Торайғыров университетінің хабаршысы
ҒЫЛЫМИ ЖУРНАЛЫ

НАУЧНЫЙ ЖУРНАЛ
Вестник Торайгыров университета

Торайғыров университетінің ХАБАРШЫСЫ

Энергетикалық сериясы

1997 жылдан бастап шығады

ВЕСТНИК Торайгыров университета

Энергетическая серия

Издается с 1997 года

ISSN 2710-3420

№ 3 (2023)

ПАВЛОДАР

НАУЧНЫЙ ЖУРНАЛ
Вестник Торайгыров университета

Энергетическая серия
выходит 4 раза в год

СВИДЕТЕЛЬСТВО
о постановке на переучет периодического печатного издания,
информационного агентства и сетевого издания
№ 14310-Ж
выдано
Министерство информации и общественного развития
Республики Казахстан

Тематическая направленность
публикация материалов в области электроэнергетики,
электротехнологии, автоматизации, автоматизированных и
информационных систем, электромеханики и теплоэнергетики

Подписной индекс – 76136

https://doi.org/10.48081/YBCY7199

За достоверность материалов и рекламы ответственность несут авторы и рекламодатели
Редакция оставляет за собой право на отклонение материалов
При использовании материалов журнала ссылка на «Вестник Торайгыров университета» обязательна

SRSTI 44.29.31

https://doi.org/10.48081/YVNV9748

A. V. Neftissov[1], I. M. Kazambayev[2], L. N. Kirichenko[3], K. M. Zhakupova[4], D. B. Urazayev[5]

[1,2,3,4,5]Astana IT University, Kazakhstan, Astana
e-mail: alexandr.neftissov@astanait.edu.kz

AN INTERACTION MODEL OF RELAY PROTECTION MEASURING TRANSDUCERS WITH COMPUTING SYSTEMS VIA IIOT TECHNOLOGY

The object of this research is the interaction model between measuring transducers and computing systems, particularly focusing on its application within the framework of Industrial Internet of Things (IIoT) and Cloud technologies. The imperative driving this study is the increasing demand for precise and efficient data acquisition, protection and processing in various industrial sectors. The research aims to address this need by elucidating an interaction model that optimizes measuring computing systems through IIoT and Cloud technologies. As a result of our research, a comprehensive interaction model that encompasses the entire data flow process was established. This model integrates data acquisition, analytics, real-time communication protocols, and secure data transmission methodologies. It offers a structured framework for acquiring, transmitting, and analyzing data with high accuracy and efficiency. The significance of our results lies in their capacity to resolve critical challenges in data acquisition and processing of the electrical power data, as well as monitoring and protection against electrical faults. These results hold practical value under diverse industrial conditions, including manufacturing, energy production and energy distribution.

Keywords: relay protection, open architecture, encryption, data processing, data visualization, internet of things

Introduction

Currently, the market is saturated with relay protection systems made by numerous manufacturers, and enterprise companies are the majority of the demand for such devices since the safety and continuity of the operations at these enterprises are bound by standards.

Systems that already exist on the market create complications during the installation and maintenance due to proprietary connections and a lack of wireless communication capabilities as a primary source of data exchange between the elements. In other words, each unit is localized to a certain segment of the power grid and is taking action in an ad-hoc manner without sharing information with neighboring units. The proprietary nature of connectors and technology used to manufacture such relay protection leads to hardships during part replacement and scaling of the protected electrical grid. In this research, an open architecture model for industrial relay protection with the usage of the modern Industrial IoT (IIoT) technology will be developed and evaluated in terms of an increase in the speed of operation, robustness, and improvement of selectiveness.

The aim of this study is to propose a model for a relay protection system which uses the IIoT and Cloud technologies and to evaluate it. Specifically, cloud computing enables real-time data analysis and sharing among all components of the protection system, fostering a collaborative and adaptive approach to grid protection. Additionally, cloud-based solutions facilitate remote monitoring, maintenance, and scalability, ensuring that relay protection systems can evolve and expand in tandem with the dynamic requirements of modern industrial environments.

