org/odihr/73405 (data obrashheniya: 25.11.2021). (Руководящие принципы по свободе мирных собраний, Издание 2-е. БДИПЧ ОБСЕ. 2011. 192 С. URL: https://www.osce.org/odihr/73405 (дата обращения: 25.11.2021).)

[36] United Nations. (2020). United Nations Strategy and Plan of Action on Hate Speech–Detailed Guidance on Implementation for United Nations Field Presences. URL: https://www.un.org/en/genocideprevention/hate-speech-strategy.shtml (дата обращения: 14.12.2021).

[37] Grambo, K. Fake news and racial, ethnic, and religious minorities: A precarious quest for truth. U. Pa. J. Const. L., 21. 2018. P. 1304.

[38] Schillinger F., Schindelhauer C. End-to-End Encryption Schemes for Online Social Networks // Security, Privacy, and Anonymity in Computation, Communication, and Storage 12th International Conference, SpaCCS 2019 Atlanta, GA, USA, July 14–17, 2019 Proceedings. Springer Nature Switzerland AG 2019. P. 138.

[39] Ullah, S., & Zahilah, R. Curve25519 based lightweight end-to-end encryption in resource constrained autonomous 8-bit IoT devices. Cybersecurity. 2021. 4(1), 1-13. P. 1

Interaction Between Blockchain Technology and Conventional Databases: a Systematic Literature Review

Received: 30 January 2023; Accepted: 5 March 2023 *Research Article*

1st Ahmet Anıl DÜNDAR
Department of Research and Development
ASELSAN Corporation
Ankara, Turkey
aadundar@aselsan.com.tr
0000-0002-4408-4002

2nd Saim Buğrahan ÖZTÜRK
Department of Research and Development
ASELSAN Corporation
Ankara, Turkey
sbozturk@aselsan.com.tr
0000-0003-1780-3558

3rd Hakan MUTLU
Department of Research and Development
ASELSAN Corporation
Ankara, Turkey
hakanmutlu@aselsan.com.tr

***Abstract*—Day by day, the popularity of blockchain technology is rising in the business sector. Companies that want to benefit from some of the features of blockchain like security, immutability, decentralization, and elimination of central authority, try to integrate this technology to their existing business use cases. During the integration process, companies must go over a decision process and decide whether the blockchain technology should replace the current system or the two systems should be combined. In order to successfully make the decision, developers or researchers must be aware of the blockchain's features and analyze the improvements that a change between databases and blockchain technology would bring to the existing system. In this paper, in order to provide an outline of differences between blockchain and databases and also ease the decision process that researchers or developers must undergo, we conduct a systematic literature review on the differences between blockchain and databases and possible features they would provide in a system.**

Keywords— Blockchain vs Database, Blockchain Database, Systematic Literature Review

I. INTRODUCTION

Blockchain technology has gained significant attention in recent years due to its potential to disrupt a wide range of industries and sectors. Blockchain can be identified as the driving technology behind cryptocurrencies like Bitcoin, Ethereum etc. Although blockchain technology is popular by its usage in cryptocurrencies, overall it can be considered as a database technology that provides a data store of transactions between the participants of the network in a decentralized way. The benefits of using blockchain are as follows:

- Security: Blockchain is decentralized and distributed, it is not controlled by any single entity. This makes it less vulnerable to attacks and ensures that the data stored on the blockchain is secure.
- Transparency: Blockchain technology allows for transparent and immutable record-keeping. All transactions on a blockchain are recorded and can be viewed by anyone with access to the network.
- Efficiency: Blockchain technology has the potential to streamline processes and reduce the need for intermediaries.
- Decentralization: Because a blockchain is decentralized, it is not controlled by any single entity. This can help to reduce the risk of censorship and ensure that all parties have equal access to the network.

The participants of the blockchain network can share data with each other without establishing trust between them. This process is made available through a mechanism called consensus which will be explained in detail in the upcoming sections of the paper.

We can certainly think of blockchain technology as a database solution with unique capabilities compared to conventional database technologies. It provides decentralized data storage among all the participants of the blockchain network. Also, eliminates the need for a central authority to govern the data storage process through consensus mechanisms between the participants of the blockchain network. It allows participants that don't trust each other to share data in a secure way via the usage of cryptographic protocols. Moreover, ensures the integrity and immutability of the data by the usage of hash chain technologies like Merkle Trees.

Blockchain technology is considered a candidate database solution for existing business use cases due to the unique capabilities it possesses. Some of these use cases can be listed as follows:

- Finance: Due to the ability of blockchain to eliminate trusted third parties from the system, blockchains can be considered as a replacement for existing data storage systems in the finance sector.
- IoT: Blockchains are decentralized by nature and this property can be integrated to the existing IoT systems to enhance the scalability of the IoT system.
- Healthcare: Blockchain could be used in healthcare to digitalize medical data and store it on the chain. In this way, we can achieve a decentralized medical system that any medical-related company can access.
- Supply Chain: Data is stored as transactions in the blockchain and the data is immutable. This property could be used in supply chains where we could track a product's lifecycle via the blockchain.

- Identity Verification: Digital credentials can be stored on the blockchain. In this way, blockchain users can authenticate the digital identity of a person or physical object in a distributed manner.

Although all the mentioned use cases above are currently being managed by existing database technologies like SQL, NoSQL, Distributed DBs, etc. many researchers in the area of blockchain think that in the future, these technologies can be enhanced or replaced by blockchain databases.

Our Contribution: In our work, in order to help researchers, decide whether a blockchain database solution suits their needs or should they replace their existing database solution with blockchain, we have conducted a systematic literature review on the subject "interaction between blockchain and databases". By doing so, we expect to outline the main differences between blockchain databases and conventional databases and explain how these technologies can complement each other's shortcomings.

The rest of this article is organized as follows. In Section II, we gave a brief background about existing blockchain technologies and database solutions. In Section III, we explained the research methodology we follow while conducting our systematic literature review process and then we analyzed our results in Section IV. Finally, we concluded our research in Section V.

II. BACKGROUND

A. An overview of Modern Database Systems

The term "Data" can be described as a collection of facts, figures, measurements and signals. It is the first step on the road to "Knowledge". Adding context to data leads us to information. And meaning plus information equal knowledge. That is exactly the step where we are utilizing the data to help to understand situations and make decisions.

As said above, data is a collection, so, like every collection, it needs to be kept in somewhere safe, accessible, and unmanipulated. That is the reason why databases are needed.

It can be said that modern databases were born in the 1970s, that is the year the relational database model came through. Most of the databases that we use today are still relational database systems. Relational databases can be described as collections of data items that have pre-defined relationships between them. The items are in the form of rows and columns. Oracle, IBM DB2, MySQL, and Google Bigquery are some examples of it.

Today, we also use non-relational databases which have commonly known as "NoSQL" since the late 2000s. In these databases, the items are not tabular. They store data in different ways from relational databases. The types are mainly document, key-value, column, and graph. MongoDB, CouchDB, CouchBase, Cassandra, HBase, Redis, Riak, and Neo4J are some examples of NoSQL databases.

B. An overview of Blockchain Technology

The Blockchain is a system that records information, generally transaction information, as a form of linked blocks. It is a decentralized system, which means that the records are kept and maintained on a peer-to-peer network without any geographical limit.

When a new record is added, the transaction record needs to be authenticated by the peers of the network. After that, it will be verified and added to the chain by linking the previous record with a uniquely encoded key.

This structure makes information manipulation impossible. Also, it cannot be controlled by a single authority due to the decentralized architecture. It can be said that centralized systems are open to manipulation and attacks, blockchain eliminates these risks.

The architecture of blockchain consists of three layers. These layers are Applications, Decentralized Ledger and Peer-to-Peer Networks. Applications developed on top of the blockchain architecture, the Application Layer, which allows users to keep track of their transactions and processes, usually through an interface. The decentralized Ledger is the middle layer and it can be considered as the main layer. All the key processes like recording, authentication, encoding, linkage occur at this layer. Finally, peer-to-peer networks are present at the bottom layer. It keeps the node types for the Decentralized layer for different processes.

C. A comparison of Database and Blockchain

A blockchain is a decentralized and distributed digital ledger that records transactions on multiple computers, making it virtually tamper-proof. This makes it an ideal solution for a variety of applications, including financial transactions, supply chain management, and identity verification. Blockchain is more decentralized, more secure due to its distributed structure, and naturally more transparent as all transactions are visible.

On the other hand, database systems have been in use for decades and are a key component of many modern systems. These systems are centralized, meaning that they are controlled by a single entity, and they use structured data storage methods to store and manage data. traditional database systems are faster, more effective and scalable systems compared to blockchain. This is because the blockchain requests verification by multiple users for each transaction.

III. RESEARCH METHODOLOGY

We have used the guidelines given in [1] to conduct our Systematic Literature Review (SLR) process. The complete flow of our process can be seen in Fig. 1. Our flow contains two phases: Source selection, Systematic Literature Review which we will discuss in the following sections.

A. Systematic Literature Review

Systematic Literature Review (SLR) is a methodical and systematic approach to reviewing research on a particular topic. It involves identifying and analyzing relevant research in a systematic and transparent manner, in order to provide a comprehensive overview of the current state of knowledge on the topic. The steps followed to create SLR are as follows:

- Define the research question.
- Identify relevant sources.
- Search and select studies.
- Assess study quality.
- Extract and synthesize data.
- Analyze and interpret the data.

Overall, conducting a SLR requires a systematic and transparent approach to reviewing the research on a particular topic.

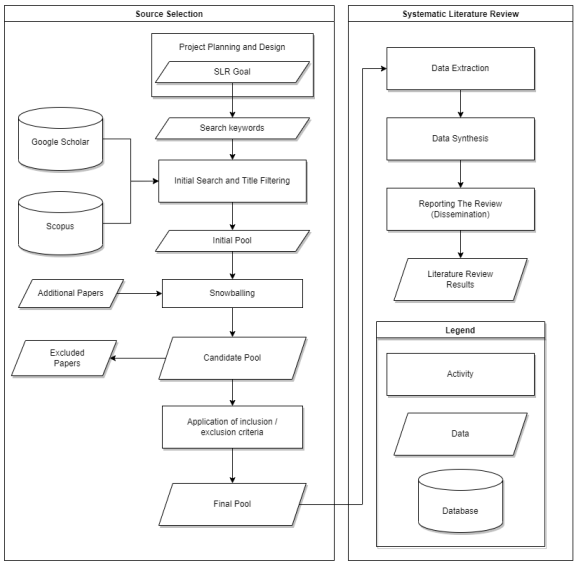


Fig. 1. Overview of our Research Process

B. Goal of our SLR

Our purpose in this study is to understand, review and analyze the effects of blockchain technology on the development of modern database systems and explain the relationship between databases and blockchains and thus provide a summary for the researchers in this area.

C. Research Questions

According to the methodology we follow in our research, specifying the research questions (RQs) is the most important part of any systematic review as these questions drive the entire systematic review process:

- Primary studies that address the research questions must be found during the search phase.
- The data extraction method must provide the necessary data to provide answers for the research questions.
- The data analysis method must synthesize the data generated from the data extraction process in order to answer the research questions.

Based on the goal of our SLR we have defined our RQs as follows:

- **RQ1 - What are the top differences between blockchain-based databases and conventional databases in terms of database functionality**? : Main differences between Blockchain-Based Database Systems and Conventional Databases.
- **RQ2 - When to use Blockchain-Based Database Storage? :** When should we use blockchain technology as a database? Develop a decision tree for the question.
- **RQ3 - Business use cases which commonly use Blockchains instead of Databases :** Which technologies like the Internet of Things (IoT), Supply Chain, and Auditing Systems use blockchain-based database systems?
- **RQ4 - For which criteria Blockchain-Based Database Systems are preferred over Conventional Databases? :** Which feature of the blockchains (immutability, decentralized technology, etc.) make them preferable over conventional databases?

D. Research Paper Pool

We have used two popular digital databases, Google Scholar and Scopus in our research process to form our initial review paper pool. Although the coverage of Google Scholar is much higher compared to Scopus, we have used Scopus to reduce the bias in the paper selection process as much as possible. We have finalized our initial research paper pool at 45 papers.

The search strings we have used in Google Scholar and Scopus platforms are given in Table 1. For our paper selection process, we have used abstract and title-based selection.

TABLE I. EARCH RESULTS FOR GOOGLE SCHOLAR AND SCOPUS

Search String	***Number of Papers***
Blockchain versus database	*92*
Blockchain and database	*155*
Blockchain database	*2900*

E. Exclusion and Inclusion Criteria

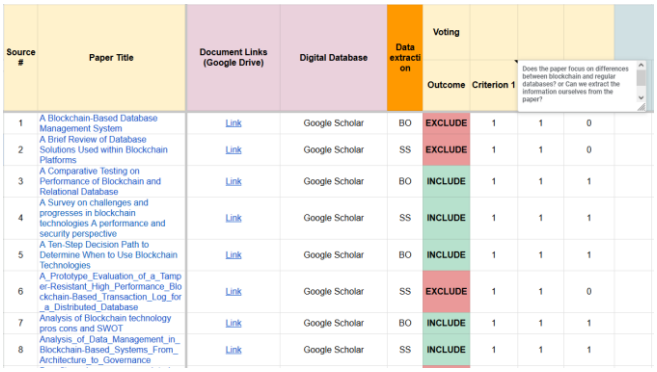
We have defined inclusion and exclusion criteria in order to guarantee that the papers that are irrelevant to our study are excluded and the ones that are relevant are included in our paper pool. The exclusion and inclusion criteria we have defined are as follows:

- Can we access the paper in pdf format?
- Is the paper written in Turkish or English?
- Does the paper focus on differences between Blockchain and Conventional Databases? Or can we extract the information ourselves from the paper?

Based on the "Yes" and "No" answers for every criterion for each paper, we have included the papers that had "Yes" for all the criteria and excluded the rest.

F. Final Pool of Papers

Our paper pool was finalized at 23 papers after applying exclusion and inclusion criteria. To ease our collaborative work, we have designed an online spreadsheet in which we could put comments for each paper after the review process. The format of the online spreadsheet is given in Fig 2.



Source #	Paper Title	Document Links (Google Drive)	Digital Database	Data extraction	Voting			
					Outcome	Criterion 1		
1	A Blockchain-Based Database Management System	Link	Google Scholar	BO	EXCLUDE	1	1	0
2	A Brief Review of Database Solutions Used within Blockchain Platforms	Link	Google Scholar	SS	EXCLUDE	1	1	0
3	A Comparative Testing on Performance of Blockchain and Relational Database	Link	Google Scholar	BO	INCLUDE	1	1	1
4	A Survey on challenges and progresses in blockchain technologies A performance and security perspective	Link	Google Scholar	SS	INCLUDE	1	1	1
5	A Ten-Step Decision Path to Determine When to Use Blockchain Technologies	Link	Google Scholar	BO	INCLUDE	1	1	1
6	A_Prototype_Evaluation_of_a_Tamper-Resistant_High_Performance_Blockchain-Based_Transaction_Log_for_a_Distributed_Database	Link	Google Scholar	SS	EXCLUDE	1	1	0
7	Analysis of Blockchain technology pros cons and SWOT	Link	Google Scholar	BO	INCLUDE	1	1	1
8	Analysis_of_Data_Management_in_Blockchain-Based_Systems_From_Architecture_to_Governance	Link	Google Scholar	SS	INCLUDE	1	1	1

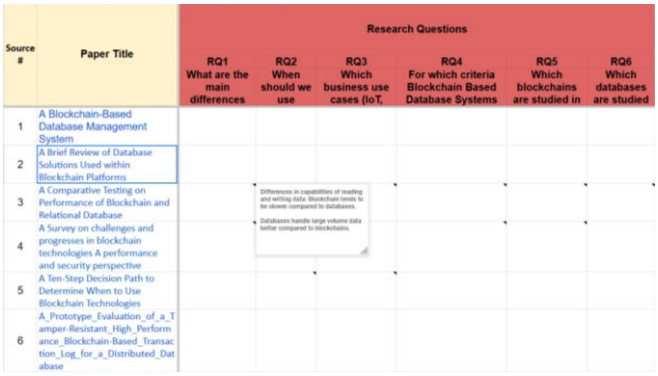
Fig. 2. Our Paper Pool

G. *Final Pool of Papers*

We divided our final paper pool into two pieces, then every member of our team extracted data from the research papers assigned to him/her. We have defined separate cells in our online spreadsheet for the data extraction process. Each data extractor added his/her comments to these cells and also added the answers to the RQs that he/she extracted from the research paper. Our extracted data has the following format:

- Name of the Data Extractor
- Date of Data Extraction
- Title, Authors, Journal, Publication Details
- Type of the Paper (Contribution Facet)
- Answers to the RQs
- Space for additional notes

Fig. 3 indicates an image of our data extraction process for the RQ1 on a paper from our paper pool. In the image, one of our team members has extracted a relevant text from the article as an answer to RQ1. This process is repeated for all of the RQs and papers in the paper pool.



