

Collecting Digital Data and Evidence with Zero Knowledge Based Smart Systems: Zk-CNNChain

Remzi GÜRFİDAN*

Isparta University of Applied Science, Isparta Vocational School of Information Technology, Turkey

E-mail: remzigurfidan@isparta.edu.tr

ORCID iD: <https://orcid.org/0000-0002-4899-2219>

*Corresponding author

Bekir AKSOY

Isparta University of Applied Sciences, Mechatronics Engineering, Turkey

E-mail: bekiraksoy@isparta.edu.tr

ORCID iD: <https://orcid.org/0000-0001-8052-9411>

Mevlüt ERSOY

Süleyman Demirel University, Computer Engineering, Turkey

E-mail: mevlutersoy@sdu.edu.tr

ORCID iD: <https://orcid.org/0000-0003-2963-7729>

Received: February 2, 2026; Revised: April 10, 2026; Accepted: May 13, 2026; Published: August 8, 2026

Abstract: Large groups can make decisions via techniques like voting, referendums, and elections. During the realization and evaluation of these events, time efficiency, counting integrity, and voting reliability are crucial factors. Users can create their own polls, votes, and surveys using the interfaces created in this study. On these designed election processes, they can cast an electronic ballot. The CNN machine learning system evaluates the votes, or the counting process, with great accuracy, preventing manipulation and bias. Blockchain and zero-knowledge proof-based infrastructures support evaluation processes concurrently, enhancing voting privacy, data security, and transparency procedures. The results of the proposed CNN algorithm and the data privacy metrics demonstrate satisfactory performance.

Index Terms: Blockchain, Zero-Knowledge Proof, Machine Learning, Data Privacy.

1. Introduction

Critical decisions for corporations, employee satisfaction surveys, local and national elections, and referendums are typically conducted via voting methods. One of the most critical concerns for voters is the integrity and fairness of the democratic process. Especially when it comes to referendums, general and local elections, huge financial expenses arise. As the scale of these events increases, the financial costs associated with gathering stakeholder opinions also rise. In addition to financial costs, there is a significant time cost associated with conducting and evaluating the voting process. Furthermore, bias errors and invalid votes during the evaluation process reduce efficiency and compromise impartiality. Therefore, ensuring that voting is fast, secure, and cost-effective is of paramount importance.

Two aspects that participants and observers consider critical in voting processes are the reliability of the system and the validity of the votes cast [1]. Voters generally expect that their votes remain anonymous and untraceable. All stakeholders of the voting result are concerned about the validity and reliability of the votes cast [2].

Electronic voting systems are susceptible to various vulnerabilities, with cyber-attacks being a primary concern. Attackers may exploit these vulnerabilities to hack into the system and alter or manipulate election results. Additionally, software errors can lead to incorrect counting or loss of voting results. Malfunctions in voter equipment can endanger election security and disrupt the process. Finally, human error remains a potential vulnerability in any system. Users may inadvertently introduce errors by selecting incorrect options or making mistakes during the voting process.

To mitigate these vulnerabilities, voting systems must implement robust security protocols designed to defend against cyber-attacks. Voting software should prioritize security and be frequently updated to ensure proper functionality. Rigorous testing is essential to detect software and hardware errors. User education is crucial to minimize human errors.

Strict monitoring of the voting process can help detect errors or hacking attempts. Finally, voting results must be verified through rigorous counting and auditing processes to ensure accuracy.

The main objective of this study is to propose a new voting infrastructure supported by a Convolutional Neural Network (CNN)-based classification model and Zero-Knowledge Proof (ZKP) technology, addressing current challenges in security, data integrity, and confidentiality in electronic voting systems. In this study, the CNN's strong pattern recognition capability, particularly for image-based data, is utilized to classify voting data, while a ZKP mechanism is integrated to protect voter identity. This study addresses the following main research questions:

- What is the applicability of ZKP in electronic voting systems and what advantages does it offer compared to existing systems?
- What is the effectiveness of a CNN-based model in voting classification compared to traditional machine learning techniques?
- How can the performance of the proposed system be evaluated in terms of security, privacy and processing time?

To answer these questions, the performance of the proposed model was tested and analyzed through extensive experiments.