Literature review

Power supply reliability is a major concern in a state where reliance on electricity and data has become a crucial part of economics, science, and general well-being. According to Chernobrovov, traditional relay protection systems and smart protection systems, by extension, can be functionally compared in terms of selectiveness, speed of operation, sensitivity, and robustness [1]. These qualities ensure that the relay protection is able to successfully prevent accidents and malfunctions, especially in manufacturing and supplying establishments, as well as achieve stability of power supply systems. Attempts were made by engineers to incorporate IT technologies into power systems to increase reliability and feedback, which resulted in the emergence of a smart grid concept. Since reliability is a major concern of the smart grid, relay protection systems are adapting as well to new technologies. In recent years, the Internet of Things (IoT), defined by Ashton in 1998 [2], has started to be used in industrial and power delivery applications, which inevitably was used in the creation of models for modern-day relay protection systems.

Recent developments in relay protection engineering are concluded in the work of Zhang et al. [3], such as the usage of transient AC and DC characteristics and the ultra-high speed protection principle to aid the progression of the smart grid. A distributed relay protection system for a smart grid was proposed by Kauhaniemi and Voima in 2012 [4]. By using an assortment of intelligent electronic devices

(IED), authors described a zone-divided approach to the power grid protection, where each zone is being measured and reported by a separate IED, which is in turn connected to the main intelligence system via a router or a switch.

In the context of relay protection systems, the selection of an appropriate cloud server type plays a pivotal role in optimizing performance and cost-effectiveness. A cost analysis demonstrates the substantial cost advantage of PC-based clusters over their multiprocessor counterparts. While the multiprocessor server may be approximately three times more expensive, it offers significantly fewer CPUs, about 22 times less RAM, and slightly more disk space [5]. This cost disparity underscores the potential cost savings that can be achieved by embracing cloud computing infrastructure that relies on PC-based clusters. The benchmarks used in the study of C. Kotas et al. are the HPC Challenge (HPCC) and the High-Performance Conjugate Gradient (HPCG) [6]. These benchmarks test various aspects of computer system performance, including computational speed, memory bandwidth, and network bandwidth. These benchmarks evaluate the performance of AWS and Microsoft Azure cloud platforms for high-performance computing applications that utilize the message-passing interface (MPI) library for communication.

In the realm of relay protection systems with IIoT integration, fault resilience is of paramount importance. Parallel processing, enabled by cloud computing, enhances fault resilience through data replication in the cloud.

Materials and Methods

For smart grid management, ESP-32's relevance is heightened on its advantages in open-source development and cost-efficiency, consolidating the CPU and WiFi/Bluetooth module for production efficiency. Within the domain of relay protection systems ESP-NOW, a connectionless IoT protocol, excels in short packet transmissions and power conservation. After the initiation of power, radio transmission of the packet reaches 20 ms at maximum, including retransmissions of the lost packets. It also supports AES-128 encryption by default, which is known for its computational efficiency and resilience against most conventional attacks [7]. In the smart grid context, efficient management and real-time extraction of insights from this dynamic time-series data are essential [8]. Big Data, as defined by De Mauro et al. signifies information with substantial volume, high velocity, and diverse variety, necessitating specialized technologies for insights extraction [9]. Thus, for smart grid management, the Bokeh Python library shines, offering interactive scalability, web-based support, and real-time data monitoring, surpassing Matplotlib for relay protection systems, enhancing dynamic analysis and decision-making [10].