Source #	Paper Title	Research Questions					
		RQ1 What are the main differences	RQ2 When should we use	RQ3 Which business use cases (IoT,	RQ4 For which criteria Blockchain Based Database Systems	RQ5 Which blockchains are studied in	RQ6 Which databases are studied
1	A Blockchain-Based Database Management System						
2	A Brief Review of Database Solutions Used within Blockchain Platforms						
3	A Comparative Testing on Performance of Blockchain and Relational Database						
4	A Survey on challenges and progresses in blockchain technologies A performance and security perspective						
5	A Ten-Step Decision Path to Determine When to Use Blockchain Technologies						
6	A_Prototype_Evaluation_of_a_Tamper-Resistant_High_Performance_Blockchain-Based_Transaction_Log_for_a_Distributed_Database						

Fig. 3. Our Data Extraction Process

IV. Research Results

In this section, we report the results of our data extraction process and provide answers to the RQs we have defined.

A. *Main differences between Blockchains and Databases*

In the first RQ, we have examined the main differences between Blockchains and Conventional Database Management Systems.

One of the key differences is the performance issue. Blockchain tends to be slower than conventional DBs in terms of reading and writing the data. It means, while working with high-volume data, DB handles this better. The average latency of transactions is higher on Blockchain than on conventional DBs. (See Papers; [2], [3], [4], [5], [6], [7], [8], [9])

Another one is centralization. Blockchain is decentralized while conventional DBs are mostly centralized. In centralized type, DB presents one place and multiple users can access it. However, in a decentralized structure, data is split and distributed through several locations within the network. The decentralized structure's main advantage is fault tolerance - robustness. Also, since it has not had a single point of failure, better able to cope with malicious attacks. Moreover, we do not need to trust a central entity to provide the correctness of the state, it is publicly verifiable.

Another difference about centralization is, transactions are accepted to the blockchain via a consensus mechanism rather than a controlling central party. (See papers; [10], [11], [4], [5], [12], [13], [14], [9])

Blockchain is transparent and immutable whereas conventional DBs are not, which means transactions on the blockchain cannot be deleted or altered by some centralized entity. These processes can be executed on conventional DBs, DBs have transaction logs for these. (See papers; [10], [11], [15], [16], [9])

Blockchain allows access to it without any central administration. There is no administrator on the blockchain whereas DB has administrators and super users. It makes accessibility easier and in a more democratized way on Blockchain compared to conventional DBs. Everyone who has a computer can join the network on Blockchain. Access is unlimited and uncontrolled, unlike DBs. This can be questioned in terms of the confidentiality of the data. For security issues, blockchain uses cryptography (chained hashes) rather than traditional access control like DBs. Authentication is assured through complex mathematics. (See papers; [10], [11], [3], [4], [13])

One of the most important concepts about databases is data analysis. For this, data querying is a key concept. Querying conventional DBs are easy with some specialized query languages like SQL. Even though querying NoSQL DBs also harder than SQL, on Blockchain, querying data is harder than conventional DBs whether it is SQL or NoSQL. Information retrieval takes extra programming efforts on Blockchain, unlike DBMS. (See papers; [16], [17], [9])

Another point is redundancy. In blockchain systems, redundancy is inherently provided through replication across the writers. In conventional DBs, redundancy is generally achieved through replication on different physical servers and through backups. Also, on the blockchain, every node is the last copy of itself whereas, on conventional DBs, the central authority has the copies. (See papers; [4], [13])

Energy consumption is massively larger on Blockchain than on conventional DBs. (See paper; [3])

B. *When do we need Blockchain?*

As discussed in the first question, the main advantage of blockchain over traditional DBMS is granting trust between parties. We need blockchain when the interaction between different parties lacks trust. When security and trust concerns come up between parties, we can use blockchain over traditional DBMS to eliminate the concerns. Transactions are

completely transparent on blockchain due to its decentralized structure. Also, the immutability feature provides the guarantee that no transaction can be manipulated by some central authority. (See papers; [2], [10], [11] [3], [18], [13], [19])

Another thing is the performance issue. Again, as discussed at the first question, blockchain's performance is worse than conventional DBs. If we do not need huge performance, if the performance requirements fit the blockchain structure, it can be needed over traditional DBs. There is a trade-off in this area, between advantages like decentralization, granting trust between parties, and security vs. performance. If this trade-off balanced well for the case, then blockchain might be a good solution for database management. (See papers; [2], [4], [5], [13], [19])

Blockchain is needed when fault tolerance is needed for large software systems. Because of the distributed nature, it is the best choice for the robustness of the database. Also, due to the uniqueness of the information and complete synchronization of the processes, data integrity can be granted in any case on the blockchain. (See papers; [15], [4], [7], [20])

We need blockchain when decentralization is the key issue. If we do not want a central authority to grant access, manipulate data, etc., we should use blockchain to everyone has control over transactions. (See paper; [18])

C. Business use cases that use Blockchain over Databases

During our data extraction process, we have tried to answer the question; which business use cases use blockchain technology as a database technology? The answer to our question can be seen in Table II.

TABLE II. BUSINESS USE-CASES

Business	***Papers***
IoT	*[2], [11], [13], [21], [22], [25], [28], [29]*
Finance and Banking	*[3], [4], [8], [11], [13], [15], [19], [20], [23], [27]*
Supply Chain	*[4], [8], [13], [18], [19], [23], [24]*
Healthcare	*[4], [8], [11], [18], [19], [21], [24]*
5G	*[21], [22], [31]*
Digital Identity & E-voting	*[11], [13], [18], [19], [24], [26]*

D. Why do we prefer Blockchain over Conventional Database?

The first criterion to prefer Blockchain over Conventional DB is its decentralized architecture. There is no central authority on Blockchain. So, it is better in the context of transparency and no need to trust a third party. The data cannot be manipulated by an authority. Transactions are recorded with consensus mechanisms. Also, decentralization grants a more robust and fault-tolerant system compared to conventional DBs due to its distributed nature. The data restoration process is much easier than conventional DBMS. (See papers; [2], [10], [11], [15], [21], [3], [22], [4], [18], [13], [19], [8], [20], [24], [9], [30])

Another criterion is integrity and data security. Due to the consensus mechanism and immutability feature, we can always be sure that data on the blockchain has not been changed and manipulated. This also brings security with cryptographic features in it. The immutability nature brings trust to the data processed on blockchain whereas cryptography secures the data completely. Therefore, with these two, we can say that blockchain is much more secure than traditional DBs. (See papers; [10], [11], [15], [5], [19], [8], [9])

The last thing is anonymity. It is due to blockchain's open-source technological background. Everyone who has a computer can join the network without any authorization. This brings the availability and universal access to the blockchain structure. Another advantage of this is reducing transaction costs. Blockchain allows everyone on the network to conduct transactions. (See papers; [11], [15], [18], [20])

V. CONCLUSION

Although blockchain technology is still in its infancy, the technology is being actively developed and improved by many professionals around the world, and its likely that due its nature, it will provide some unique capabilities to the system where it is used. In the context of analyzing the interaction between blockchains and databases, we have conducted a systematic literature review where we outlined the main differences between blockchains and databases, identified the business use cases that can benefit from blockchains, and listed the advantages of blockchain systems over databases. We also tried to answer the question “When do we need a blockchain?”.

During our study, in order to ease our research process and improve our work as a team, we used a well-known systematic literature review guideline for software engineering [1]which sped up our research process.

We believe that our research will benefit the sector professionals or the researchers in deciding if the system at hand can benefit from a blockchain or a database solution should be enough and also provide a guideline when examining blockchain capabilities over databases.

REFERENCES

[1] S. Keele et al., “Guidelines for performing systematic literature reviews in software engineering,” Technical report, Ver. 2.3 EBSE Technical Report. EBSE, Tech. Rep., 2007.

[2] S. Chen, J. Zhang, R. Shi, J. Yan, and Q. Ke, “A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems,” in International Conference on Distributed, Ambient, and Pervasive Interactions. Springer, 2018, pp. 21–34.

[3] P. J. McAliney and B. Ang, “Blockchain: business’ next new “it” technology—a comparison of blockchain, relational databases, and google sheets,” International Journal of Disclosure and Governance, vol. 16, no. 4, pp. 163–173, 2019.

[4] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, “Blockchain versus database: a critical analysis,” in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018, pp. 1348–1353.

[5] P. Ruan, T. T. A. Dinh, D. Loghin, M. Zhang, G. Chen, Q. Lin, and B. C. Ooi, “Blockchains vs. distributed databases: Dichotomy and fusion,” in Proceedings of the 2021 International Conference on Management of Data, 2021, pp. 1504–1517.

[6] A. Sharma, F. M. Schuhknecht, D. Agrawal, and J. Dittrich, “Blurring the lines between blockchains and database systems: the case of

hyperledger fabric," in Proceedings of the 2019 International Conference on Management of Data, 2019, pp. 105–122.

[7] S. Bergman, M. Asplund, and S. Nadjm-Tehrani, "Permissioned blockchains and distributed databases: A performance study," Concurrency and Computation: Practice and Experience, vol. 32, no. 12, p. e5227, 2020.

[8] E. Safak, A. F. Mendi, and T. Erol, "Hybrid database design combination of blockchain and central database," in 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). IEEE, 2019, pp. 1–5.

[9] M. Raikwar, D. Gligoroski, and G. Velinov, "Trends in development of databases and blockchain," in 2020 Seventh International Conference on Software Defined Systems (SDS). IEEE, 2020, pp. 177–182.

[10] X. Zheng, Y. Zhu, and X. Si, "A survey on challenges and progresses in blockchain technologies: A performance and security perspective," Applied Sciences, vol. 9, no. 22, p. 4731, 2019.

[11] M. Niranjanamurthy, B. Nithya, and S. Jagannatha, "Analysis of blockchain technology: pros, cons and swot," Cluster Computing, vol. 22, no. 6, pp. 14 743–14 757, 2019.

[12] S. Cohen and A. Zohar, "Database perspectives on blockchains," arXiv preprint arXiv:1803.06015, 2018.

[13] K. Wüst and A. Gervais, "Do you need a blockchain?" in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018, pp. 45–54.

[14] Z. Ge, D. Loghin, B. C. Ooi, P. Ruan, and T. Wang, "Hybrid blockchain database systems: Design and performance," VLDB Endowment, vol. 15, no. 5, pp. 1092–1104, 2022.

[15] H.-Y. Paik, X. Xu, H. D. Bandara, S. U. Lee, and S. K. Lo, "Analysis of data management in blockchain-based systems: From architecture to governance," Ieee Access, vol. 7, pp. 186 091–186 107, 2019.

[16] P. Chitti, J. Murkin, and R. Chitchyan, "Data management: Relational vs blockchain databases," in International Conference on Advanced Information Systems Engineering. Springer, 2019, pp. 189–200.

[17] S. Helmer, M. Roggia, N. E. Ioini, and C. Pahl, "Ethernitydb integrating database functionality into a blockchain," in European Conference on Advances in Databases and Information Systems. Springer, 2018, pp. 37–44.

[18] M. E. Peck, "Blockchain world-do you need a blockchain? This chart will tell you if the technology can solve your problem," IEEE Spectrum, vol. 54, no. 10, pp. 38–60, 2017.

[19] S. K. Lo, X. Xu, Y. K. Chiam, and Q. Lu, "Evaluating suitability of applying blockchain," in 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS). IEEE, 2017, pp. 158–161.

[20] N. A. Popova and N. G. Butakova, "Research of a possibility of using blockchain technology without tokens to protect banking transactions," in 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2019, pp. 1764–1768.

[21] L. Tseng, X. Yao, S. Otoum, M. Aloqaily, and Y. Jararweh, "Blockchain-based database in an iot environment: challenges, opportunities, and analysis," Cluster Computing, vol. 23, no. 3, pp. 2151–2165, 2020.

[22] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5g: Opportunities and challenges," in 2019 IEEE Globecom Workshops (GC Wkshps). IEEE, 2019, pp. 1–6.

[23] A. B. Pedersen, M. Risius, and R. Beck, "A ten-step decision path to determine when to use blockchain technologies," MIS Quarterly Executive, vol. 18, no. 2, pp. 99–115, 2019.

[24] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE). IEEE, 2018, pp. 1–6.

[25] O.Novo, Scalable Access Management in IoT Using Blockchain: A Performance Evaluation, 6, 4694-4701, 10.1109/JIOT.2018.2879679, 2019.

[26] M. Pawlak, A. Poniszewska-Marańda, N. Kryvinska, Towards the intelligent agents for blockchain e-voting system, Procedia Computer Science, Volume 141, ISSN 1877-0509, 2018 pp. 239–246.

[27] N. Dhanda, Cryptocurrency and Blockchain: The Future of a Global Banking System In Regulatory Aspects of Artificial Intelligence on Blockchain, 181-204. Hershey, PA: IGI Global, 2022.

[28] K. Christidis, M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2016, pp. 2292-2303.

[29] E. Zeydan, Y. Turk, S. B. Ozturk, H. Mutlu, A. A. Dundar, Post-Quantum Blockchain-Based Data Sharing for IoT Service Providers, IEEE Internet of Things Magazine, vol. 5, no. 2, 2022, pp. 96-101.

[30] Z. Kaspars, S. Renāte, Blockchain Use Cases and Their Feasibility, Applied Computer Systems, vol. 23, 2018, pp. 12-20. 10.2478/acss-2018-0002.

[31] M. Hajar, S. Cherkaoui, L. Khoukhi, An Overview of Blockchain and 5G Networks, Computational Intelligence in Recent Communication Networks. EAI/Springer Innovations in Communication and Computing, 2022 pp. 1-20.

Physical Tracking of ESP32 IoT Devices with RSSI Based Indoor Position Calculation

Received 30 January 2023; Accepted: 5 March 2023 *Research Article*

Özlem Şeker
Department of Computer Engineering
Graduate School of Natural and Applied Sciences
Dokuz Eylul University
Izmir, Turkey
ozlem.yerlikaya@cs.deu.edu.tr
0000-0002-8686-340X

Batuhan Şahin
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey
batuhan.sahin@ceng.deu.edu.tr

Tunahan Akdoğan
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey
tunahan.akdogan@ceng.deu.edu.tr

Gökhan Dalkılıç
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey
dalkilic@cs.deu.edu.tr
0000-0002-0130-1716

***Abstract*— In recent days, the increase in the number of devices that can access the Internet and the variety of areas where it is used have made it essential to ensure the security of the transmitted data. The unique values embedded in the hardware can be used as keys or secret values within cryptographic algorithms to provide the confidentiality and integrity of the data. In such a situation, maintaining the security of the Internet of things (IoT) device used is a prominent element as well as the privacy of the data. The security requirement of each IoT application may be different. While some applications contain sensitive personal or commercial information, for some applications only the presence of the device may be important. In addition, it is likely to have different devices capable of processing cryptographic algorithms. Within the scope of this study, the distance information was calculated with received signal strength indication (RSSI) data based on 4 reference points of the ESP32 IoT device located indoors. The error rate was observed with the positioning based on the RSSI information of the current position of the device. It has been tested whether it is possible to detect whether the device that transfers the data is legitimate or not via indoor position calculation using RSSI.**

Keywords*— indoor localization, IoT, RSSI, ESP32, Wi-Fi.