The motivations for this study are as follows:

- It contributes to the democratic process by minimizing invalid votes.
- The time required for vote evaluation and counting is reduced.
- Errors in counting and validating votes are eliminated.
- By ensuring voter data privacy, the security and transparency of election results are enhanced.

Specifically, the paper makes the following contributions:

- To build scalable solutions using blockchain technology, a detailed analysis is conducted to identify and emphasize the significance of characteristics such as block size, block generation rate, and transaction processing speed.
- Extensive experimentation is carried out to identify and highlight performance limitations in both permissioned and permissionless blockchain settings, which may benefit researchers in various application domains.
- A novel blockchain-based electronic voting system is presented, investigating the technology's potential to enable both permissioned and permissionless voting models.

Previous studies have emphasized the security dimensions of blockchain-based voting systems [3]. Notably, blockchain technology has been increasingly applied in various fields due to its economic, political, and reliability benefits. It is used for money transfers, remittances, and payment transactions in cryptocurrency applications. It enhances the security of loan records, mortgages, and futures transactions in economic, market, and financial sectors. Efficient applications have been developed in fields such as healthcare, government, and science. Few studies have addressed privacy issues using Zero-Knowledge Proof (ZKP) in blockchain-based voting systems [4]. In this study, a secure and efficient infrastructure is proposed to maximize valid voter participation.

ZKP is a cryptographic protocol that allows one party (the prover) to prove that it has a certain piece of information without revealing the content of that information to the other party (the verifier). This feature provides a significant advantage, especially in applications such as authentication and election systems where confidentiality is critical. Nowadays, different ZKP techniques such as zk-SNARKs and zk-STARKs are used to enhance cryptographic privacy and scalability. zk-SNARKs offer faster verification, while zk-STARKs offer a more secure infrastructure.

Data privacy refers to the protection of personal information, including sensitive data such as financial records, health information, and personally identifiable information (PII) [5]. Examples of personal data include identification numbers, names, dates of birth, and places of birth. Technological advancements have facilitated transactions using personal data [6]. Data privacy ensures that personal information is collected and used fairly in accordance with national and international laws. Collected data can be shared with platforms that ensure secure and confidential usage. Securely stored data can remain under personal control through encryption.

Data privacy laws and regulations in the EU, such as the General Data Protection Regulation (GDPR), mandate certain practices to protect personal information. Organizations that collect and use personal information must comply with these laws or face penalties. This constitutes the legal compliance aspect of data privacy. Personal information, such as names, dates of birth, and ID numbers, is sensitive and requires protection. It can be misused if it falls into unauthorized hands. Therefore, preventing unauthorized access, use, or disclosure of personal data is central to data protection. Organizations collecting personal information must maintain the trust of those whose information they collect. Ensuring data privacy is crucial for organizations handling personal information. Organizations must demonstrate their commitment to data privacy and assure users that their information is kept safe from unauthorized access. This assurance fosters continuous trust in data privacy practices.

Data privacy has become increasingly important. Even accessing a website often requires users to provide personal information during registration [7]. The risk of unauthorized access during inter-institutional data sharing is a major

concern. During transactions with companies, unauthorized users may access and leak personal information. Various security measures are implemented to ensure data confidentiality [8].

Blockchain technology has several features that can help protect data privacy. Key features include decentralization, immutability, encryption, access controls, and smart contracts. Blockchain networks are not controlled by a single chain, the data recorded in the blocks cannot be changed later, the transactions are encrypted, and it provides the general security and privacy of the blockchain as it provides access control [9].

Blockchain consists of a block of multiple data packets. Block chains are expanded by adding additional blocks and recorded in the chain. Authentication of blocks is verified by cryptographic networks. During the validation of the block, validation with the hash value (time stamp) can be added [10].

Blockchain technology ensures the confidentiality of data with chains. Data that is not protected by a single chain stores all transaction data in its memory, publicly and distributed. The fact that the data stored with blockchain technology is public can be learned by people who do not have permission to interact. ZKP (Zero Knowledge Proof) is recommended for the security of blockchain data [11].