Results and Discussion

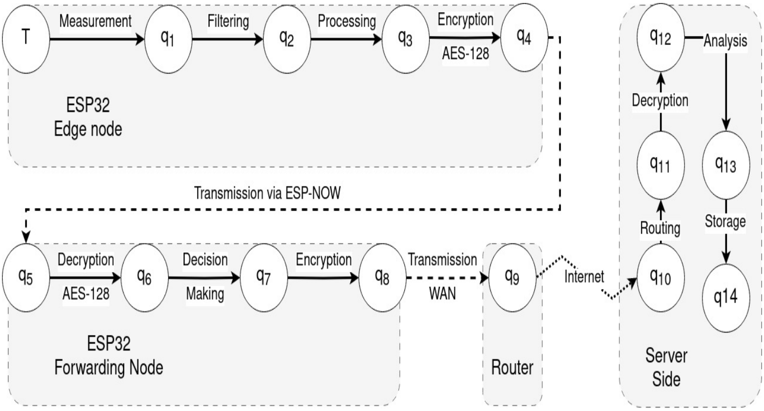

Fig 1. The proposed relay protection system model.

Time complexity of the AES-128 on the link between (q4) and (q5) can be considered as O(n) if the size of the block exceeds 128 bits [11].

$$2O(n)+en\_tr\_time \tag{1}$$

The size of a common ESP-NOW with an empty payload is 36 bytes, which already satisfies the O(n) requirements of the AES-128 encryption algorithm. This makes the time complexity of the data transfer between the edge and forwarding nodes equal to the value presented on the Equation 1.

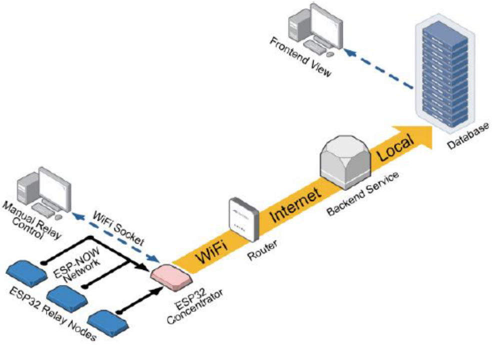

Fig 2. Overview of the proposed model.

As it was mentioned earlier, transmission time for the ESP-NOW packet can be as low as 1 ms, with a maximum of 20 ms if packets were to be retransmitted. Thus, latency from data acquisition until it will be accepted by the forwarding node is close to negligible.

For the WAN transmission from the forwarding node to the server, AES-256 encryption algorithm has been chosen. A study conducted by Singh in 2013 shows that the AES group of the symmetric encryption algorithms is faster and more secure in comparison with the asymmetric RSA algorithm, along with the DES and 3DES [12].

Since the AES-256 works with the same encryption method as the AES-128, we can also consider the complexity to be O(n), albeit since the length of the block is 256 bits, it takes longer time to encrypt and decrypt. It is plausible to ignore the decryption costs from the server side because computation power is marginally higher than that of a microcontroller. With these considerations, the complexity of the data transmission to the server from the forwarding node is:

$$O(n) + wan\_tr\_time + intertnet\_tr\_time \tag{2}$$

Where O(n) is the time required to encrypt the packet, ‘wan_tr_time’ is the time required to reach the router via WAN, and ‘internet_tr_time’ is the time needed for the packet to be perceived by the server.

Considering all the operations throughout the whole process of encryption mathematically it can be described as:

$$\begin{cases} b_i' = (b_i \oplus b_{(i+4)\bmod 8} \oplus b_{(i+5)\bmod 8} \oplus b_{(i+6)\bmod 8} \oplus b_{(i+7)\bmod 8} \oplus c_i \mid b_i \in B); \\ c_i = 01100011_2; \\ m_i' = b_0' x^0 + b_1' x^1 + b_2' x^2 + b_3' x^3 + b_4' x^4 + b_5' x^5 + b_6' x^6 + b_7' x^7, \end{cases} \tag{3}$$

where b_i – is encrypted byte, b_i – is byte and c_i – constant and mi is mathematical description of the encrypted symbol.

$$\begin{Vmatrix} b_0' \\ b_1' \\ \cdots \\ b_7' \end{Vmatrix} = A \cdot \begin{Vmatrix} b_0 \\ b_1 \\ \cdots \\ b_7 \end{Vmatrix} + c_i \qquad (4)$$

where A – is the matrix of bits for every byte.