I. INTRODUCTION

Internet of things (IoT) devices have less processing power, storage, and power consumption than computers or other complicated electronic devices. Therefore, the usage area of IoT devices is limited due to having these three features. For instance, a device with a low processing power means less computation and code execution. The disadvantage of resource constraints creates advantages such as cheapness and less power consumption of IoT devices. Using IoT devices in an application requires a well-done specification analysis. The advantages need to outnumber the disadvantages of the application. The comparison between sophisticated devices (computer, mobile phone) and IoT devices are generally compared based on price and power consumption in the system. However, the most important part is mostly ignored which is security. An application on a computer or a mobile phone will use more processing power and will be able to run cryptographic algorithms that require more computational power. IoT devices may lack to process huge computations of cryptographic algorithms. Therefore, it is more difficult to ensure security with IoT devices.

Most IoT devices do not have an operating system to execute programs dynamically. IoT devices can be used as stations or access points in a local network or mesh networks [1]. They can broadcast data in the local network. This behavior may protect them from threats that come over the Internet. However, it causes a critical security vulnerability in the local network. Any device within the range of the local network can access the network. It can spread inconsistent data by impersonating the devices found in the application, making the network unusable by constantly sending data, and collecting data such as important personal information in the application and misusing it. To solve this physical threat, we decided to use an indoor positioning system (IPS). In IoT applications, without human interaction, and without a user interface, determining the location of the devices in the communication network is of great importance in terms of secure device management. Furthermore, it should not be forgotten that a huge communication network that grows with devices is expected [2, 3]. Positioning can monitor IoT devices, with information related to multiple reference points within the located area. It is possible to diversify examples of outdoor localization such as global navigation satellite system (GNSS) including global positioning system (GPS), global navigation satellite system (GLONASS), Galileo, and BeiDou [2]. Among these, the most common one is the GPS. However, these outdoor positioning systems cannot meet the expected performance for detecting devices in indoor environments due to the density of objects and signal attenuation by various building materials. For this purpose, the IPS technique is examined to determine the location of objects where GPS cannot determine the position. In various IoT applications such as smart home applications, IoT devices can be mostly used indoors and in small buildings. Therefore, localization using Wi-Fi and Bluetooth is used instead of GPS.

Considering the physical tracking of the devices, the distance of the devices to each other or the distance to the

wireless access point will allow us to have information about the device's location. In our implementation and benchmark tests, the location of the IoT devices that are ESP32-WROOM-32 version of ESP32, is determined by using IPS. If the ESP32 gateway is aware of the location information of all devices in the IoT application, it can decide which device is legitimate and which device is an external threat. ESP32 [4] supports both Wi-Fi and Bluetooth low energy (BLE) wireless communication. Therefore, RSSI is used as an indicator of the strength of the signal. The strength of the signal is expressed in decibel milliwatts (dBm). As the distance increases, the signal strength will decrease [5]. While dBm has a definite value with international validity, the received signal strength indicator (RSSI) value is determined by companies and has no definite value. Its value is determined as a percentage. At -90 dBm, the signal strength begins to get very low, and loss of control occurs. Signal loss in a short distance is due to logarithmic variation and ideal signal strength is determined between -30 and -80 dBm. The presence of the devices may be computed with such as the trilateration method where the relative distance from each receiver is calculated based on the RSSI value.

In the experimental study, the ESP32 device is located in a room with four reference nodes (ESP32 devices) whose locations are predetermined. It has been observed that the location of a device outside the room can be detected by RSSI value. The data transmission of the devices that is not in the specified area is blocked. In addition, the location information of the device belonging to the application is calculated with RSSI and the error rate is specified.

The remainder of the paper is organized as follows: Section 2 provides a state-of-the-art review on the methodologies and techniques of the indoor position systems. Section 3 gives brief information about implementation of the cases of ESP32 positioning and the experimental studies are presented and discussed. Finally, Section 4 gives some concluding remarks and future directions.

II. Related Work

Misal et al. [6] represented a prototype that includes determining the position of three ESP32 devices in the indoor area. For this purpose, RSSI information is gathered with BLE beacon and transmitted to the server via MQTT protocol in order to calculate RSSI to distance. The trilateration algorithm also predicts the coordinate of the BLE beacon with the distance information. The output of the study gives accuracy up to 2.3 meters to the actual position of the BLE beacon.

GPS is not proposed for tracking physically indoor devices due to no visibility and the disadvantages of signal spreading from walls. AlQahtani et al. [7] suggested a proximity-based authentication on the ad-hoc networks via Wi-Fi communication by calculating Euclidean distance with device service set identifier (SSID), basic service set identifier (BSSID), and RSSI information. Sophia et al. [8] determined the coordinates of four ESP32 devices with a fixed location using RSSI and trilateration algorithm by using BLE based indoor positioning system. This reference [9] is yet another work using the trilateration algorithm to perform an indoor navigation system where a mobile application assists the users to navigate inside a building without the need for external maps or human intervention by using BLE. Dijkstra algorithm is used to indicate the shortest path in their navigation system.

The participation of the students in the class was carried out with location information using Bluetooth [10]. The Bluetooth-based indoor positioning is preferred because of the various easily accessible devices such as mobile phones, smartwatches, and smart wearables with Bluetooth wireless communication technology. Also, Bluetooth has ultra-low power consumption with a small amount of data transmission. Students are registered with their mobile phone's media access control (MAC) address. Fingerprinting technique was used to collect and verify RSSI, and trilateration algorithm was used to calculate the distance using RSSI values.

Wi-Fi-based indoor positioning techniques are indicated with the latest research results by comparing range-based positioning methods and performance in terms of accuracy, complexity, extensibility, and cost [11].

In the paper [12], a random statistical method is proposed to improve the positioning accuracy of IPS using Wi-Fi fingerprinting. And the suggested method is compared with weighted k-nearest neighbor (WKNN) algorithm based on Euclidean distance to indicate the accuracy of indoor positioning. The experimental result of the paper is that the statistical method with the maximum positioning error is less than 0.75 meters, while the average positioning error with the WKNN algorithm is 1.5 meters. Wi-Fi fingerprint positioning technique is mainly described by He and Chan [13]. Different from the application areas of the studies mentioned in the literature, the security of the devices has been tried to be ensured. Wireless communication skills were tested by using an IoT device with limited processing capability instead of the advanced devices used in the studies.

III. Implementation and Testbed

The security need of IoT applications may vary according to the resource constraints of IoT devices and the sensitivity of the data. Our study aims to perform physical tracking of resource-constrained devices that cannot run compute-intense cryptographic algorithms due to the fact that cryptographic algorithms that can ensure data confidentiality and device verification include computations that require processing power. For this purpose, our example case is four ESP32 IoT devices located at fixed points in an indoor area, communicating with each other and transmitting their data to the gateway. It is aimed to ensure that our devices are in their positions without human intervention so that the data flow transmitted from these devices is not interrupted by a physical intervention. ESP32 devices work as both stations and access points. Thus, RSSI signals were collected and sent to the gateway with the MQTT protocol for distance calculation. The fixed position and distance information of our devices are shown in the Figure 1. At the same time, the actual distance information of our devices is recorded on our server with the device's MAC information to compare with the calculated RSSI to distance. Distance from RSSI information was calculated with the following formula [6]. Indicated n in the formula, used as 4 in our calculation, is an external factor varying between 2 and 4.

$$Distance = 10^{\wedge}(Measured\ Power - RSSI)/10*n \quad (1)$$

As seen from Figure 1, four ESP32 devices are positioned to form a rectangular area and act as access points. ESP32 device operating in station (STA) mode is placed in this area and it scans Wi-Fi and collects RSSI data periodically according to the four devices at our reference points. The collected RSSI values related to each device are sent to the

gateway located on the Raspberry Pi using the MQTT protocol. And the RSSI values are stored in the server. The server also keeps the actual distance values of the ESP32 devices according to the reference points. Mosquitto is used as the message queue telemetry transport (MQTT) broker and includes added Python script plugin to calculate the distance according to the RSSI-to-distance formula. The most repeated out of 10 collected RSSI values is taken as an input to the formula. The error rate is found by comparing the calculated distance value with the actual distance value.

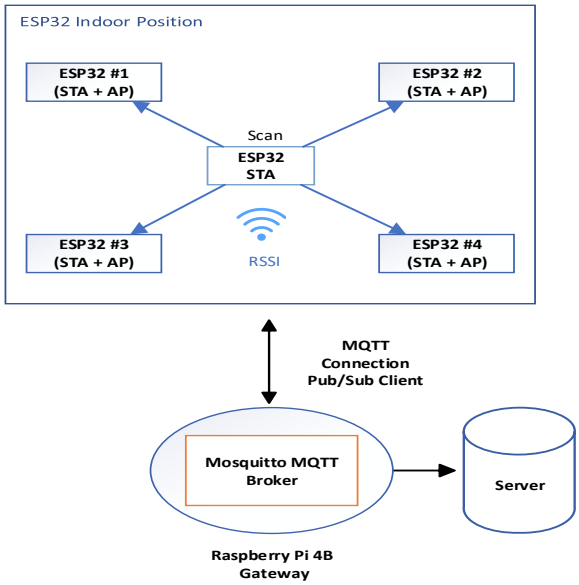


Fig. 1. The component, relation and interaction of indoor position scheme.

The RSSI values of the four reference fixed points are measured as between -61 and -67 that are shown in Figure 2. When the ESP32 device is away from the reference point, the RSSI value gets lower. RSSI values are measured according to the locations within this area where device boundaries are specified. The reference point is determined as respectively 4 and 2, and the situations where the device is inside and outside the area are considered. The device and its reference nodes are examined in 4 cases that are illustrated in Figure 3. The first case is positioned so that the device is outside the reference points. And the actual distance between the device's current location and the reference points is set to more than 1 meter. The purpose is to detect an unauthorized device that does not belong to the application. In this way, the data of the device whose location is not verified will not be included in the network.

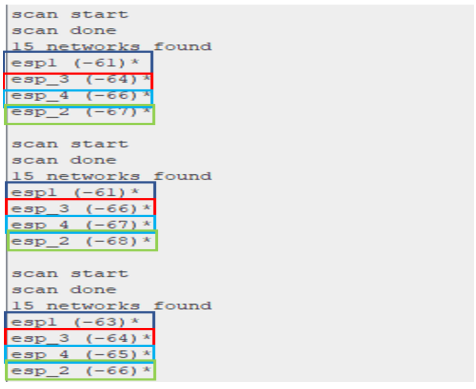


Fig. 2. The output of RSSI value of references nodes at fixed points.

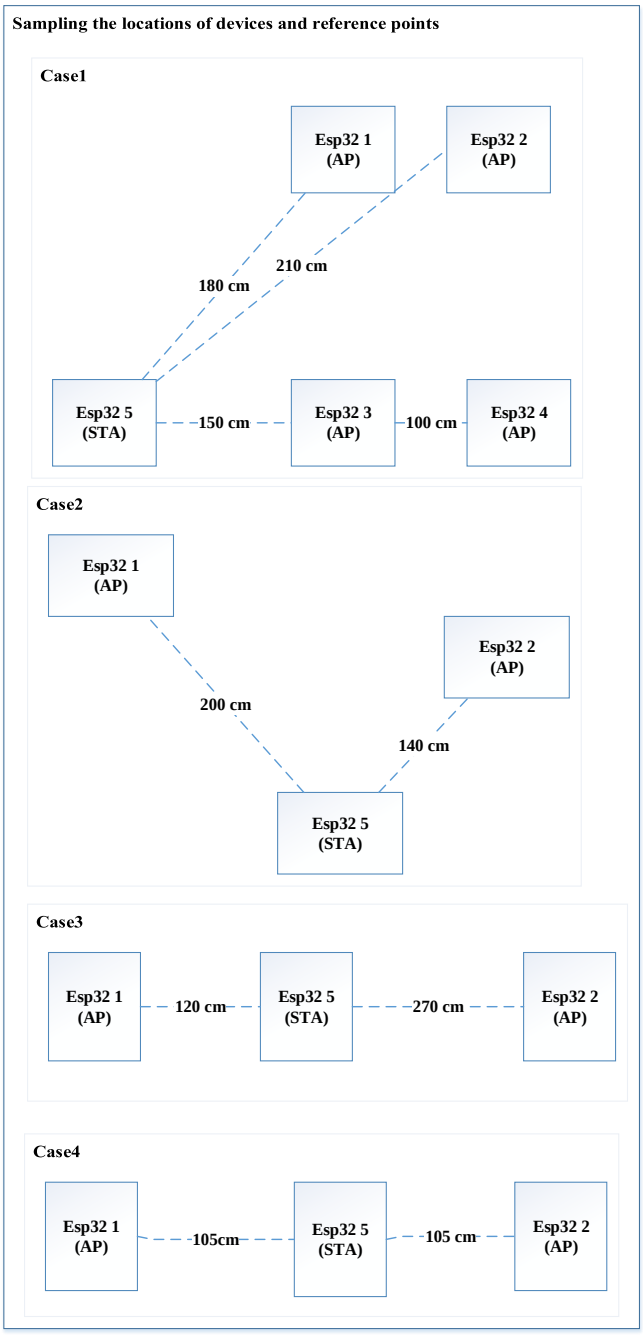


Fig. 3. RSSI value of references nodes at fixed points.

In Case2 and Case3, the number of reference nodes has been reduced to 2 and the device is positioned between the reference points. Distance based on RSSI values is calculated by positioning away from more than 1 meter between reference points and the ESP32 device. And in the last case, the RSSI value was measured at a distance of approximately 1 m between 2 reference points.

The results of RSSI measurement and RSSI-to-distance formula calculation 4 cases are shown in Table 1. The measured power value in the formula means the RSSI value measured at 1m. Considering the actual distance and the calculated distance, the error rate is indicated as a percentage.

TABLE III. ACTUAL DISTANCE COMPARED WITH RSSI-TO-DISTANCE

References Nodes	RSSI	Measured Power	N	Distance (cm)	Result From Calculation (cm)	Distance Error (cm)	Average Error Margin (%)
Case1 - Four References Nodes / ESP32 outside							
ESP32 1	-74	-68	4	180	141	39	20.54
ESP32 2	-85	-68	4	210	266	56	
Esp32 3	-77	-68	4	150	167	17	
Esp32 4	-90	-68	4	250	354	104	
Case2 - Two References Nodes / ESP32 inside							
ESP32 1	-40	-28	4	200	199	1	2.75
ESP32 2	-33	-28	4	140	133	7	
Case3 - Two References Nodes / ESP32 inside							
ESP32 1	-31	-27	4	120	125	5	7.26
ESP32 2	-46	-27	4	270	298	28	
Case4 - Two References Nodes / ESP32 inside							
ESP32 1	-71	-69	4	105	112	7	6.66
ESP32 2	-71	-69	4	105	112	7	

In the first case, as 4 devices are used as access points, the coverage area is much higher than the following cases that also causes higher error rates. Another core reason of the error is the electromagnetic interference as the experiments are not proceeded in a laboratory environment. Also the ESP32 device is not so much stable in wireless communication. In the remaining cases, the error rate is much lower. Considering all the cases, error rates are acceptable to detect whether the device is in the coverage area or not.