When the user wants to log in to an institution or system, he can log in by verifying it with ZKP without using his digital signature. ZKP consists of verifier and prover. During login to the system, the confirmatory information is compared with the authenticator, if it is the same, the login to the system is allowed, if it is different, the login to the system is blocked. ZKP schemas consist of integrity and robust logic. The verifier should be able to prove himself with minimum error and answer sequentially [12]. With ZKP, the user does not need to use their digital signature while logging into the system. With the help of ZKP technology, when the user logs into the system, he/she proves his/her identity without sharing personal information. Data privacy and security are ensured when ZKP and blockchain technology are combined.

2. Related Works

While examining similar studies with this study, a search was made under two headings. The first of these titles is the studies in which ZKP, blockchain and artificial intelligence technologies are used together. The other is the examination of studies in which CNN algorithm and blockchain technology are used together.

Table 1. Aims and contributions of current studies in the subject area

Works	Year	Method	Aim	Contribution & Innovation
[13]	2020	GKR Protocol, ZKP	They aimed to provide new zero-knowledge proof for arithmetic circuits that do not have reliable setup.	The GKR protocol has proven its confidentiality and robustness with zkPVD. Proof of the time of the plan is fast. It is one time faster than the current ZKP systems and the proof-time is milliseconds.
[14]	2022	Federated learning	When a patient who is treated in one hospital goes to another hospital, his data is hidden by other hospitals. This problem has been solved	The patients were engaged in the study of unified learning, paying attention to the efficient transmission, optimization, and confidentiality of the test data.
[15]	2022	MPC	A zero-knowledge proof using the MPC-in-the-head protocol is proposed.	It has presented a zero-knowledge proof-supported signature protocol that proves the solution for syndrome decoding using the MPC-in-the-head protocol.
[16]	2022	Blockchain, ZKP	Desired to ensure data validity and consistency between data owners and cloud service providers	Resolves issues of data privacy security, data availability and consistency, and data transaction traceability in data sharing
[17]	2023	CNN, zkSNARK, ZKP	Preventing an attacker from tampering with the machine learning model, thereby breaking the model's integrity.	The zero-learning model is used to hide the data in the deep learning model.
[18]	2023	Zk-SNARK	It is aimed at developing an encryption method in which verifiable credentials prove themselves to be in digital devices.	The merkle tree created with Zk-SNARK created a digital identity by encrypting the information of the people.

In Table 1, six different studies were examined under the headings of the authors, the years of the study, the method used, the objectives of the study, and the results and innovations.

Computers are trained with one or more-layer artificial neural networks (ANNs) or multilayer deep learning algorithms. Computers trained from data with multiple layered ANNs, or multiple algorithms are expected to obtain new data. CNN (Convolutional neural network), one of the deep learning models, is trained using visual image data. Data trained with visual images can be classified with the CNN algorithm.

CNN and Blockchain technology are used together in the storage of biometric data [19, 20], in image recognition in disease prediction [21], in graphic prediction of crypto assets [22].

Today, it is seen that the use of machine learning in every field is increasing. In the medical field, health problems and deaths from diseases are increasing. Studies in the field of medicine have increased to reduce deaths because of diseases. Studies in deep learning and artificial neural networks are seen in studies such as detecting diseases and controlling the treatment process. Pawar et al. In his studies, the detection of lung diseases and the evaluation of the

treatment process were detected with Enhanced Convolutional Neural Networks (ECNN) algorithms. Algorithms trained using IOT images were classified into two classes as cancerous and non-cancerous and achieved 96.88% accuracy [23].

In another health study, Ramanan et al. It is the education and classification of mammography results of breast cancer. The data trained with the cyber-physical system (CPS) classification model classified the diseases and achieved 98% accuracy [24].

Bolete mushroom is frequently consumed by consumers due to its flavor and rich nutritional value. Dong et al. In his study, he performed machine learning to mix the bolete mushroom with poisonous mushrooms. These data, which were trained using four different machine learning, were classified into two classes. Nearly 100% accuracy was achieved with the two-dimensional correlation spectroscopy (2DCOS) model. Users can classify by logging into the system without using their personal information in the model created with the blockchain.

Changing climatic conditions and material and moral damage caused by natural disasters cause serious harm to people. Identification of flood hazard areas in Bangladesh Mia et al. It has been studied by his work. Damages in flood zones are stored by protecting their privacy with blockchain technology. This stored dataset was used to train the model. By using the CNN algorithm, areas that may be flooded have been identified [25].