Fig 3. Demonstrates the behavior of the model and shows the relationship between time and three different signals: ADC and Encryption, Output relay, and Blocking signal. The x-axis is time in milliseconds and the y-axis is the signal value.

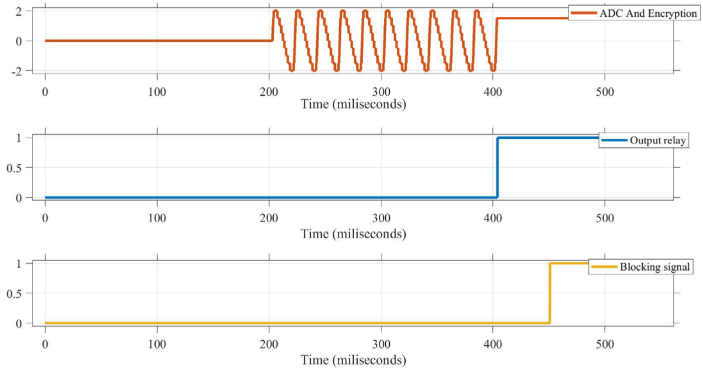

Fig 3 – Simulated signals.

The first graph is an orange line representing ADC and Encryption activity. Output and Blocking are responsible for the state of the relay at the end of the data filtration, processing and decision making operation of the model. The Matlab model of a control system is shown on Fig.4.

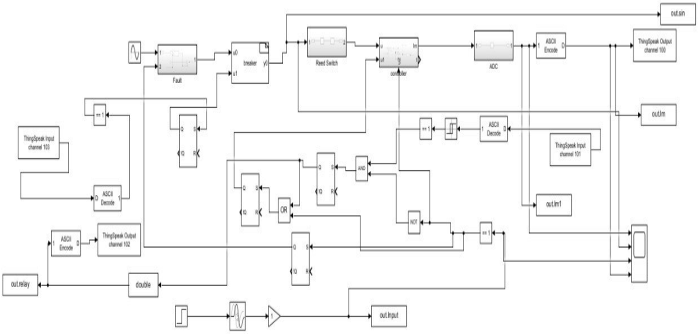

Fig 4 – Model design in MatLab.

The model is used to simulate and analyze the behavior of the proposed relay protection system. Three main inputs are designated: «Plant», «Reference», and «Disturbance». The model has two outputs: «Output» and «Control», which describe the state of the certain node, which enforce the state upon a remote relay node the data is originating from. The output data then can be stored and analyzed on one of the cloud services. Resultant formula of the interaction can be described on Eq. 3 as:

$$data\_acq + 3O(n) + wan\_tr\_time + internet\_tr\_time \qquad (5)$$

where «data_acq» is time required for current measurements, filtration and processing and other components are derived from the Eq. 1 and Eq. 2 in a summative manner. This applies for each tick of any of the relay nodes.

On the other hand, the mathematical description of the wave modulation

$$u_{am}(t) = U_c\left[1 + m\frac{u_m(t)}{|u_m(t)|_{\max}}\right]\cos(\omega_c t), \qquad (6)$$

where m – modulation constant, Uc – carrier wave voltage amplitude, ωc – carrier wave cyclic frequency.

Options of cloud providers in Kazakhstan

The top three notable cloud providers operating in Kazakhstan are as follows: their strengths, offerings, and unique attributes.