IV. CONCLUSION

In our study, unlike cryptographic algorithms that require high processing power to verify devices in IoT applications, physical tracking has been used for a simple authentication. By calculating the distance with the RSSI value, it is examined whether the devices are in the coverage area we have determined. The ESP32 devices are located in a room and have been tested to observe whether there is interference to the network from a device outside the home or not. To experiment this, measurements are taken at different locations according to the reference points of the ESP32 devices. The process is repeated with 2 and 4 nodes at the reference points. While the average RSSI value at a distance of 1 m from the reference points of the ESP32 device is -67 dBm, the RSSI value (-90 dBm) of an external device and its distance calculation shows that the device is not in the coverage area and it is unauthorized. The error rates that occur when detecting that the ESP32 device in its location are negligible due to the fact that the environment is affected by the magnetic field.

In future works, moving devices can be detected in the environment and the physical tracking of the RSSI data collected by both BLE and Wi-Fi communication technologies will be tested by trilateration and fingerprint methods.

REFERENCES

[1] Ö. Şeker and G. Dalkiliç, “Implementation and Performance Analysis of a Multi-Protocol Gateway,” in 2022 Innovations in Intelligent Systems and Applications Conference (ASYU),” pp. 1-6, September 2022.

[2] S. M. Asaad and H. S. Maghdid, “A comprehensive review of indoor/outdoor localization solutions in iot era: Research challenges and future perspectives,” Computer Networks, 109041, 2022.

[3] S. J. Hayward, K. van Lopik, C. Hinde and A. A. West, “A survey of indoor location technologies, techniques and applications in industry,” Internet of Things, vol. 20, 100608, ISSN 2542-6605, 2022.

[4] ESP32-S ESP-IDF programming guide, Jan. 2023, [online] Available: https://docs.espressifcomlprojects/esp-idf/en/v4.2-beta1/esp32s2/esp-idf-en-v4.2-beta1-esp32s2.pdf.

[5] S. Akleylek, E. Kiliç, B. Söylemez, T. E. Aruk and A. Çavuş,“Kapalı mekan konumlandirma üzerine bir çalişma, ” Mühendislik Bilimleri ve Tasarım Dergisi, vol. *8*(5), pp. 90-105, 2020.

[6] S. R. Misal, S. R. Prajwal, H. M. Niveditha, H. M. Vinayaka and S. Veena, “indoor positioning system (IPS) using ESP32, MQTT and Bluetooth,” in Fourth International Conference on Computing Methodologies and Communication (ICCMC),” pp. 79-82, March 2020.

[7] A. A. S. AlQahtani, H. Alamleh and B. Al Smadi, “IoT Devices Proximity Authentication In Ad Hoc Network Environment,” in International IOT, Electronics and Mechatronics Conference (IEMTRONICS), pp. 1-5, June 2022.

[8] S. Sophia, B. Maruthi Shankar, K. Akshya, AR. C. Arunachalam, V. T. Y. Avanthika and S. Deepark,” Bluetooth Low Energy based Indoor Positioning System using ESP32,” in Third International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 1698-1702, 2021.

[9] A. Rakshith, V. H. Navneeth, P. S. Dravya, K. U. Holla, K. N. Pushpalatha, “Indoor Navigation System using BLE and ESP32,” in International Journal for Research in Applied Science & Engineering Technology (IJRASET), November 2020.

[10] A. Puckdeevongs, N. K. Tripathi, A. Witayangkurn and P. Saengudomlert,” Classroom Attendance Systems Based on Bluetooth Low Energy Indoor Positioning Technology for Smart Campus,” Information, vol. 11(6):329, 2020, https://doi.org/10.3390/info11060329.

[11] F. Liu, J. Liu, Y. Yin, W. Wang, D. Hu, P. Chen and Q. Niu,” Survey on WiFi-based indoor positioning techniques,” The Instution of Engineering and Technology, vol. 14(9), pp. 1372-1383, 2020.

[12] D. B. Ninh, J. He, V. T. Trung, D. P. Huy, “An effective random statistical method for Indoor Positioning System using WiFi fingerprinting, ”Future Generation Computer Systems, vol. 109, pp. 238-248, 2020.

[13] S. He and S. H. G. Chan, “Wi-Fi Fingerprint-Based Indoor Positioning: Recent Advances and Comparisons,” IEEE Communications Surveys & Tutorials, vol. 18(1), pp. 466-490, 2016.

Enhancing Zero-Shot Learning Based Sign Language Recognition Through Hand Landmarks and Data Augmentation

Received: 30 January 2023; Accepted: 5 March 2023 *Research Article*

Giray Sercan ÖZCAN
Department of Computer Engineering
Baskent University
Ankara, Turkey
gozcan@baskent.edu.tr
0000-0002-8770-2085

Emre SÜMER
Department of Computer Engineering
Baskent University
Ankara, Turkey
esumer@baskent.edu.tr
0000-0001-8502-9184

Yunus Can BİLGE
Image and Video Processing Group
HAVELSAN
Ankara, Turkey
ycbilge@havelsan.com.tr
0000-0003-2811-3747

***Abstract*— Sign language recognition remains a challenging area and may require a considerable amount of data to obtain satisfactory results. To overcome this, we use readily available motion text data in addition to videos for achieving recognition of unobserved classes during the training phase. Zero-Shot Sign Language Recognition (ZSSLR) with a novel technique is focused on this work, which learns a model from seen sign classes and recognizes unseen sign classes. To achieve this, the ASL-Text dataset is used which combines the video of word signs and descriptions in sign language dictionaries. Moreover, this dataset consists of sign language classes and their corresponding definitions in the sign language dictionary. In various Zero-Shot Learning (ZSL) applications, it is common for datasets to contain a limited number of examples for numerous classes across different domains. This makes the problem of sign language recognition extremely challenging. We try to overcome this by using a new approach which includes augmented data and hand landmarks. The experiment on augmented data resulted in 50.91 for top-5 accuracy. Hand landmarks are used with unaugmented data which is applied to average and LSTM deep learning layers resulting in 49.41 and 48.21 for top-5 accuracies, respectively.**

Keywords—sign language recognition, zero-shot learning

I. INTRODUCTION

The objective of Sign Language Recognition (SLR) systems that have been created is to convert sign language into either text or speech, with the goal of enabling communication between deaf people and those who can hear. This process has a significant impact on society, but the complexity of hand and finger actions make SLR very challenging. The task of developing systems for recognizing sign language remains a formidable challenge. Although sign language definitions are well-defined and organized, slight variations in body posture, hand movements, facial expressions and hand positioning can drastically alter the intended meaning of the sign language [3], [4]. Distinguishing and annotating the well-established hand shapes within sign languages can prove to be a formidable task, especially in situations where there are variations in viewpoints [31]. Moreover, akin to how natural languages transform and incorporate diversity throughout history, sign languages also undergo modifications and accept variations as time passes. Therefore, a model that can adapt to these changes is needed. The current methods used for SLR necessitate a considerable quantity of labeled information for each class. [11], [12], [13], [17]. In this study, unseen sign language classes were recognized without annotated visual data by taking advantage of sign language descriptions. In this regard, Zero-shot Sign Language Recognition (ZSSLR) has been defined in [5]. Unlike normal supervised learning, the ZSSLR method tries to predict classes that are not seen in the training phase. Compared to common ZSL studies [6], [7], [8], [9], ASL-Text [5] dataset used in this study contains significantly fewer examples per class for training which makes this task a hard zero-shot learning problem [23]. In general, ZSSLR consists of two primary components. The first component focuses on the arrangement of visual information by utilizing 3D-CNN and LSTM to examine both the temporal and spatial structure. The second one is the ZSL component which contains text data. The system developed with these two components aims to learn the closest text description of the visual data. The ASL-Text dataset was created using easily accessible and expert-prepared sign language definitions of words in the sign language dictionary. In the current study, we improved the effort introduced in [5]. We applied data augmentation and hand landmarks extraction by feeding them to the deep learning layers such as mean layer and LSTM layer. The experimental results were evaluated by top-1, top-2, and top-5 accuracies. The rest of the paper is proceeded as follows: The previous studies are examined in Section 2, the proposed approach is explained in Section 3, the applied experiments is presented in section 4, the results are discussed in Section 5 and the conclusion is addressed in Section 6.

II. RELATED WORK

SLR has been a subject of research for more than thirty years [32]. There are two main types of SLR techniques that have gained widespread popularity. These are (i) Isolated SLR [33], which focuses on recognizing individual instances of signs, and (ii) Continuous SLR [34], which aims to recognize all signs in sign language sequences. Our research falls under the category of Isolated SLR since we focus on recognizing individual sign instances. In the initial stages of SLR research, hand-crafted features were predominantly utilized in conjunction with classifiers such as support vector machines [33], [35]. Additionally, Conditional Random Fields, Hidden Markov Models (HMM), and neural network based techniques were also investigated as potential methods to model temporal patterns [36], [37]. More recently, various SLR methodologies have been proposed that leverage deep learning techniques [38], [39]. ZSL has garnered significant attention in the fields of learning and vision research in recent years, particularly after the groundbreaking works of Lampert et al. [40] and Farhadi et al. [6]. The majority of ZSL methodologies depend on transferring semantic knowledge from observed classes to those that have not been seen. In recent years, various studies have been conducted for action recognition based on semantic

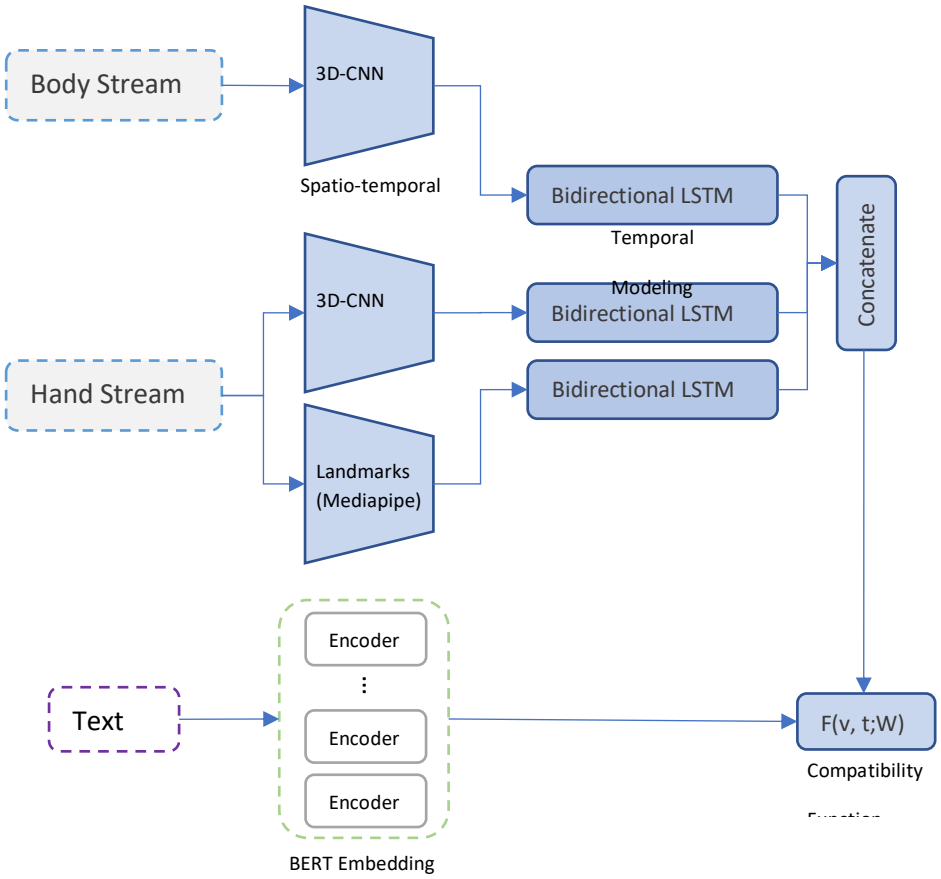


Fig. 1. General outline of the study

embedding [42], regression [43], and many others [44], [45], [46], [1], [2].

Bilge et al. [5] are the first ones who defined the ZSSLR problem and proposed a solution. They created the ASL-Text dataset by combining sign language videos with related text descriptions in the sign language dictionary, which is also used in this study. They divided the dataset into hand and body streams. They applied the embarrassingly simple zero-shot learning (ESZSL) [21], semantic auto encoder (SAE) [22], and logistic label embedding (LLE) [5] methods to the streams and obtained various results. The experiment in which they applied the LLE method by combining the hand and body streams gave the best result of 20.9% for top-1 accuracy.

In their subsequent work [20], the authors enhanced the ASL-Text dataset by adding binary feature matrices in addition to the text descriptions used in the second component of the ZSSLR system. They also created two new benchmark datasets, MS-ZSSLR-W and MS-ZSSLR-C, and applied a shift-based CNN [24] in addition to the 3D-CNN and LSTM used in their previous work. They also introduced the problem of Generalized Zero-Shot Sign Language Recognition (GZSSLR), in which the model is trained to recognize both observed and unobserved classes. The results obtained in the study are given in two different settings: ZSL and generalized zero-shot learning (GZSL). ZSL setting achieved 31.3% and 14.7%, the GZSL setting achieved 26.9% and 34.7% for top-1 accuracies on ASL-Text and MS-ZSSLR-C datasets, respectively.

III. METHODOLOGY

The general structure of the developed architecture can be seen in Figure 1. In this section, first, the problem definition is presented and then solution methods are described.

Problem definition: ZSSLR relies on two distinct information sources: a *visual domain* that comprises sign language videos and a *textual domain* consisting of explanations for the gestures and motions performed in these videos. During the training phase videos, labels and sign language descriptions of the observed classes $\mathbb{C}_s$ are incorporated. The objective at test phase is to classify the unobserved novel classes $\mathbb{C}_u$.

The set of training samples, denoted by $S_{tr} = \{(v_i, c_i)\}_{i=1}^{N}$ contains N instances. Here, v_i represents the i-th training video, and $c_i \epsilon \mathbb{C}_s$ is the corresponding sign language video. It is assumed that there is access to the textual descriptions, denoted by $\tau(c)$ for each class. The objective is to acquire a zero-shot classifier capable of assigning each test video to a class in $\mathbb{C}_u$ based on the textual descriptions provided.

The aim is to establish zero-shot classifier model that employs label embedding. To achieve this, a compatibility function, denoted as $F(v, c)$, is defined to measure the similarity between a given input video and class pair, generating a score that reflects the degree of confidence that video v belongs to class c. Based on the compatibility function F, zero-shot classification function at test time $f: \mathbb{V} \longrightarrow \mathbb{C}_u$ is defined as:

$$f(v) = \arg\max F(v, c) \quad (1)$$

$c \in \mathbb{C}_u$

Using this method, the compatibility function can classify novel unobserved classes that are encountered during the testing phase.

Short-term spatiotemporal representations were obtained with I3D [30] while longer-term dependencies were found with bi-LSTM [25]. The goal of using bi-LSTM [25] is to capture longer term dependencies as effectively as possible. Hand landmarks are extracted from streams using Mediapipe [26]. Text-based class embeddings for sign language descriptions are extracted using BERT [27], which is state-of-the-art in this area. BERT is essentially an encoder stack. The advantage of BERT over word2vec [28] and glove [29] is that the extracted representation is more sensitive to other words in the sentence. The bi-linear compatibility function utilized establishes a relation between the video and representations of class as follows:

$$F(v, c) = \theta(v)^T W \phi(\tau(c)) \quad (2)$$

$\theta(v)$ represents the d-dimensional representation of video v, while $\phi(\tau(c))$ is the m-dimensional BERT embedding of the textual descriptions, $\tau(c)$, for class c. The compability matrix, denoted by W and comprising $d \times m$ dimensions. For calculating this matrix, we use the formula given in [5].