Classification of data trained by machine learning is very fast and saves us time. Data sets are obtained from visual images. In this case, data privacy is important. Data used in datasets can be trained by encrypting people's information. Data privacy can be achieved by using blockchain technology.

A security protection plan based on blockchain, and zero trust has been proposed for chargers and cloud platforms in the studies. The aim of the research is to contribute to improving the safety of chargers, and finally to alleviating the energy crisis and environmental pollution. A significant part of the model supports the idea of zero trust, which can effectively protect the security of the entire lifecycle of data [26]. A new distributed BC-based access control protocol for IoT-based medical applications in e-health systems is proposed in another study to take advantage of the security procedures of blockchain. The efficiency and robustness of the protocol were analyzed with BAN logic. The findings show that the protocol has strong resistance to various competing attacks [27].

Hjálmarsson et al. proposed a new blockchain-based voting system to address the limitations of existing electronic voting systems. To this end, they evaluated various popular blockchain infrastructures to determine the most suitable platform for building a distributed electronic voting system. They aimed to securely record votes by utilizing the transparency and immutability features of blockchain. There are no experiments measuring the performance of the system they created in the study [28].

Berenjestanaki et al. state that blockchain-based e-voting systems offer advantages in terms of security, transparency and privacy compared to traditional systems. However, challenges such as scalability and technical limitations may hinder the widespread adoption of these technologies. Therefore, it is suggested that future research should address these challenges and develop more efficient blockchain-based e-voting solutions. There are no experiments measuring the performance of the system created in the study [29].

Hanifatunnisa and Rahardjo designed a blockchain-based voting registration system to address the vulnerabilities of existing electronic voting systems. This system aims to ensure that votes are securely recorded and stored in a decentralized network. The proposed approach guarantees the integrity and immutability of the data by adding each voting transaction as a blockchain block. There are no comprehensive tests that measure the performance of their system [30].

Tanwar et al. examine the use of blockchain technology to increase security and transparency in electronic voting processes. They developed a decentralized e-voting application using smart contracts on the Ethereum blockchain. This application aims to ensure that the votes are recorded in a transparent and unalterable manner while ensuring that voters remain anonymous. There are no comprehensive tests that measure the performance of the system they created in the study [31].

3. Background And Technical Preliminaries

In this section, the technical infrastructure, technology, and methods used in the realization of the study will be explained.

3.1. Zero-knowledge Proof Arguments

NP (complexity) is the complexity class that decides in undetermined polynomial time in computational complexity theory. NP problem instances are set with Turing machine proofs in polynomial time. The proof system of the NP relationship, G , specifies the setup step of the proof system to generate the general parameters. Clusters of $k \times k$ size are created for the setup phase. In the P stage, it is the proofs stage of the polynomial. The merging step of the disjoint sets tests whether it can be solved in polynomial time. If the polynomial can be solved deterministically with a Turing machine in time, then the proof of $P=NP$ is provided in the system. The V phase is the validation phase. It is proved that the sum of the subsets of the NP set is equal to the sum of the sets [17].

$(x, w) \in R$, in this part x is the input parameter of R and w is the witness. *Definition 1.* $L \in NP$ the proof system is non-interactive zero knowledge proof. [17].

Integrity: If $(x, w) R$ is a valid entry for and $(EK, VK) \leftarrow G(C, I^1)$, $\pi \leftarrow P(EK, w, x)$. $\Pr [V(VK, x, \pi)=1] = 1$

Robustness: If $(x, w) \in R$ If it is not a valid entry for P^* for a polynomial time subtractor $\mathcal{E}^A$, $\pi^* \leftarrow P^*(EK, x)$, $w \leftarrow \mathcal{E}^A(EK, x, \pi^*)$ [17]. $\Pr[V(VK, x, \pi^*)=1]$.

Zero Knowledge: There is a polynomial-time simulator S developed with zero knowledge, which witnesses from w to R for all valid inputs of x . The following two probability distributions are computationally indistinguishable [17]. $D_1: (EK, VK) \leftarrow G(C, I^\lambda); \pi \leftarrow P(EK, VK, x, \pi)$

$D_2: (EK, VK, \pi) \leftarrow S(x) : P(EK, VK, x, \pi)$

3.2. Zk-SNARK

Zero knowledge proof technologies are a method that allows a group of unknown knowledge to prove that they have knowledge by transmitting a small part of the knowledge to another group, which has the knowledge. Snarks, like Starks, are zero-knowledge proof technology that operates with different mathematical processes in ZKP solutions. The word Snark is formed from the initials of the words Succinct, non-interactive, Argument and Knowledge. Succinct means succinct. It refers to the use of only a part of the data instead of the whole. It states that the non-interactive proof verifier does not need to constantly ask questions.