PS Internet Company, a key player in Kazakhstan's cloud ecosystem, offers an intriguing array of cloud services. These encompass virtual private servers (VPS), dedicated servers, and domain registration. Notably, the company operates a data center situated in Almaty, Kazakhstan. The company's local data center presence in Almaty enhances data transfer efficiency and reduces latency, considerations of utmost importance in cloud computing. Jusan Mobile is a prominent figure in the Kazakhstani telecommunications and IT services sector. It provides access to a spectrum of services, including virtual servers and data storage solutions. Kazakhtelecom, Kazakhstan's national telecommunications operator, extends its services to include cloud and data center solutions. Their clientele predominantly comprises businesses and government organizations within the country. Kazakhtelecom's cloud venture's scientific underpinning is rooted in national relevance and security.

It is noteworthy to emphasize that none of the three major global cloud providers, namely AWS, Azure, and Google Cloud, have established dedicated servers within the territory of Kazakhstan. However, when considering the imperative requirements of relay protection systems within the smart grid context, which necessitate comprehensive system-wide power quality monitoring and flexible near real-time system state simulation, a pressing need emerges for local cloud providers. This need is driven by critical factors such as security, rapid outage mitigation, and the reduction of connection timeouts, all of which are intrinsically linked to the hazards associated with electricity, including power outages and the risk of emergencies.

Comparison of foreign cloud-computing providers

According to data compiled by Synergy Research Group [13], as of the second quarter of 2023, the top three largest Cloud Service Providers are AWS, Microsoft Azure, and Google Cloud, based on their respective market shares in the global cloud infrastructure market with 32 percent, 23 percent, and 10 percent. Collectively, these leading cloud service providers command a substantial 65 percent share of the global cloud infrastructure market.

Research by R. Aljamal et al. presents a comparison between the selected cloud providers from the High-Performance Computing (HPC) user perspective [14]. It concludes that Amazon Elastic Compute Cloud (EC2) – a part of AWS – offers the most diverse range of virtual machine options, including instances optimized for CPU, memory, storage, and GPU. On the other hand, Microsoft Azure offers the most powerful GPU instances, with up to 24 NVIDIA Tesla V100 GPUs per virtual machine. Google Cloud offers the most flexible networking options, including the ability to create custom virtual private clouds (VPCs). Table 1 shows the comparison of the selected cloud providers from the perspective of

IaaS, including virtual machine options, operating systems (OS), networking, pricing, and billing details.

Table 1 – Analysis of Popular Cloud Service Providers

	Amazon	Azure	Google
Value propositions stated on the official websites [15–17]	Elasticity with auto-scaling capabilities.	High reachability.	Customized virtual machines tailored to specific needs
	Secure resource management.	Trusted brand, 90% of Fortune 500 companies choose Azure.	Leading the way in price-performance competition.
Pricing model details	Hourly on demand pricing	On demand pricing	Monthly on demand pricing
Upfront payment	✓	✓	✖
Region based billing	✓	✓	✓
OS based billing	✓	✖	✓
Instance family based billing	✓	✓	✖ (only based on amount of RAM and virtual CPUs)
Network type based billing	✓	✖	✖
Available regions	18	54	18
Available countries	190	140	35
Traffic routing	✓	✓	✖
Data Encryption	✓	✓	✓

To sum up, AWS would be the most suitable option because it offers a wide range of virtual machine options and a robust ecosystem of data analysis and processing tools, allowing for scalable and efficient analysis of large datasets in real time, which aligns well with the requirements of relay protection systems.

Conclusion

This research highlights the connection between cloud computing and emerging relay protection system models, offering a path to modernization, efficiency, and safety in dynamic industrial environments. Unlike conventional tasks, these systems operate in demanding and high-stakes environments, requiring speed, fault tolerance, and security.

An open architecture model with IIoT to enhance relay protection systems was addressed. Cloud computing plays a pivotal role, enabling real-time data analysis, remote monitoring, and scalability, vital for adaptability and security. Cost-effective PC-based clusters in cloud infrastructure offer potential cost savings. Fault resilience is ensured through parallel processing with data replication in the cloud. Furthermore, collected data in the cloud could be used for subsequent analysis. Using the ESP32 microcontroller and ESP-NOW communication protocol ensures low latency and efficient data exchange. AWS is the recommended choice for relay protection systems due to its versatile virtual machine options and robust data analysis tools.