IV. Experiments

Four experiments were conducted, these are (i) the baseline study that achieved the best results in [5], (ii) the study conducted with augmented data, (iii) the study conducted using average pooling layer on hand landmarks, and (iv) the study conducted using LSTM on hand landmarks.

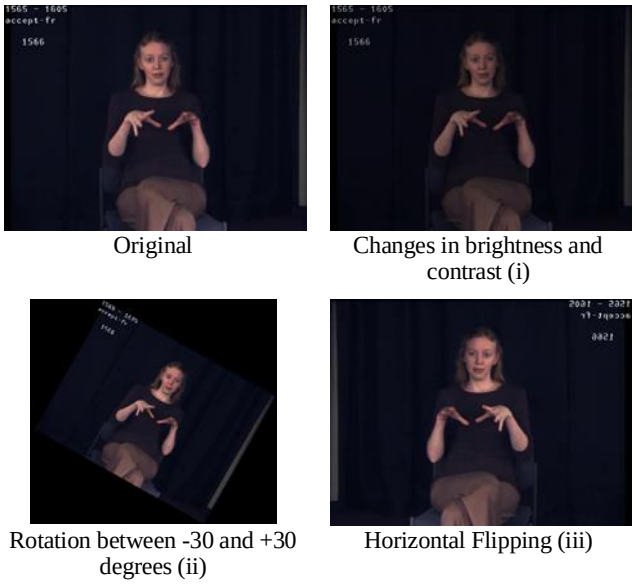
Firstly, hand streams were extracted from ASL-Text which contains signers' body streams. Therefore, two streams were worked on: Body stream and hand stream. These videos were split into 8-frame small video segments. Then we extracted short-term spatiotemporal features and longer-term dependencies from these segments.

The applied augmentations can be seen in Figure 2. These are (i) changes in brightness and contrast, (ii) rotation between -30 and +30 degrees, (iii) horizontal flipping and (iv) mix of augmentations mentioned in (i), (ii), (iii). The dataset was increased five-fold in this way, spatiotemporal representations were obtained, and longer-term dependencies were captured.

Results were obtained by extracting hand landmarks and feeding them to the average pooling layer or LSTM.

V. Results

The results can be seen in Table 1, which includes our study conducted with augmented data and landmarks. In the baseline study, a success rate of 20.38 was achieved on the validation dataset, while for the top-1, top-2, and top-5 on the test dataset, success rates of 16.94, 27.31, and 47.91 were obtained, respectively. In the study conducted with augmented data, a success rate of 19.98 was achieved on the validation dataset, while for the top-1, top-2, and top-5 on the test dataset, success rates of 19.11, 30.89, and 50.91 were found, respectively. In the study conducted using hand landmarks with average pooling, a success rate of 20.4 was obtained on the validation dataset, while for the top-1, top-2, and top-5 on the test dataset, success rates of 18.7, 28.32, and 49.41 were achieved, respectively. In the study conducted using hand landmarks with LSTM, a success rate of 19.98 was found on the validation dataset, while for the top-1, top-2, and top-5 on the test dataset, success rates of 19.31, 28.76, and 48.21 were achieved, respectively.



Original | Changes in brightness and contrast (i)

Rotation between -30 and +30 degrees (ii) | Horizontal Flipping (iii)

Fig. 2. Applied augmentations

Table 1 shows that the results obtained from the experiments are better than those obtained from the baseline study.

Experiments	Val (30 Classes)	Test (50 classes)		
	Top-1	Top-1	Top-2	Top-5
Baseline	20.38	16.94	27.31	47.91
Augmented Data	19.98	19.11	30.89	50.91
Landmarks (average pooling)	20.4	18.7	28.32	49.41
Landmarks (LSTM)	19.98	19.31	28.76	48.21

TABLE IV. Experimental Results

VI. Conclusion

In this study, we aim to do sign language recognition with zero-shot learning method. We utilized techniques to increase the amount of data available for training and extracted hand landmarks by inputting them into deep learning layers like the mean layer and LSTM layer. Even with average pooling, using hand landmarks has led to an improvement in results. The best results are obtained from the study conducted using hand landmarks and LSTM. Better results can be obtained by generating more augmented data.

References

[1] J. Qin, L. Liu, L. Shao, F. Shen, B. Ni, J. Chen, and Y. Wang, "Zeroshot action recognition with error-correcting output codes," in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2017, pp. 2833–2842.

[2] M. Hahn, A. Silva, and J. M. Rehg, "Action2vec: A crossmodal embedding approach to action learning," in The British Machine Vision Conference (BMVC), September 2018.

[3] W. C. Stokoe Jr. “Sign language structure: An outline of the visual communication systems of the american deaf.” Journal of deaf studies and deaf education, 10(1):3–37, 2005.

[4] Y. Wu and T. S. Huang, “Vision-based gesture recognition: A review. In International Gesture Workshop,” pp.103–115. Springer, 1999.

[5] Y. C. Bilge, N. İ. Cinbiş, R. G. Cinbiş, “Zero-Shot Sign Language Recognition: Can Textual Data Uncover Sign Languages?,” in British Machine Vision Conference (BMVC), 2019

[6] A. Farhadi, I. Endres, D. Hoiem, and D. Forsyth. “Describing objects by their attributes,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., pp.1778–1785. IEEE, 2009.

[7] C. H. Lampert, H. Nickisch, and S. Harmeling, “Attribute-based classification for zero-shot visual object categorization,” IEEE Transactions on Pattern Analysis and Machine Intelligence, 36(3):453–465, 2014.

[8] G. Patterson and J. Hays, “Sun attribute database: Discovering, annotating, and recognizing scene attributes,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., pp.2751–2758. IEEE, 2012

[9] C. Wah, S. Branson, P. Welinder, P. Perona, and S. Belongie. “The caltechucsd birds-200-2011 dataset,” 2011.

[10] P. Kumar, H. Gauba, P.P. Roy , D.P. Dogra, “A multimodal framework for sensor based sign language recognition,” Neurocomputing, vol.259, pp.21-38, 2017.

[11] O. Koller, J. Forster,H. Ney, “Continuous sign language recognition: Towards large vocabulary statistical recognition systems handling multiple signers,” in Computer Vision and Image Understanding, vol.141, pp.108-125, 2015.

[12] S. Tamura and S. Kawasaki, “Recognition of sign language motion images,” Pattern recognition, vol. 21, no. 4, pp. 343–353, 1988.

[13] M. B. Waldron and S. Kim, “Isolated asl sign recognition system for deaf persons,” IEEE Transactions on rehabilitation engineering, vol. 3, no. 3, pp. 261–271, 1995.

[14] M. W. Kadous et al., “Machine recognition of auslan signs using powergloves: Towards large-lexicon recognition of sign language,” in Proc. Workshop on the Integration of Gesture in Language and Speech, vol. 165, 1996

[15] M. Zahedi, D. Keysers, T. Deselaers, and H. Ney, “Combination of tangent distance and an image distortion model for appearancebased sign language recognition,” in Joint Pattern Recognition Symposium, 2005, pp. 401–408

[16] H. Cooper and R. Bowden, “Sign language recognition using boosted volumetric features,” in Proc. IAPR Conference on Machine Vision Applications, 2007, pp. 359–362

[17] O. Koller, O. Zargaran, H. Ney, and R. Bowden, “Deep sign: hybrid cnn-hmm for continuous sign language recognition,” In British Machine Vision Conference, 2016.

[18] K. Grobel and M. Assan, “Isolated sign language recognition using hidden markov models,” In IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, vol. 1, pp. 162–167. IEEE, 1997.

[19] C. L. Huang and W.Y. Huang. “Sign language recognition using model-based tracking and a 3d hopfield neural network,” Machine vision and applications, 10(5-6):292–307, 1998

[20] Y. C. Bilge, N. İ. Cinbiş, R. G. Cinbiş, “Towards Zero-Shot Sign Language Recognition,” Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 1, pp. 1217-1232, 2023.

[21] B. Romera-Paredes and P. Torr, “An embarrassingly simple approach to zero-shot learning,” in Proc. Int. Conf. Mach. Learn., 2015, pp. 2152–2161.

[22] E. Kodirov, T. Xiang, and S. Gong, “Semantic autoencoder for zero-shot learning,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2017, pp. 3174–3183.

[23] N. Madapana and J. P. Wachs, “Hard zero shot learning for gesture recognition,” in IAPR International Conference on Pattern Recognition, 2018, pp. 3574–3579.

[24] J. Lin, C. Gan, and S. Han, “Tsm: Temporal shift module for efficient video understanding,” in Proc. IEEE International Conference on Computer Vision, 2019, pp. 7083–7093.

[25] A. Graves and J. Schmidhuber, “Framewise phoneme classification with bidirectional lstm and other neural network architectures,” Neural Networks, vol. 18, no. 5-6, pp. 602–610, 2005.

[26] C. Lugaresi, J. Tang, H. Nash, C. McClanahan, E. Uboweja, M. Hays, F. Zhang, C.L. Chang, M. Yong, J. Lee, W.T. Chang. “Mediapipe: A framework for perceiving and processing reality.” InThird Workshop on Computer Vision for AR/VR at IEEE Computer Vision and Pattern Recognition (CVPR) 2019 Jun (Vol. 2019).

[27] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, “BERT: Pretraining of deep bidirectional transformers for language understanding,” in NAACL, 2019, pp. 4171–4186.

[28] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, and J. Dean,“Distributed representations of words and phrases and theircompositionality,” in Proc. Adv. Neural Inf. Process. Syst., 2013, pp.3111–3119.

[29] J. Pennington, R. Socher, and C. Manning, “Glove: Global vectors for word representation,” in Proc. of conference on empirical methods in natural language processing (EMNLP), 2014, pp. 1532–1543.

[30] J. Carreira and A. Zisserman, “Quo vadis, action recognition? A new model and the kinetics dataset,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2017, pp. 6299–6308.

[31] C. Neidle, A. Thangali, and S. Sclaroff, “Challenges in development of the american sign language lexicon video dataset (asllvd) corpus,” in Proc. 5th Workshop on the Representation and Processing of Sign Languages: Interactions between Corpus and Lexicon, Language Resources and Evaluation Conference (LREC) 2012, 2012

[32] S. Tamura and S. Kawasaki, “Recognition of sign language motion images,” Pattern recognition, vol. 21, no. 4, pp. 343–353, 1988.

[33] H. Wang, X. Chai, X. Hong, G. Zhao, and X. Chen, “Isolated sign language recognition with grassmann covariance matrices,” ACM Transactions on Accessible Computing (TACCESS), vol. 8, no. 4, p. 14, 2016.

[34] N. Cihan Camgoz, S. Hadfield, O. Koller, H. Ney, and R. Bowden, “Neural sign language translation,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2018, pp. 7784–7793.

[35] M. B. Waldron and S. Kim, “Isolated asl sign recognition system for deaf persons,” IEEE Transactions on rehabilitation engineering, vol. 3, no. 3, pp. 261–271, 1995.

[36] K. Grobel and M. Assan, “Isolated sign language recognition using hidden markov models,” in IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, vol. 1, 1997, pp. 162–167.

[37] C.-L. Huang and W.-Y. Huang, “Sign language recognition using model-based tracking and a 3d hopfield neural network,” Machine vision and applications, vol. 10, no. 5-6, pp. 292–307, 1998.

[38] D. Li, C. Rodriguez, X. Yu, and H. Li, “Word-level deep sign language recognition from video: A new large-scale dataset and methods comparison,” in The IEEE Winter Conference on Applications of Computer Vision, 2020, pp. 1459–1469.

[39] B. Saunders, N. C. Camgoz, and R. Bowden, “Progressive transformers for end-to-end sign language production,” in European Conference on Computer Vision (ECCV), 2020.

[40] C. H. Lampert, H. Nickisch, and S. Harmeling, “Learning to detect unseen object classes by between-class attribute transfer,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2009, pp. 951–958.

[41] J. Liu, B. Kuipers, and S. Savarese, “Recognizing human actions by attributes,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2011, pp. 3337–3344.

[42] M. Jain, J. C. van Gemert, T. Mensink, and C. G. Snoek, “Objects2action: Classifying and localizing actions without any video example,” in Proc. IEEE Int. Conf. on Computer Vision, 2015, pp. 4588–4596.

[43] X. Xu, T. M. Hospedales, and S. Gong, “Semantic embedding space for zero-shot action recognition,” 2015 IEEE International Conference on Image Processing (ICIP), pp. 63–67, 2015.

[44] X. Xu, T. Hospedales, and S. Gong, “Transductive zero-shot action recognition by word-vector embedding,” International Journal of Computer Vision, vol. 123, no. 3, pp. 309–333, 2017.

[45] Q. Wang and K. Chen, “Alternative semantic representations for zero-shot human action recognition,” in Joint European Conference on Machine Learning and Knowledge Discovery in Databases, 2017, pp. 87–102.

[46] A. Habibian, T. Mensink, and C. G. Snoek, “Video2vec embeddings recognize events when examples are scarce,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 10, pp. 2089–2103, 2017.

Methods for Increasing the Cyber Resilience of Critical Infrastructures Methods for Increasing the Cyber Resilience of Critical Infrastructures

Received: 30 January 2023 Accepted: 6 March 2023 ***Research Article***

Fatih Furkan Bayar
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
fbayar@havelsan.com.tr
0000-0003-1157-482X

Sila Sibil Bardak
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
ssibil@havelsan.com.tr

Ender Saribay
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
esaribay@havelsan.com.tr

Ozmen Emre Demirkol, Ph.D.
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
oedemirkol@havelsan.com.tr

Mert Ozarar, Ph.D.
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
mozarar@havelsan.com.tr

***Abstract*— Cybersecurity is a critical topic that has become increasingly important in today's world, due to the increasing dependency on technology and interconnected systems. As digitalization increases, the need for cybersecurity measures becomes even more important for several systems that are crucial for society, nuclear facilities, energy systems, finance transportation and healthcare systems. Any damage to critical infrastructures from inside or outside will lead to the deterioration of the social order of countries, the loss of international reputation and the undermining of their credibility. The integration of information technology (IT) and operational technology (OT) within industrial control systems (ICS) has resulted in an expanding attack surface for cyber threats. In order to establish complete cyber-defence solution, innovative artificial intelligence solutions must be utilized alongside traditional cyber security approaches. In the digital transformation process of countries and organizations, the increasing cyber threats are addressed by explaining the five crucial solutions needed, based on international standards. This study aims to provide an overview of strategies to enhance the cyber security maturity level of critical infrastructures, examines both traditional cyber security approaches and artificial intelligence approaches. An architecture is specified to build cyber resilient critical infrastructures.**

Keywords—Critical Infrastructure, Operational Technology, Industrial Control Systems, Cyber Resilience, Artificial Intelligence

I. INTRODUCTION

In the 21st century, technology continues to advance, and people all over the world are becoming more dependent on it. Information technologies (IT) and operational technology (OT) are two examples of the concepts introduced by this discipline, which grew in popularity notably when the internet was discovered. Written sources were replaced by electronic sources when information began to be created, processed, stored, and consumed in an electronic context. As a result, information technologies have emerged as one of the most essential and rapidly evolving technological components of the 21st century. With benefits like quick access and processing power, as well as time and resource savings, information technologies have a significant impact on both the social structure of states and individual usage. Systems utilizing information technology, which are now widely employed in all industries, have become the main focus of evil individuals. Through the utilization of advanced technologies, cybercriminals are now able to engage in illegal acts, including gaining unauthorized access to information systems and compromising or exfiltrating data. It has become a top priority in national and international levels to prevent potential risks from adversarial individuals to information technology systems. Since attacks to cyber systems constantly increase and have more and more impact, the concept of cybersecurity has emerged, and security of technological systems became a fundamental concern. Cybersecurity is the set of all technologies employed by groups or individuals to protect their assets. Any entity having Internet connection naturally causes the attack surface to expand, which makes the protection necessary. Although the foundation of cybersecurity is information technology security, operational technology has continued to advance. Operational technology is the hardware and software that directly monitors and/or controls industrial assets, equipment, processes, and events in order to detect or implement changes [1]. The main reason operational technologies have not received top priority in terms of cybersecurity is that this field of technology typically operates at remote locations without direct Internet access, such as factories, production facilities, energy distribution centers, water treatment plants, or nuclear power plants. The very small attack surface created by the lack of internet connection on the devices operating the equipment in these situations virtually limits the prospect of an assault unless there is physical access. Today, however, the demand for remote equipment monitoring and control has resulted in widespread Internet access by the devices that manage the equipment. Due to this circumstance, the fields of information technology and operational technology have begun to merge into integrated systems. Critical infrastructures including those in the areas of transportation, health, energy, and military all rest on information and operational technology systems that, if they fail, will cause major disruptions to the state and society. It is important to consider national security while evaluating how secure critical infrastructures should be, as well as how resilient they should be to cyberattacks. To ensure the security of critical infrastructures, various cyber security solutions should be brought together and the

necessary infrastructure should be developed. To construct and improve the cyber resilience of critical infrastructures, policies should be created and put into place.