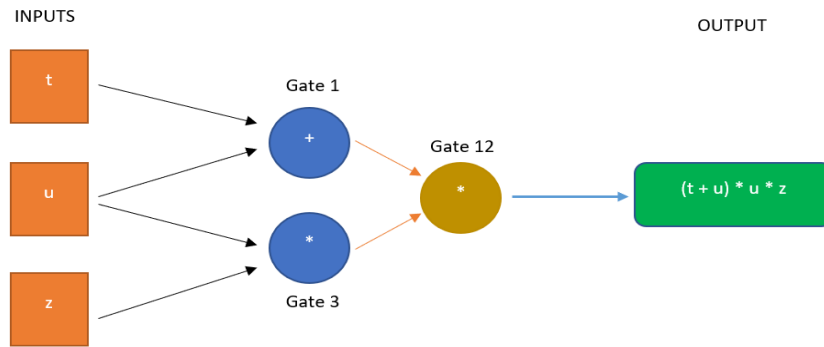


Fig.1. Optional organizational arrangement structure

Figure 1 shows how the input parameters are converted into an equation as output values. A five-step process is carried out to create proof with Zk-Snark. These processes are shown in Figure 2.

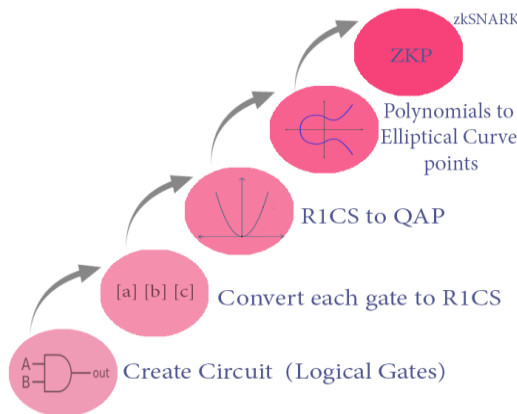


Fig.2. Optional organization edit panel

There are temporal performance differences between Zk-Starks and Zk-Snarks. Because Starks use hash functions and prefer a trustless model, they verify proofs later than Snarks, while prove time is lower than Snarks.

3.3. R1CS and QAP

Zero-knowledge proof protocols can be categorized in different ways as interactive or non-interactive. Concise Non-Interactive Information Arguments (SNARK), Scalable Transparent Information Argument (STARK), Verifiable Polynomial Delegation (VPD), and Brief Non-Interactive Arguments (SNARG) are four of them. For the writing of smart contracts within the chain, it is necessary to convert it to the Rank-1 Constraint System (R1CS) form. R1CS is a set of three vectors (a, b, c) and it is a model that expresses the product between vectors for its solution and must satisfy the mathematical equation established. The constructed mathematical equations are turned into circuits by means of logic gates. R1CS formed after these processes is taken and converted into QAP form that works with polynomial application. While R1CS performs its calculations with dot products, the Quadratic Jump Problem (QAP) performs its operations on the polynomial. After performing the equation reduction operations, you will need to resort to LaGrange Interpolation

when you want to draw a polynomial that intersects your points (x, y) with a set of coordinate pairs. The time and complexity spent on this process, with the degree of the polynomial being k ; It is calculated as $O(nk)$. Cost profitability is very important because the functions used in SNARK algorithms have many gates. At this point, Fourier transform algorithms will help us. The reason why we prefer QAP as the next step after the RICS form is that instead of checking the constraints in RICS one by one, all constraints can be checked simultaneously by doing inner product checks on polynomial lines. Using finite field arithmetic eliminates rounding errors and makes the system's zk-SNARK protocol truly secure. The necessary infrastructure is prepared for it to work in harmony with the elliptic curves required for safety.