Acknowledgement

The research was carried out within the framework of grant funding of the scientific project IRN AP13067967 «Development of technology for building microprocessor-based resource-saving relay protection devices based on open architecture».

REFERENCES

1 **Chernobrovov, N. V., Semenov, V. A.** Releinaia zashchita energeticheskikh sistem [Relay protection of energy systems]. // Energoatomizdat, 1998. – 800 p.

2 **Ashton K.** That 'internet of things' thing. // RFID journal 22.7, 2009. – 97–114p.

3. **Zhang, B., Hao, Z., & Bo, Z.** (2016). New development in relay protection for smart grid. // Protection and Control of Modern Power Systems, 1, 1–7.

4 **Kauhaniemi, K., & Voima, S.** (2012, March). Adaptive relay protection concept for smart grids. // Renewable Efficient Energy II Conference (P. 1-10).

5 **Barroso L. A., Dean J., Hölzle U.,** «Web Search For a Planet: The Google Cluster Architecture», // IEEE Micro, 23(2):22–28, April 2003.

6 **Kotas, C., Naughton, T., & Imam, N.** (2018). A comparison of Amazon Web Services and Microsoft Azure cloud platforms for high performance computing. // 2018 IEEE International Conference on Consumer Electronics (ICCE).

7 **Urazayev, D., Eduard, A., Ahsan, M., & Zorbas, D.** (2023, May). Indoor Performance Evaluation of ESP-NOW. // 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST) (P. 1–6). IEEE.

8 **Rusitschka, S., Eger, K., & Gerdes, C.** (2010). Smart Grid Data Cloud: A Model for Utilizing Cloud Computing in the Smart Grid Domain. // 2010 First IEEE International Conference on Smart Grid Communications.

9 **De Mauro, A., Greco, M., & Grimaldi, M.** (2015, February). What is big data? A consensual definition and a review of key research topics. In AIP conference proceedings (Vol. 1644, No. 1, P. 97–104). American Institute of Physics.

10 **Jolly, K.** (2018). Hands-on data visualization with Bokeh: Interactive web plotting for Python using Bokeh. // Packt Publishing Ltd. 0

11 **Pranav, P., Dutta, S., & Chakraborty, S.** (2021). Empirical and statistical comparison of intermediate steps of AES-128 and RSA in terms of time consumption. // Soft Computing, 25(21), 13127–13145.

12 **Singh, G.** (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. // International Journal of Computer Applications, 67(19).

13 URL:https://www.srgresearch.com/articles/q1-cloud-spending-grows-by-over-10-bi llion-from-2022-the-big-three-account-for-65-of-the-total [Electronic resource]

14 **Aljamal R., El-Mousa A., Jubair F. A** User Perspective Overview of The Top Infrastructure as a Service and High Performance Computing Cloud Service Providers // 2019. P. 244–249.

15 [Electronic resource] – URL:https://docs.aws.amazon.com/ [Electronic resource]

16 [Electronic resource] – URL:https://learn.microsoft.com/en-us/azure/?product=popular&WT.mc_id=Portal-Microsoft_Azure_Support

17 [Electronic resource] – URL:https://cloud.google.com/docs/

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 **Чернобровов, Н. В., Семенов, В. А.** Релейная защита энергетических систем. // Энергоатомиздат, 1998. – 800 p.

2 **Ashton K.** That 'internet of things' thing. // RFID journal 22.7, 2009. – 97 – 14 p.

3 **Zhang, B., Hao, Z., & Bo, Z.** (2016). New development in relay protection for smart grid. // Protection and Control of Modern Power Systems, 1, 1–7.