II. BACKGROUND

In this section, we aim to explain concepts such as cyber security, critical infrastructures, the convergence of technology and critical infrastructures, cyber attacks targeting these infrastructures, and the role of artificial intelligence in these concepts in order to effectively convey the details of our research.

A. Cyber Security

Cyber security is a concept involving ensuring the security of cyber systems, such as mobile phones, computers, websites, and servers. Even though these are the first devices that come into the mind when it is questioned what is tried to be protected in context of cyber security, the amount of devices that are to be protected is much more than those. For instance, it is possible to discuss the cyber security of operational technology devices, particularly those found in critical infrastructure. Therefore, the term cyber security covers a wide range of devices, which also means that ensuring cyber security of a complex environment consisting of many different types of devices is a challenging task.

Nowadays, the term cyber security is much more important than it was, e.g., 20 years ago. Recent developments in technology has shown that cyber environments are now places where the most critical operations are performed, such as money transactions, citizenship procedures, taking exams, submitting documents, which may include sensitive data, for crucial tasks, and many more daily-life cases where the cyber security is the key part for making it possible for these operations to be performed healthily without any dangerous consequences. Since the attackers know that the cyber environments are of great importance for most tasks, they improve their attack vectors more and more as the time goes on. The twenty first century can be referred to as the century of cyber cases since numerous cyber attacks have been performed on numerous organizations and targets, which include critical infrastructures as well.

B. Critical Infrastructure

W.J. Clinton, who was the president of the U.S. at the time, became the first one to use the term critical infrastructure in 1996. The term was first mentioned in the order named as “Executive Order 13010 - Critical Infrastructure Protection” [2]. Based on this executive order, a commission was founded in the U.S. to focus on critical infrastructures' cybersecurity, and related studies had been started. Several distinct pieces of hardware, software, and control equipment in the areas of information and operational technology come to mind when the assets and systems specified in this definition are taken into account. Therefore, physical hardware and virtualized solutions are combined to provide cybersecurity of critical infrastructures.

C. Convergence of IT & OT Systems

Systems for information technology and systems for operational technology were once considered to be independent systems. Information technology teams and operational technology teams were separate within organizations. Teams could only work on systems in which they have expertise. This situation started to alter in the 21st century, and the boundaries between the two disciplines vanished.

The requirements for rapid process execution, real-time execution, and decision tracking have evolved in the 21st century. Therefore, there is an increasing number of OT systems connected to at least one communication network or the Internet. They enable the flow of data into IT environments and the exchange of information between industrial control systems (ICS) components such as sensors and actuators via network connections. With the processing and analysis of this data in information environments, the status and performance of physical devices are monitored and useful statistics that can be used for process management are produced. Remote device configuration for OT systems is possible with IT systems.

It is obvious that combining OT and IT systems has many advantages, but it also carries significant risks. Systems that are not isolated in an environment where all OT and IT networks connected to the Internet are merged are more susceptible to cyberattacks, which can have severe material and physical repercussions.

D. Cyber Threats Against Critical Infrastructures

Industrial control systems are one of the most crucial aspects of the cybersecurity of critical infrastructures. It is feasible to completely halt these physically situated devices' operations and do significant harm with a cyberattack.

Due to newly discovered weaknesses in industrial control systems, which have emerged as a result of the confluence of the information and operational technology domains, these critical infrastructures are now the main target of cyberattacks. The usage of operational technology equipment for 30 to 50 years creates various cybersecurity risks, even while information technology devices are replaced every 3 to 5 years [3]. It is usually not possible to suspend the system and perform an upgrade on it because operational technologies, unlike information technologies, prioritize accessibility and integrity [3]. The attack surface for critical infrastructures has increased significantly due to the convergence of information and operational technology and the ability to access legacy industrial control systems from the virtual world via the Internet.

Since the 21st century, numerous cyberattacks such as the STUXNET attack on Iran's nuclear program, Havex, and Black Energy have been carried out against industrial control systems and critical infrastructures [4]. Some other notable examples of cyberattacks targeting industrial control systems include the Ukraine power grid attack in 2015 and the attack on the Saudi Arabian oil company Aramco. These attacks have utilized various techniques such as malware injection, phishing, and exploitation of vulnerabilities in software and hardware.

One of the most concerning techniques used in these attacks is the ability to gain access to and manipulate industrial control systems through Remote Access Trojans (RATs) and Advanced Persistent Threats (APTs). These types of malware allow attackers to remotely control and manipulate the functionality of industrial control systems, potentially causing damage or disruption to critical infrastructure, as well as collecting sensitive intelligence information. For instance, Havex is a type of RAT used against industrial systems and organizations. It is distributed to target systems by attackers

via phishing e-mails, malicious links, and by injecting the malware inside the software packages presented by ICS software providers through compromised websites [5]. After infecting a system found in a critical infrastructure, Havex downloads and installs its ICS plugin that scans for OPC servers from which it obtains valuable data and transmits the obtained data in an encrypted format to remote servers so that the attackers can gather information regarding the infected infrastructure [5]. Researchers, through reverse engineering and behavioural analysis, have found that Havex malware is vulnerable to honeypots, i.e., it is easily deceivable that a honeypot system is actually among the targets of the malware, by analysing the steps taken by the virus while searching for the targets. This study also shows that improving cybersecurity of critical infrastructures through establishing specialized defenses against known viruses by analyzing vulnerabilities of malwares is possible [5].

Another example of malwares threatening critical infrastructures is, as mentioned above, Stuxnet, which is a complex malware that can provide control of a system to attackers by infiltrating target computers. In case of attack performed on Iran's nuclear program, the malware has disrupted the operation of centrifuges by controlling the electrical current managing the centrifuges so that they change speed in such a rate that they are not designed to be capable of [6]. This provided the attackers a way to slow down Iran's nuclear program without actually needing to perform military attacks on Iran's nuclear systems, and these types of cyberattacks also provide a way for attackers to hide their identities [6].

Additionally, attacks can also leverage social engineering tactics, such as phishing and spear-phishing, to gain access to sensitive information and systems. These attacks seriously harmed the nations' reputation and social order in addition to interfering with the operation of critical infrastructures. As it can also be understood by the cyberattack examples given up to here, one of the biggest dangers to critical infrastructures is the vulnerability of industrial control systems, and cyberattacks on these systems are growing every day [7]. It is now vital to prioritize critical infrastructure cybersecurity at the national level due to the rise in cyberattacks against critical infrastructures and industrial control systems.

E. Artificial Intelligence

Artificial intelligence (AI), is a field of research and engineering that focuses on creating intelligent systems that can perform tasks typically requiring human intelligence, including tasks such as image recognition, natural language processing, speech recognition, decision-making, and language translation. Rule-based systems and machine learning systems are the two basic categories into which AI systems can be split. A branch of artificial intelligence known as machine learning (ML) focuses on creating algorithms and statistical models that let systems get better with practice. ML algorithms can be broken down into three groups: reinforcement learning, unsupervised learning, and supervised learning.

Algorithms under supervision gain knowledge from labeled training data and make assumptions about unobserved data. Unsupervised learning algorithms find significant patterns or structures in unlabeled data by learning from it. Algorithms that use reinforcement learning learn from their interactions with the environment and adjust their behavior to maximize a reward signal. A branch of machine learning named as deep learning focuses on building deep neural networks made up of many layers of artificial neurons. Applications for deep learning techniques include speech recognition, image classification, natural language processing, and game playing. Deep learning algorithms are successful in a wide range of tasks and have been used successfully in various industries such as banking, healthcare and transportation.

While AI solutions are being used at many areas, cyber security starts to become one of the focus areas of artificial intelligence field. Hence, there exists numerous research on detecting cyberattacks by using artificial intelligence techniques. It is possible to use artificial intelligence to support and strengthen cybersecurity solutions to improve cybersecurity of critical infrastructures.

III. CYBER SECURITY STANDARDS

Many countries and organizations are focusing on critical infrastructure-related cybersecurity issues. Research has led to the emergence of many different, globally accepted models and standards. Organizations develop cyber defense solutions around these criteria to ensure the cybersecurity of critical infrastructures.

Fig. 1. Use of International Cybersecurity Standards

The most preferred cybersecurity standards internationally are ISA / IEC 62443 and NIST CSF as shown in Fig. 1 [8]. Even though the developed standards are meant to provide critical infrastructure cybersecurity, each of them proposes a different cybersecurity strategy. Industrial control systems construct the foundations of critical infrastructures. Standards for information technologies are not applicable for industrial control system cybersecurity since IT have different requirements and criterion [9]. IEC 62443 model contains approaches regarding operational technologies' cybersecurity to provide critical infrastructure cybersecurity. This model defines the procedures that are to be carried out and system-level requirements for ensuring cybersecurity of industrial control systems.

The NIST CSF model essentially outlines the procedures to be followed in order to guarantee cybersecurity and provides examples. The main and sub-categories of functions, as well as informative references, form the basis of the model [10]. NIST defines five functions, namely, identify, protect, detect, respond, and recover. Identifying means to identify and detect the devices and systems to be protected, for which asset management is a crucial task to handle. Protecting describes the act of taking precautions against the cyber threats, such as management of access to the assets and collecting the required logs, which then can be analysed furtherly. Detecting is to recognise cyber threats at the moment they emerge, for which

various tools and technologies can be leveraged. Responding means to take required actions as response to an ongoing cyberattack. Recovering is the process of restoring the system from any damage caused after a cyberattack occurs. The cyber defense solution must perform each function in order to provide cybersecurity in critical infrastructures. As more categories within the functions can be implemented successfully, more cyber-resistance will be offered.

The C2M2 (Cybersecurity Capability Maturity Model) defines various domains, each indicating a defined group of applications related to a certain field [11]. C2M2 model not only focuses on information technologies (IT) security, but it also deals with operational technologies' (OT) cybersecurity. The domains defined by C2M2 are asset, threat, risk, access, situation, response, third-parties, workforce, architecture, and program, as specified by Office of Cybersecurity, Energy Security, and Emergency Response, U.S [11]. The model proposes a different set of objectives for each domain. The asset domain proposes the objectives related to asset management. Threat domain is related to vulnerability management. The risk domain copes with risk management issue, while access domain is about management of access and identity. The situation domain describes the situational awareness of cybersecurity of the system to be protected. The response domain proposes objectives to define how cyber incidents are to be responded once they occur. Third-parties domain is about how to manage risks related to third-parties, while workforce domain is about how to manage workforce. The architecture domain defines objectives regarding how cybersecurity architecture should be designed, and program domain proposes objectives for managing the cybersecurity program as a whole. The C2M2 model also defines three main maturity indicator levels (MILs), namely, MIL1, MIL2, and MIL3. These levels are said to be initiated, performed, and managed, respectively.

Numerous more cybersecurity standards specify templates and/or guidelines for guaranteeing protection against cyber threats. Another cybersecurity standard developed for establishing requirements to guarantee the cybersecurity of critical infrastructure is NERC CIP (Critical Infrastructure Protection). Examination of cybersecurity standards shows that even if they differ from each other, they all address at least the essential elements for a cyber-secure environment: identifying assets, maintaining ongoing protection, and detecting cyberattacks.

IV. IMPROVING CYBER RESILIENCE IN CRITICAL INFRASTRUCTURES

Creating a robust cyber defense infrastructure is accomplished by integrating various cybersecurity solutions together. There are several techniques that organizations can use to improve cyber resilience in critical infrastructure. The proposed approach uses a methodology comprising of five different solutions in setting up a cyber defense system infrastructure for the underlying infrastructure. Effective management of resources by utilizing suitable technologies and methods for monitoring and controlling assets, vulnerability management systems should be employed to identify assets and potential vulnerabilities, and risk management should be conducted based on the potential impact of these vulnerabilities. Solutions for intrusion detection should be implemented and methods should be established to facilitate incident investigation by maintaining event logs. Artificial intelligence and automation techniques should be applied in the development of the necessary infrastructure.

A. Asset Management

An asset in critical infrastructure refers to any physical or virtual component or system that is essential for the functioning of a critical infrastructure system. Assets are items that an organization needs in order to maintain its operations in a smooth and efficient manner. These assets that are essential for the functioning of a critical infrastructure system include physical devices, software products, information and operational technology assets, and essential information needed for operations. Companies must secure all of their valuable assets against potential threats.

With the rise of the 4th Industrial Revolution, the ability to access and control many IT and OT devices over the internet has made it even more crucial for organizations to also protect these assets in the cyber realm. In order to effectively protect assets, organizations must first identify and manage them.

Asset management is used to identify all the devices, software and systems that are connected to the organization's network and to keep track of assets in order to identify any potential cyber threats that might be brought on by asset weaknesses. Organizations cannot defend against attacks due to their undetectable and unseen existence. To automatically find assets in the network, there are numerous asset discovery techniques. Other than information technology equipment like servers, workstations, and routers, industrial control system hardware like sensors, relays, and actuators should also be automatically found while doing asset discovery in critical infrastructures. During asset detection, information can be gathered via ”active” scanning methods, which transmit network packets to devices, and ”passive” scanning methods, which extract information by observing network traffic . Passive scanning can be a good way to perform safe discovery of networks and devices in industrial control systems [12].

In order to obtain as much information regarding assets found in a critical infrastructure as possible, a study has been performed on the exploration of the hybrid scanning approach, which is the mixture of active and passive scanning techniques [13]. The usage of hybrid scanning method has been shown to make obtaining more thorough information on assets possible, according to research performed.

Asset discovery should be used to gather a variety of crucial data, such as the configuration details of the assets as well as their software and hardware versions, physical location, asset manager, and severity level. Asset data should be digitally archived and accessible via a graphical user interface for viewing and management. By using the asset management approach, it will be possible to spot unauthorized software or configuration changes on assets as well as irregularities in their operation. Vulnerabilities in the assets' current configuration or software will also be discovered, and cyberattacks against the assets will be identified. Asset management in critical infrastructure using artificial intelligence (AI) can involve using AI algorithms and models to automatically identify, classify, and track assets, as well as predict and detect potential vulnerabilities. By using AI algorithms for asset management in critical infrastructure, organizations can improve their ability to identify and

prioritize assets that need protection, as well as detect and respond to potential threats in a timely and efficient manner. The study examines existing machine learning methodologies for developing an effective asset management framework for power distribution systems, as well as for predicting the lifespan and operating stability of electrical equipment [14]. The goal of another article is to showcase the different ways in which Artificial Intelligence (AI) can aid in the management of information assets and enhance the security of enterprise systems. In addition, the research explains that using the Isolation Forest algorithm, it is possible to predict whether an asset in the dataset is rogue or an approved asset [15]. Yawar Rasool Mir tried to analyze the port scan results using artificial intelligence. In this review, they used Artificial Neural Network, Random Forest (RF) and Support vector machine (SVM) calculations to find port scan attempts based on the new CICIDS2017 dataset, with accuracy rates of 98.87%, 99.20% and 72.19%, respectively [16].