3.4. Deep Learning Models

A total of 400 images consisting of 100 images evenly distributed for all classes constitute our data set. The picture, which is the system input, is first passed through a filter. The values formed after the filter form an attribute map for the image. In this filtering step, the image is converted to matrix form. In this way, even the smallest details in the image are taken into account. The given image has not been converted to black and white form. For pictures presented in color, this process is applied separately for each color scale (Red-Green-Blue). After the completed convolutional layer, it is passed to the Pooling layer. This layer works on the attribute matrix. The largest and smallest values in the selected dimensions are extracted in the pooling layer. To do this, max pooling or min pooling operations can be preferred. In the method performed in this study, max pooling was preferred. Convolution and pooling layers can be repeated according to the working precision. The matrix form will need to be flattened so that the matrix values obtained from these layers can be used in the Fully Connected layer. This flattening operation will be performed in the Flattening layer. After this layer, the output value will be produced according to the selected activation function. The general operating architecture of the system is shown in Figure 3.

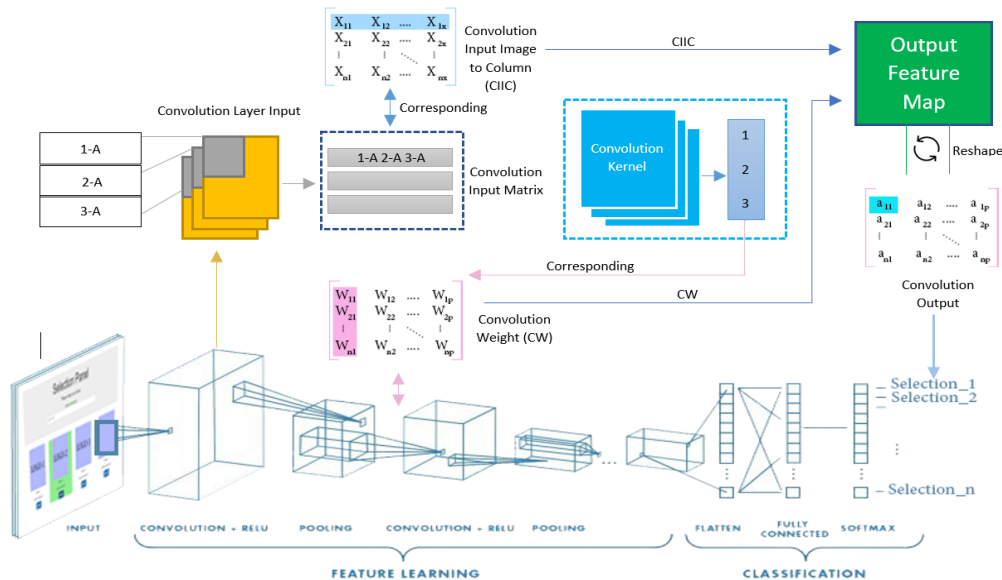


Fig.3. The overall architecture of the system

3.5. Overview of Our Scheme

With the prepared interface, it is possible to determine the preference screen and choices that will be seen by authorized voters. In this interface, the explanation sentence and selection options that will be directed to the voters are determined. The designed interface is shown in Figure 4.

Fig.4. Optional organization edit panel

The options that the voters can choose are displayed on the selection screen prepared by the authorized person. When the voter selects the option he prefers, that selection area is marked green. Voters can only make one choice. If the voter does not make an election, he cannot complete the voting process. Example images of different elections preferred by the voters are shown in Figure 5. Coloring the selected boxes facilitates the feature and feature extraction processes in the CNN algorithm.



Fig.5. Selected interface

The architecture of the data privacy and security parts of the proposed model is shown in Figure 6. After the choices made by the user in the electronic environment are classified by the CNN algorithm, the process is started to transfer the output score obtained to the block chain section.

The reason why CNNs are preferred is related to their strong learning capacity, especially on multidimensional and structured data types. Unlike traditional machine learning algorithms, CNNs can learn directly from raw data, thus eliminating the need for manual feature engineering. The capacity of CNNs to learn visual and spatial patterns is possible thanks to their ability to model local contextual relationships through convolutional layers. By extracting local features from image and spatial data, convolutional operations can identify important distinguishing features such as edges, textures, shapes and structural patterns within the data. This process brings CNNs to the forefront in problems such as vote classification, as it provides effective feature extraction, especially in multidimensional data structures.