4 **Kauhaniemi, K., & Voima, S.** (2012, March). Adaptive relay protection concept for smart grids. // Renewable Efficient Energy II Conference (P. 1–10).

5 **Barroso L. A., Dean J., Hölzle U.** «Web Search For a Planet: The Google Cluster Architecture», // IEEE Micro, 23(2):22–28, April 2003.

6 **Kotas, C., Naughton, T., & Imam, N.** (2018). A comparison of Amazon Web Services and Microsoft Azure cloud platforms for high performance computing. // 2018 IEEE International Conference on Consumer Electronics (ICCE).

7 **Urazayev, D., Eduard, A., Ahsan, M., & Zorbas, D.** (2023, May). Indoor Performance Evaluation of ESP-NOW. // 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST) (P. 1–6). IEEE.

8 **Rusitschka, S., Eger, K., & Gerdes, C.** (2010). Smart Grid Data Cloud: A Model for Utilizing Cloud Computing in the Smart Grid Domain. // 2010 First IEEE International Conference on Smart Grid Communications.

9 **De Mauro, A., Greco, M., & Grimaldi, M.** (2015, February). What is big data? A consensual definition and a review of key research topics. In AIP conference proceedings (Vol. 1644, No. 1, P. 97–104). American Institute of Physics.

10 **Jolly, K.** (2018). Hands-on data visualization with Bokeh: Interactive web plotting for Python using Bokeh. // Packt Publishing Ltd. 0

11 **Pranav, P., Dutta, S., & Chakraborty, S.** (2021). Empirical and statistical comparison of intermediate steps of AES-128 and RSA in terms of time consumption. // Soft Computing, 25(21), 13127–13145.

12 **Singh, G.** (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. // International Journal of Computer Applications, 67(19).

13 [Electronic resource] – URL:https://www.srgresearch.com/articles/q1-cloud-spending-grows-by-over-10-bi llion-from-2022-the-big-three-account-for-65-of-the-total

14 **Aljamal R., El-Mousa A., Jubair F. A** User Perspective Overview of The Top Infrastructure as a Service and High Performance Computing Cloud Service Providers // 2019. С. 244–249.

15 [Electronic resource] – URL:https://docs.aws.amazon.com/

16 [Electronic resource] – URL:https://learn.microsoft.com/en-us/azure/?product=popular&WT.mc_id=Portal-Microsoft_Azure_Support 17 URL:https://cloud.google.com/docs/

Accepted for publication on 18.09.23

**А. В. Нефтисов*[1], *И. М. Казамбаев*[2], *Л. Н. Кириченко*[3],
К. М. Жакупова[4], *Д. Б. Уразаев*[5]
[1,2,3,4,5]Astana IT University, Қазақстан Республикасы, Астана қ.

Басып шығаруға 18.09.23 қабылданды.