B. Vulnerability Management

A cybersecurity vulnerability is a weakness or gap in the security of IT and OT equipment and software, configurations or communication with other assets that can be exploited by attackers to gain unauthorized access, steal sensitive information, or disrupt operations. Each asset within a system can contain its own unique vulnerabilities. Malicious actors can exploit these vulnerabilities to launch attacks such as infiltration, data theft, data alteration, destruction or disruption of system operations.

In order to ensure cybersecurity resilience in critical infrastructures, it is necessary to minimize vulnerabilities in assets. With the convergence of IT and OT fields, the ability to access OT devices via the Internet has expanded the attack surface for industrial control systems attacks on critical infrastructures [17]. 70% of the vulnerabilities created by industrial control systems are network-based vulnerabilities, and organizations should primarily develop vulnerability management solutions to address these vulnerabilities [17].

Data about assets must be gathered and evaluated in order to identify vulnerabilities and fix them. Utilizing asset management, penetration testing, and vulnerability scanning technologies, vulnerability analysis should be carried out. Despite the fact that there are numerous vulnerability detection tools available focusing on information technologies, it is crucial to be careful when applying these tools on ICS (Industrial Control Systems) equipment. The operation of the system may be harmed by network-based brute force scenarios employed during vulnerability scanning because ICS devices have typically not been upgraded or modified for many years [18]. For use on ICS devices, specialized vulnerability scanning tools for the OT field must be created. It is necessary to follow the threat intelligence and analysis reports of the Cybersecurity and Infrastructure Security Agency (CISA) and use the Common Vulnerability Scoring System (CVSS) databases that are accessible online in order to assess the potential impact of vulnerabilities identified in the results of vulnerability scans. In order to determine which vulnerabilities should be fixed first to ensure the security of the system, the vulnerabilities are rated according to their potential impact. Priority risks' vulnerabilities should have action plans made for them, and those vulnerabilities should be fixed as part of these plans.

The increasing number of hardware and software vulnerabilities discovered each year makes manual classification of vulnerability types more difficult [19]. The article investigates algorithms for automatic vulnerability type classification using machine learning. It has been demonstrated in another article that the Gradient Boost Classifier is fully suitable for automatic vulnerability type classification and can be used in practice [20]. In another study, it has been presented that using machine learning algorithms can be an effective way for predicting vulnerabilities [21].

C. Risk Management

Risk management helps identify potentially harmful events, determine their probability of occurrence and predict their potential impact. In other words, it helps identify potential problems and the likelihood of their occurrence and the consequences they cause when they occur [22].

As it is crucial for all kinds of organisations, risk management is an important aspect of ensuring protection and operability of industrial control systems as well. Poor management of risks in an ICS environment may lead to unrecoverable damage as a result of a cyber-attack, a malfunction occurred in the system, a human-error, or many other possible causes. Therefore, identifying risks, determining precautions against them, and defining actions to be taken to mitigate them once they occur are crucial to increase the cyber resilience and reliable operation of critical infrastructures.

Risk management frameworks lay out methodologies and instructions on how to apply risk management in an organized way to ensure risks are treated well enough to mitigate any possible harm to an extent as most great as possible. NIST RMF (Risk Management Framework) is one of existing risk management frameworks, and it consists of 7 main steps, namely, prepare, categorize, select, implement, assess, authorize, and monitor [23].

NIST, in its Guide to Industrial Control Systems (ICS) Security publication, describes how to apply NIST RMF to industrial control systems [24]. Application of NIST RMF on ICS environments is discussed in context of 4 steps, namely, categorize, select, assess, and implement.

NIST advises that systems and network assets should be categorized with a focus on systems used in the ICS environment. The categorization process is advised to be differentiate devices and systems such as PLCs, HMIs, DCS, and SCADAs. Moreover, list of assets in the ICS environment is advised to be updated at least once a year, and each time an asset is added to or removed from the environment [24].

At the select step of risk management for ICS, as advised by NIST, security controls to be applied are to be selected by taking into account ICS environment’s categorization, and selected security controls should be listed in security plan of ICS environment [24].

NIST suggests, at assess step, performing risk assessment by identifying possible impacts -as results of any possible harm to ICS environment- to operations and assets of the organization, as well as to different organizations and to the country. As a result of risk assessment, vulnerabilities causing risks for security of ICS systems, as well as possible mitigation procedures against those risks, may be identified, and risks should be assessed more than several times [24].

At the implement step, it is advised by NIST to sort the risks with respect to size of their impact and to put effort to mitigate critical risks first. In order to be able to determine the criticalness of the risks, results of risk assessment should be examined in detail [24].

D. Detection

The ability to briefly observe the conditions of all the assets present in critical infrastructure systems is one of the most crucial elements in building cyber resilient infrastructures. Monitoring every second the system is in use and every action taken ensures that the defence set up against cyberattacks has the highest level of resistivity. This includes real-time detection of abnormal activities like unauthorized accesses, unauthorized configuration changes, and unusual network traffic that occurs outside of normal operations.

The development of the cyber security field has resulted in the creation of numerous diverse defence systems. As a result, malicious attackers create and employ brand-new attack strategies every day. In the first quarter of 2021, 74% of cyberattacks were zero-day attacks [25]. New cyberattacks that render cyber security measures useless appear every day. Considering the expanding attack surfaces and growing attack channels, enterprises are increasingly at risk from cyberattacks as time goes on.

One cyber defence strategy is insufficient to fend against the evolving and increasingly sophisticated cyberattacks that occur daily. It is necessary to develop a cyber defence infrastructure with a variety of strategies and solutions in order to perform a cyber defence at a high degree of resistivity and maturity. Using various techniques enables the detection of various cyberattack kinds. Establishing cyberattack detection systems for systems in the field of operational technology is equally crucial to constructing cyber defence infrastructures as it is for systems in the field of information technology. To identify cyberattacks conducted on OT devices, various techniques have been developed [26]. Industrial control systems can be kept cyber-secure using solutions for signature and anomaly-based detection that should be positioned inside the network topology, just like in the field of information technologies [26]. By comparing the network traffic with the models built using signatures belonging to known cyberattacks, signature-based solutions can determine whether or not similar attacks have been carried out [27]. While signature-based solutions are effective at identifying known attack types, they are unable to identify zero-day attacks that they come across for the first time. By utilizing anomaly detection tools, which can spot unusual system behavior brought on by zero-day attacks, the range of detectable attack routes should be expanded. Artificial intelligence techniques should be used to develop anomaly detection systems that model the system's usual state and determine whether or not the system deviates from it more than a predetermined rate by tracking network traffic [27]. A complete cyber infrastructure for the detection of cyber-attacks should be developed by using hybrid approaches that combine signature-based and anomaly-based detection technologies.

A variety of assets found across an organization may be the target of cyberattacks. Devices identified in various parts of the organization may therefore serve as the initial point of each attack. Taking control of workstations and endpoints that are running an operating system, causing harm to the system's functionality, or leaking information by altering network traffic, are the basic beginning points for cyberattacks. In order to defend critical infrastructure systems against cyberattacks, developing solutions for endpoint security is just as crucial as developing those that analyze network traffic.

Cyberattacks are less likely to inflict system harm if they are discovered as soon as they occur. To safeguard crucial infrastructures from cyberthreats, endpoint and network traffic security solutions should be created for the fastest possible detection of cyberattacks. Once a cyber-attack starts and becomes successful to penetrate the system, every moment with the intruder inside the system causes a great risk for accessibility, integrity, and confidentiality of cyber systems of an organization. For critical infrastructures, this risk becomes even greater. Therefore, decreasing the probability of a cyber-attack attempt being successful as much as possible in a time interval as narrow as possible is of great importance.

One way to achieve this is to perform access management to make sure that no user has more privilege than they need. This may make it harder for attackers to gain as much access as they need to perform a successful cyberattack, e.g., taking possession of a user with limited access may not be useful for an attacker until a privilege escalation attempt becomes successful, which is a situation that make attackers lose time while making cyber operations centres have more time to interfere with and prevent the cyber-attack attempt. Access management is the management of access privileges assigned to users such that each user has restricted amount of access privileges, just enough to perform the tasks assigned to them. Privileged Access Management (PAM) software technologies should be used to manage the privileges of users, as well as to prevent data breaches [28]. PAM software also makes it possible to monitor activities performed by the users. This is an important information to have for tracking the activities being performed. In case of a cyberattack, if a user account is compromised by an attacker, analyzing the activities performed by the attacker becomes much easier by monitoring the activities done by the compromised user thanks to sophisticated activity monitoring properties of PAM software. Therefore, activity monitoring information gathered from PAM software can be of great importance for SoC teams for interfering with an occurring cyberattack or analyzing a cyberattack after it has happened.

Managing accesses of users is not enough on its own to ensure cyber security of critical infrastructures. Restriction of the incoming and outgoing network traffic is crucial to establish a resistant cyber-secure environment. With the fact that industrial control systems become more and more reachable from outside nowadays for the sake of monitoring them easily, protecting the devices located in critical infrastructure areas from prohibited access incoming through the public network has become an important problem to tackle. It is known that cybersecurity of a contemporary substation can be improved by using a firewall [29]. Firewalls provide protection to a good extent in terms of keeping unwanted traffic outside the internal network of organizations, which is an important factor in preventing attackers from easily communicating with the devices and networks found in the targeted systems. Therefore, using firewall technologies is an important component of ensuring cyber security of critical infrastructures.

Not all of the devices found in a critical infrastructure environment need the same network restrictions and protections. To be able to better manage the communications within the critical infrastructures and to create a more robust

environment in terms of cyber security, network segmentation should be used. Network segmentation is the process of dividing a big computer network into several segments, typically to increase security. This technique, when used appropriately, is one of the most efficient ways to lessen the attack surface of cyber attackers in the event of an infiltration [30]. Network segmentation makes it possible to manage and rule each sub-network separately, e.g., critical devices and servers may be in a tightly restricted sub-network while devices and servers communicating with the public network are located in a sub-network where communication with the public network is possible. Granular network segmentation is a type of network segmentation where devices are located in well-separated networks, and it should be preferred in critical infrastructures to directly prevent almost half of the incoming cyberattacks [30]. Despite all the precautions taken in terms of network and system configurations and cyber security technologies, sophisticated cyber-attacks may still bypass these systems, which means that taking precautions does not guarantee that penetration of the attackers into the system will be avoided. Even though the attackers are avoided before they can penetrate, having information regarding what kind of cyber-attack vectors have been tried on the system is important to know for identifying which parts of the system should be strengthened against cyber threats. Therefore, being able to detect intrusions along with the attempts performed by the attackers is a required skill to have cyber-secured critical infrastructure systems. Intrusion detection systems (IDS) are systems that track and log abnormal network activities along with events occurred in the network by monitoring network traffic. Therefore, they should be used as important components of cyber security systems of critical infrastructures since they provide crucial intelligence to cyber operations centers. Intrusion detection can be performed by using software performing signature-based detection such as Snort [31] and Suricata [32], while machine learning techniques such as Naïve Bayes, Multilayer Perceptron, AdaBoost, etc. can also be applied to perform network intrusion detection, where the detecting intrusion is considered to be a supervised learning problem with nominal and numerical attributes, with the aim of performing multi-class classification [33].

E. Security Monitoring

Events that compromise a system's integrity, accessibility, and efficiency are known as “cyber security events.” These events are those that deviate from a system's normal behavior. A cyber security incident that arises from the routine or expected behavior of a system does not always indicate that a cyberattack has taken place. Each day, an organization creates hundreds of event records. These event logs must be monitored, and it must be decided whether or not they suggest a risk to cyber security. Additionally, necessary safeguards and procedures must be taken to protect against any situations that could provide a threat to cyber security. They should compile and analyze on a centralized management system all asset data and records pertaining to the communications they carried out. Cyber cases may arise from cyber security threat incidents. A cyber case is a cyber incident or series of events that affects or has the potential to affect the assets or services of a critical infrastructure system [34]. In contrary to cyber occurrences, cyber incidents can have negative repercussions on enterprises. As a result, cyber cases must be found as soon as possible, and the required action plan must be developed and put into practice. Systems that contain many cyber security solutions are known as cyber defense substructures, and they are prevalent in critical infrastructures. The cyber defense substructure becomes more complex with each new cyber security solution deployed, making system monitoring more difficult. Given the complexity and multi-stage structure of modern cyberattacks, it becomes clear that in the majority of cases, it is possible to detect these attacks by examining the outputs of many defense solutions. Cyber operation centers should be developed where the defense solutions are regulated and monitored in order to guarantee the cyber security of critical infrastructures. Analysts, operators, and administrators keep an eye on a system's infrastructure, applications, services, and defense mechanisms in cyber operation centers in order to spot and stop cyberattacks, close security gaps, and handle other cyber incidents [35]. Switches, firewalls, servers, IT devices, SCADA systems, PLCs, OT devices, and other critical infrastructure components all generate logs. These logs are frequently kept in the local storage of these devices. This makes it difficult to monitor and track the system from a single location. Collection of logs, which is the first and most crucial stage of monitoring, should be carried out to avoid this issue. Log collection is performed to gather the information stored on local storages together in a collective storage so that the analysis of logs coming from different sources can be carried out in a central manner [35]. It is important that SoC monitors the analyses of collected logs on a regular basis so that any possible cyber threats can be detected while cyber events also get processed before it is too late. Since SoC is the main department responsible for monitoring logs, the log files stored in devices should be transferred to central log storages located in SoC. Choosing methods to follow for collecting logs is an important decision when it comes to performing log collection effectively. There are two main methods to collect logs, namely, agent-based and agentless. It is not possible to assert that one is superior to the other for all possible systems since these methods have different advantages and disadvantages for different systems [36]. Agent-based log collection is performed by installing agent software to servers that are aimed to be monitored, whereas agentless log collection is realized through requests sent from the log collection center to APIs provided by monitored devices. While agent-based log collection method provides much more information than agentless log collection can provide, the latter is much easy to deploy and use than the other since installing agents on each server to be monitored is not always an easy task. Moreover, some devices’ logs cannot be collected using the agent-based log collection method, such as network devices. In those cases, using agentless log collection is a better option, whereas in other cases, agent-based collection solutions are preferable due to large amount of information they can provide. In critical infrastructures, using a log collection environment consisting of both agentless and agent-based log collection techniques seems reasonable since they contain many different types of devices for which the need to collect logs may emerge. So, for components for which it is possible to install agent software easily, using agent-based log collectors is the way to choose, whereas for components for which it is either hard or impossible to use agent-based log collection solutions, using agentless log collectors is the correct option.