This process must meet data privacy, data privacy and data security criteria. Received values are simulated by insertion into themselves by identical, different ledger structures. The purpose of this simulation is to eliminate the risk of the data sent to the ledgers being changed by outside intervention, the risk of being exposed to a poisoning attack, and the risk of the ledger structures being corrupted. In the data insertion simulation, each ledger combines its records with the last value to reveal an eigenvalue. The eigenvalues of identical notebooks that are different from each other should be equal. The reason why eigenvalues are preferred in this section is irreversible, one-way eigen algorithms are completely irrelevant to the data content and provide the privacy policy.

The obtained eigenvalues are sent to the validator mechanism. The verification mechanism compares the eigenvalues of different incoming ledgers with each other. The purpose of this comparison is to verify that the ledger is executed properly, and that the same data is received in each ledger. If there is any differentiation or non-matching situation because of the verification process, the rejection of data in addition to the distributed ledgers and the transition to safe mode information are sent. In this case, since the existing ledger structures have not yet added new data, the ledgers with solid records are transferred to the new chain structure with a mandatory branching process, ensuring data security and integrity. We call this situation safe mode in our system. If the values obtained because of the verification are completely identical to each other, confirmation and real data addition notification is sent to the ledgers. Notebooks that receive this approval add the information they previously simulated and maintain their identity.

ZK-CNNCHAIN exposes a global API (window.ZK-CNNCHAIN) to the metaverse environments that users access at their address, as illustrated in Algorithm 1 (Table 2). With the use of this API, websites may read data from users connected blockchains, sign their assets, and claim their ZK-CNNCHAIN accounts. To determine what platform or browser the provider is using, the @ZK-CNNCHAIN/detect-provider Provider object should be utilized, which points to a ZK-CNNCHAIN user. This procedure is detailed in Algorithm 1 (see Table 2).

Table 2. Algorithm for connecting users to ZK-CNNCHAIN

Algorithm 1 Request to connect user's accounts in ZK-CNNCHAIN	
	Input: provider - Output: true - false
1:	Import detect ZK-CnnChainProvider from "@ZK-CNNCHAIN/detect_provider."
2:	provider ← detect ZK-CnnChainProvider().
3:	if provider == true then
4:	
5:	AppStart(provider)
6:	else

```

7:         alert ("You have to Install ZK-CNNCHAIN")
8:     end if

```

This method of user transaction security creates a digital stamp that is associated with the transaction and displays the precise day, month, and year of the transaction using a peer-to-peer network-based system. The entire time it took to construct the digital certificate and digital signatures is treated as a block of data under the timestamping principle, which is then encrypted to produce a code showing the date the transaction was made. This procedure is represented by Algorithm 2 (Table 3).

Table 3. Algorithm for creating ZK-CNNCHAIN accounts

Algorithm 2 Creating ZK-CNNCHAIN	
Input: new_Block - Output: none	
1: class ZK-CNNCHAIN start class.	
2: constructorMethod ()	
3: this.ZK-CNNCHAIN $\leftarrow$ [this.createGenesisBlock()];	
4: initGenesisBlock ();	
5: return new CryptoBlock(0, "25.04.2023", "Initial Block in ZK-CNNCHAIN", "0");	
6: latestBlock();	
7: return this.ZK-CNNCHAIN[this.ZK-CNNCHAIN.length - 1]	
8: addNewBlock(new_Block);	
9: new_Block.nextHashValue $\leftarrow$ this.latestBlock().HashValue;	
10: new_Block.HashValue $\leftarrow$ new_Block.computeHashValue();	
11: this.ZK-CNNCHAIN.push(new_Block);	
12: end class	