ІІОТ ТЕХНОЛОГИЯСЫ АРҚЫЛЫ ЕСЕПТЕУ ЖҮЙЕЛЕРІМЕН ӨЛШЕУ ТҮРЛЕНДІРГІШТЕРІНІҢ ӨЗАРА ӘРЕКЕТТЕСУ МОДЕЛІ

Бұл зерттеудің объектісі өлшеу түрлендіргіштері мен есептеу жүйелері арасындағы өзара әрекеттесу моделі болып табылады, оны өнеркәсіптік Заттар интернеті (IIoT) және бұлтты технологиялар шеңберінде қолдануға ерекше назар аударылады. Бұл зерттеудің негізгі қажеттілігі-әртүрлі салалардағы деректерді дәл және тиімді жинауға, қорғауға және өңдеуге сұраныстың артуы. Зерттеу IIoT және бұлттық технологиялар арқылы өлшеу есептеу жүйелерін оңтайландыратын өзара әрекеттесу үлгісін нақтылау арқылы осы қажеттілікті қанағаттандыруға бағытталған. Біздің зерттеулеріміздің нәтижесінде деректерді берудің барлық процесін қамтитын өзара әрекеттесудің кешенді моделі жасалды. Бұл модель деректерді жинауды, аналитиканы, нақты уақыттағы байланыс хаттамаларын және деректерді берудің қауіпсіз әдістерін біріктіреді. Модель деректерді жоғары дәлдікпен және тиімділікпен жинауға, беруге және талдауға арналған құрылымды қамтиды. Біздің нәтижелеріміздің маңыздылығы модельдің электр қуаты туралы деректерді жинау және өңдеу, сондай-ақ электр ақауларын бақылау *және қорғау бойынша маңызды мәселелерді шешу қабілетінде жатыр. Бұл нәтижелер энергияны өндіру және бөлуді қоса алганда, әртүрлі өнеркәсіптік жагдайларда практикалық құндылыққа ие.*

Кілтті сөздер: релелік қорганыс, ашық архитектура, шифрлау, деректерді өңдеу, деректерді визуализациялау, заттар интернеті

**А. В. Нефтисов[1], И. М. Казамбаев[2], Л. Н. Кириченко[3], К. М. Жакупова[4], Д. Б. Уразаев[5]*

[1,2,3,4,5]Astana IT University, Республика Казахстан, г. Астана

Принято к изданию 18.09.23.

МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ИЗМЕРЯЮЩИХ ПРЕОБРАЗОВАТЕЛЕЙ С ВЫЧИСЛИТЕЛЬНЫМИ СИСТЕМАМИ ПОСРЕДСТВОМ ТЕХНОЛОГИИ IIOT

Объектом данного исследования является модель взаимодействия между измерительными преобразователями и вычислительными системами, особое внимание уделяется ее применению в рамках промышленного Интернета вещей (IIoT) и облачных технологий. Настоятельной необходимостью, лежащей в основе этого исследования, является растущий спрос на точный и эффективный сбор, защиту и обработку данных в различных отраслях промышленности. Исследование направлено на удовлетворение этой потребности путем выяснения модели взаимодействия, которая оптимизирует измерительные вычислительные системы с помощью IIoT и облачных технологий. В результате наших исследований была разработана комплексная модель взаимодействия, которая охватывает весь процесс передачи данных. Эта модель объединяет сбор данных, аналитику, коммуникационные протоколы в режиме реального времени и безопасные методы передачи данных. Модель включает в себя структуру для сбора, передачи и анализа данных с высокой точностью и эффективностью. Значимость наших результатов заключается в способности модели решать критические задачи по сбору и обработке данных об электрической мощности, а также по мониторингу и защите от электрических неисправностей. Эти результаты имеют практическую ценность в различных промышленных условиях, включая производство, выработку и распределение энергии.

Ключевые слова: релейная защита, открытая архитектура, шифрование, обработка данных, визуализация данных, интернет вещей

Теруге 18.09.2023 ж. жіберілді. Басуға 29.09.2023 ж. қол қойылды.
Электронды баспа
29.9 Mb RAM
Шартты баспа табағы 22,2. Таралымы 300 дана. Бағасы келісім бойынша.
Компьютерде беттеген: А. К. Мыржикова
Корректор: А. Р. Омарова, Д. А.Кожас
Тапсырыс №4140

Сдано в набор 18.09.2023 г. Подписано в печать 29.09.2023 г.
Электронное издание
29.9 Mb RAM
Усл. печ. л. 22,2. Тираж 300 экз. Цена договорная.
Компьютерная верстка: А. К. Мыржикова
Корректор: А. Р. Омарова, Д. А. Кожас
Заказ № 4140

«Toraighyrov University» баспасынан басылып шығарылған
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.

«Toraighyrov University» баспасы
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.
67-36-69
E-mail: kereku@tou.edu.kz
www.vestnik-energy.tou.edu.kz