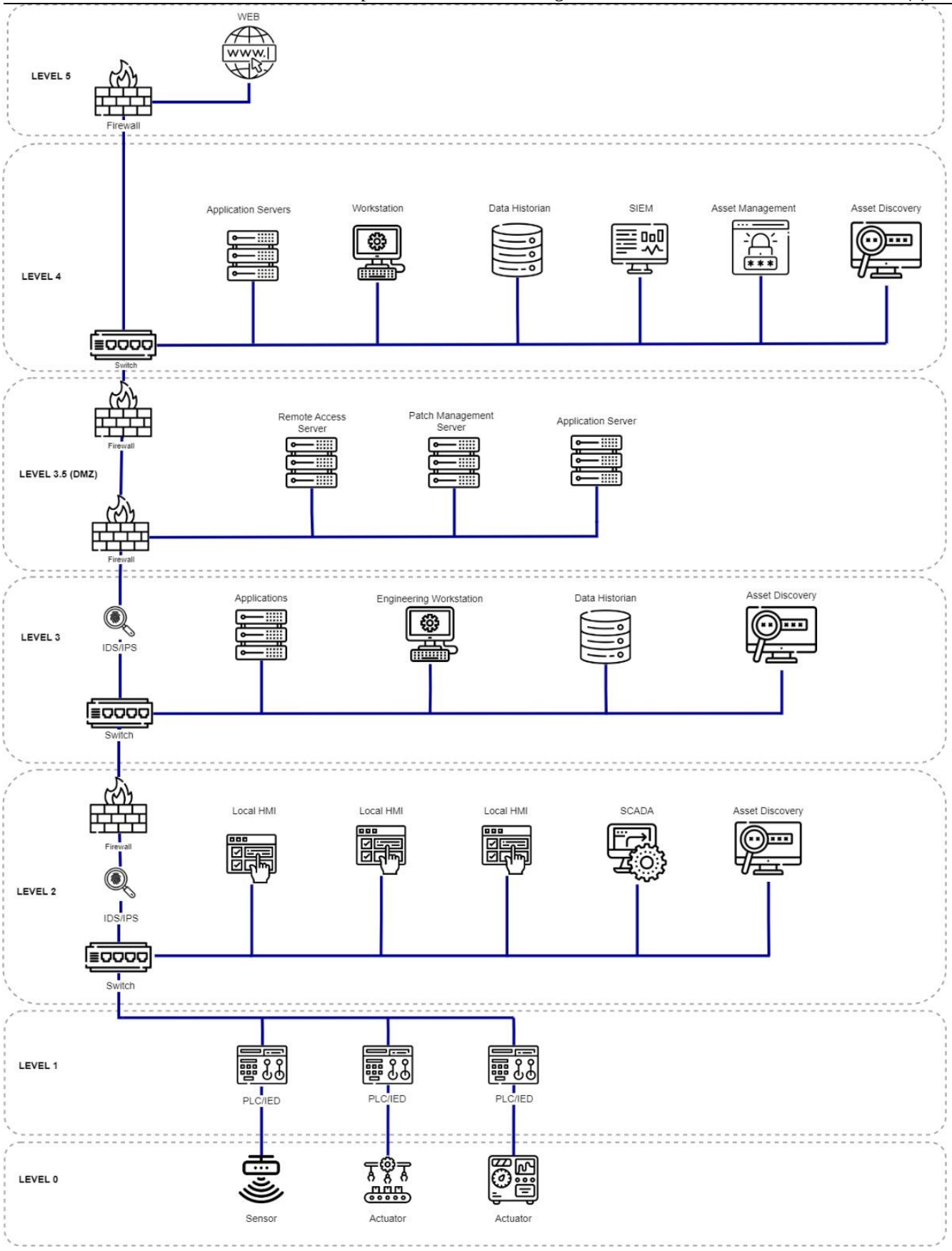


Fig. 2 Architecture of Critical Infrastructure with Cybersecurity Solutions

Collecting logs to a central storage is not enough to detect and mitigate cyber threats on its own. Analysis of the cyber event logs is of crucial importance to detection, mitigation, and prevention of cyber threats since the analysis results obtained from event logs provide the necessary information to be able to deal with cyber threats as much as possible. Manual inspection of these logs is error prone. Moreover, analysis of immense amount of logs, which is the case nowadays, by humans is much far from being possible [35]. In order to make automated analysis of cyber event logs possible, Security Information and Event Monitoring (SIEM) solutions should be used by SoC teams. SIEM solutions aim to identify anomalous events and activities by inspecting and analyzing event logs [37]. For analyzing the logs, there are three main approaches. These are called automated, semi-automated, and hybrid analyses. In automated analysis, only automated tools are used, which implies that humans do not intervene with the analysis of the tool. In semi-automated analysis, both automated and manual analyses take place. On the other hand, hybrid analysis consists of automated analysis where in decision making, humans also take place. Hybrid analysis should be preferred since it provides the best means to perform analysis in the sense that the monitoring can be performed in such a way that it is both uninterrupted and trustable enough in terms of protection that it provides. SIEM solutions can be used together with machine learning algorithms, where the dataset for training the machine learning algorithms are collected from SIEM systems, and the trained machine learning algorithms can be used to produce intrusion predictions, which is useful to predict an attack before it actually occurs [38]. Also, the operators in critical infrastructures can be notified by using machine learning algorithms on whether there is an occurring anomaly and what type of anomaly is predicted to be occurring [39].

V. ARCHITECTURE OF CYBER RESILIENT CRITICAL INFRASTRUCTURES

Cyber resilience is achieved by integrating several cyber security solutions. Security solutions are organized into several infrastructure segments based on their functions. Cyber resilience in critical infrastructure can be improved by managing all solutions in a single security operation center. Purdue model is a model that describes how the devices in critical infrastructures should be separated into different network segments. In Purdue model, there are 6 levels in total, from level 0 to level 5, and one additional level is actually there to strengthen separation between level 3 and level 4, which is called level 3.5 [40]. IT devices are located at upper levels, whereas OT devices are located at lower levels. The level 0 is the physical process level, where the fundamental physical components of the infrastructure are found, such as actuators. At level 1, intelligent devices that can sense and manipulate physical processes are found, whereas control systems such as SCADA are found at level 2. Level 3 consists of manufacturing operations systems, and level 3.5 is the “demilitarized zone” that is crucial to ensure that communication between IT and OT sides are well separated. Corporate IT is found at level 4, while cloud access is at level 5 [40]. Applying Purdue model is required to strengthen the cybersecurity of critical infrastructures since it is a special type of network segmentation model designed especially for critical infrastructures. First and primarily, it must be determined which assets the critical infrastructure have. To achieve this, asset discovery and management solutions, which will be located separately in the IT and OT segments, can be used to discover assets and monitor their status. This solution can detect changes made to asset configuration by unauthorized users. It will also make it easier to detect system failures. Other procedures such as vulnerability management and risk management will be easier to complete if assets are visible.

Asset management, vulnerability management, and risk management are all passive approaches to increasing cyber resilience. In order to present an effective defense against cyber attacks, active solutions should be used as well as passive methods. For this, IT and OT should be segmented in network topology. A firewall should be used to control the transitions between IT and OT segments. Furthermore, by placing a firewall between Level 2 and Level 3 in the OT segment, it will provide additional protection for the security of the devices in the field, even if attackers infiltrate the OT segment. Also, network traffic analysis can be done with IDS/IPS systems to be placed in front of or behind firewalls. In this way, abnormal network traffic that is not blocked by the firewall and caused by the activity of the attacker can be detected. In addition to traditional signature-based detections on this network traffic, artificial intelligence-based behavior analysis detection systems can be used to provide more advanced protection. With the access management solutions to be used, the authorizations in the IT and OT segments can be controlled from a single point, and access to physical devices in the OT area can be controlled. All cyber security solutions generate event records. These event logs should be collected and stored on a centralized server. As a result, the outcomes of various solutions can be correlated, and analyses can be performed. SIEM solutions should be used for achieving this capability. Administrators can be notified and incident response procedure can be applied by monitoring all event records in SIEM in the case of cyber incidents. The criteria in international cyber security standards for critical infrastructures can be met by the system we suggested on the Purdue model. Different cyber security solutions offer advantages in meeting various criteria. A comprehensive cyber security platform can be established and cyber resilience can be increased by placing all solutions in accordance with the suggested approach shown in Fig. 2.

VI. CONCLUSION

Critical infrastructures are essential systems that support the continuity of the social and economic system as well as the health and safety of society. Critical infrastructure destruction from either the inside or outside will have a negative impact on a nation's social structure, harm its standing abroad, and undermine its legitimacy. Systems with multiple physical and virtual components from the information and operational technology domains compose critical infrastructures. In the past, closed networks were used to administrate industrial control systems, which include the majority of hardware, devices, and automation tools in the field of operational technology. The disciplines of information and operational technology have converged as a result of the digital transformations performed as of the 21st century, and industrial control systems are now available over the internet. This convergence has revealed industrial control systems' weaknesses, increased the attack surface for cyberattacks on critical infrastructures, and made operational technology systems' vulnerabilities the main target of cyberattacks. Nations should protect their critical infrastructures against cyber threats to guarantee security of critical infrastructures.

Since critical infrastructures are vital to countries and societies, critical infrastructure cyber security should be regarded as a national security issue. Nations should invest adequately in the necessary technologies while developing cyber security policies for their critical infrastructure. To support the security of operational technology devices, the breadth of information technology cyber security solutions must be expanded. Important data in the IT and OT areas, as well as hardware, software, and other resources, must be under the supervision of cybersecurity system that will be placed in critical infrastructures. To identify the assets' vulnerabilities, the data obtained during asset management should be compared to the most recent vulnerability lists. Prioritizing the actions required to address the vulnerabilities is crucial due to dangers that they present. To identify cyberattacks in real time, solutions based on signature and anomaly-based attack detection should be developed in addition to the system's current vulnerabilities. To avoid management issues that could develop as a result of each new solution making the cyber defense platform more complex, the complete cyber defense platform should be controllable from a single center. Thus, cyber risks can be better studied, cyber attack detection times can be reduced, and cyber cases can be handled faster by combining visualization, control, analysis, and management from a single operation center.

REFERENCES

[1] "Operational Technology (OT)." Gartner, Gartner, www.gartner.com/en/information-technology/glossary/operational-technology-ot. Accessed 15 Jan. 2023.

[2] Clinton, William Jefferson. "Executive order 13010-critical infrastructure protection." Federal register 61.138 (1996): 37347-37350.

[3] Shah, Rajiv. Protecting critical national infrastructure in an era of IT and OT convergence. Australian Strategic Policy Institute, 2019.

[4] Hemsley, Kevin E., and E. Fisher. History of industrial control system cyber incidents. No. INL/CON-18-44411-Rev002. Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[5] Rrushi, Julian, et al. "A quantitative evaluation of the target selection of havex ics malware plugin." Industrial control system security (ICSS) workshop. 2015.

[6] Farwell, James P., and Rafal Rohozinski. "Stuxnet and the future of cyber war." Survival 53.1 (2011): 23-40.

[7] "Threat Landscape for Industrial Automation Systems in H1 2021." Securelist, Kaspersky Lab, securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2021/104017/. Accessed 17 Jan. 2023.

[8] Bristow, Mark. "A SANS 2021 Survey: OT/ICS Cybersecurity." eng. In (2021).

[9] "Understanding IEC 62443." IEC, International Electrotechnical Commission, www.iec.ch/blog/understanding-iec-62443.

[10] Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP 4162018 (2018).

[11] "Cybersecurity Capability Maturity Model (C2M2)." Energy.gov, U.S. Department of Energy, 2023, www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2. Accessed 18 Jan. 2023.

[12] Wedgbury, Adam, and Kevin Jones. "Automated asset discovery in industrial control systems-exploring the problem." 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3. 2015.

[13] Mytilinaios, Artemis, Michel van Veen, and Pavlos Lontorfos. "Real time asset inventory in ICS." (2021).

[14] Lal Rajora, Gopal, Miguel A. Sanz-Bobi, and Carlos Mateo Domingo. "Application of Machine Learning Methods for Asset Management on Power Distribution Networks." Emerging Science Journal 6.4 (2022): 905-920.

[15] Adebayo, Abimbola, Mhd Saeed Sharif, and Wael Elmedany. "The Role of Artificial Intelligence in Asset Management of Enterprise Systems." 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). IEEE, 2022.

[16] Mir, Yawar Rasool, and Navneet Kaur Sandhu. "Port Scan Detection using AI." (2019).

[17] Guevara, Isaac, and Chen Fradkin. "Growing ICS vulnerabilities mandate prioritization: Use vulnerability management at the convergence of information and operational technologies to lower risk to industrial control systems." Control Engineering 68.2 (2021): 31-34.

[18] "The Ultimate Guide to OT Vulnerability Management." Verve Industrial, verveindustrial.com/resources/guide/the-ultimate-guide-to-ot-vulnerability-management/. Accessed 20 Jan. 2023.

[19] Yosifova, Veneta, Antoniya Tasheva, and Roumen Trifonov. "Predicting vulnerability type in common vulnerabilities and exposures (CVE) database with machine learning classifiers." 2021 12th National Conference with International Participation (ELECTRONICA). IEEE, 2021.

[20] Yosifova, Veneta. "Vulnerability Type Prediction in Common Vulnerabilities and Exposures Database with Ensemble Machine Learning." 2021 International Conference Automatics and Informatics (ICAI). IEEE, 2021.

[21] Khan, Saad, and Simon Parkinson. "Review into state of the art of vulnerability assessment using artificial intelligence." Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach (2018): 3-32.

[22] Kaplan, Stanley, and B. John Garrick. "On the quantitative definition of risk." Risk analysis 1.1 (1981): 11-27.

[23] "About Risk Management Framework (RMF)." NIST Computer Security Resource Center, National Institute of Standards and Technology, csrc.nist.gov/projects/risk-management/about-rmf. Accessed 12 Mar. 2023.

[24] National Institute of Standards and Technology. "Guide to Industrial Control Systems (ICS) Security." NIST Special Publication 800-82 Revision 2, U.S. Department of Commerce, 1 May 2015, doi: 10.6028/nist.sp.800-82r2.

[25] "Zero-Day Malware: Q1 2021." Help Net Security, 29 June 2021, www.helpnetsecurity.com/2021/06/29/zero-day-malware-q1-2021. Accessed 20 Jan. 2023.

[26] Murray, Glenn, et al. "Detection techniques in operational technology infrastructure."(2018).

[27] Fernandes, Gilberto, et al. "A comprehensive survey on network anomaly detection." Telecommunication Systems 70 (2019): 447-489.

[28] Purba, Anton, and Mohammad Soetomo. "Assessing Privileged Access Management (PAM) using ISO 27001: 2013 Control." ACMIT Proceedings 5.1 (2018): 65-76.

[29] Anderson, Dwight, and Nathan Kipp. "Implementing firewalls for modern substation cybersecurity." proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA. 2010.

[30] Korman, Matus, et al. "Analyzing the effectiveness of attack countermeasures in a scada system." Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids. 2017.

[31] "Snort." Snort.org, snort.org. Accessed 21 Jan. 2023.

[32] "Suricata." Suricata, suricata.io. Accessed 21 Jan. 2023.

[33] Hamid, Yasir, M. Sugumaran, and Ludovic Journaux. "Machine learning techniques for intrusion detection: a comparative analysis." Proceedings of the International Conference on Informatics and Analytics. 2016.

[34] Klaver, Marieke, and Eric Luiijf. "Analyzing the cyber risk in critical infrastructures." Issues on Risk Analysis for Critical Infrastructure Protection. IntechOpen, 2021.

[35] Onwubiko, Cyril. "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy." 2015 international conference on cyber situational awareness, data analytics and assessment (cybersa). IEEE, 2015.

[36] Pandey, Himanshu, and Er Kushagra Mittal. "Analogy between Agent Less Monitoring and Agent Based Monitoring." Reliability: Theory & Applications 15.3 (2020): 117-124.

[37] Wenge, Olga, et al. "Security information and event monitoring as a service: a survey on current concerns and solutions." PIK-Praxis der Informationsverarbeitung und Kommunikation 37.2 (2014): 163-170.

[38] Anumol, E. T. "Use of machine learning algorithms with SIEM for attack prediction." Intelligent Computing, Communication and Devices: Proceedings of ICCD 2014, Volume 1. Springer India, 2015.

[39] Hindy, Hanan, et al. "Improving SIEM for critical SCADA water infrastructures using machine learning." Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers 2. Springer International Publishing, 2019.

[40] Garton, D. "Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation." U.S. Department of Energy, 14 Oct. 2022, www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf. Accessed 21 Jan. 2023.