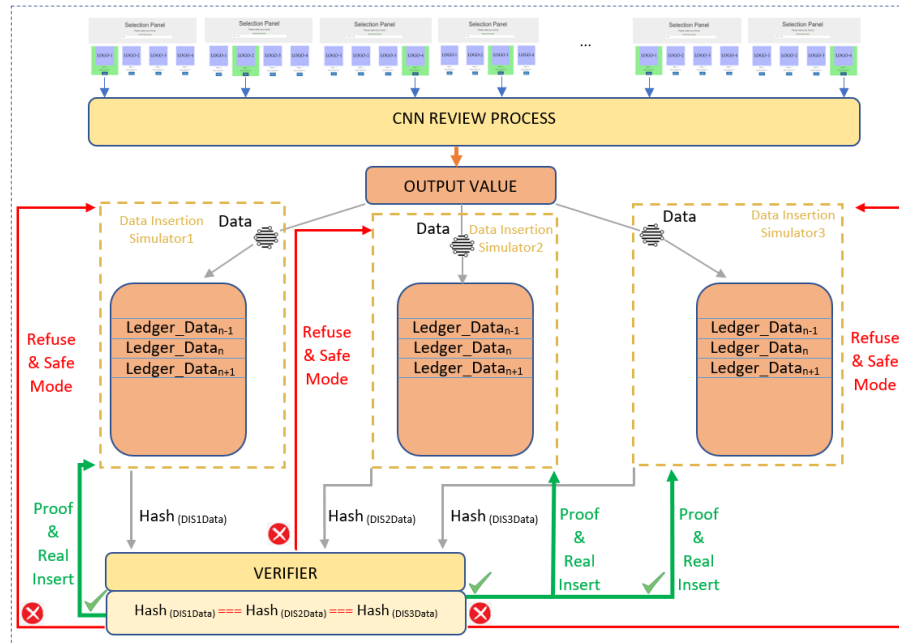


Fig.6. Architecture with data privacy and security

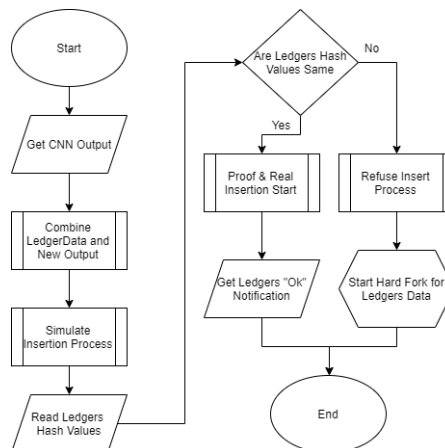


Fig.7. Optional organization edit panel

Thanks to this structure, the ledgers contribute to data privacy by not processing the content of the data. The algorithmic flowchart of the mentioned structure is shown in Figure 7.

For the security of the ZK-CnnChain blockchain, it is required to update a block after it has been added to the network using the checkValidity() method without invalidating the chain integrity. By creating a new hash for each modification made in the block, the entire blockchain is updated. Additionally, it is verified that the cryptographic hashes of the interconnected blocks are consistent. The validation function returns false if any block in the blockchain fails verification. Conversely, it returns true if the chain integrity is maintained. This procedure is represented by Algorithm 3 (Table 4).

The proposed blockchain-based electronic voting system has a hybrid structure including a CNN-based vote classification model and Zero-Knowledge Proof (ZKP) mechanism. The basic operation of this system can be summarized as follows:

- Voting: Users cast votes via smart contracts deployed on the blockchain network.
- CNN Classification: The verification process is carried out by analysing the data entered by the user through the CNN-based model.
- Verification with ZKP: The integrity of the voting data is verified with the Zero-Knowledge Proof (ZKP) mechanism without revealing the voter identity.
- Blockchain Registration: The verified vote data is recorded on the blockchain network, thus being stored securely and transparently without the need for a central authority.

Table 4. Algorithm for verifying ZK-CNNCHAIN transactions

Algorithm 3 Block validity check with check Validity	
	Input: index, current Block - Output: true - false
1:	for index in this.ZK-CNNCHAIN.length do
2:	currentBlock ← this.ZK-CNNCHAIN [index]
3:	nextBlock ← this.ZK-CNNCHAIN[index - 1]
4:	if current_Block.hash != current_Block.computeHashValue()
5:	return false
6:	end if
7:	if (currentBlock.nextHashValue!=nextBlock.HashValue)
8:	return false
9:	end if
10:	return true
11:	end for

4. Experimental Implementation and Evaluation

The performance metrics of the blockchain structure used in the developed system were measured. The purpose of this measure is to ensure data security and integrity, and prevent data tampering, while revealing the time cost of the transactions performed. Equation 1 determines the number of transactions per second for a specific time, peer u, from t_i to t_j .

$$TPS_u = \frac{Count(T_{xin}(t_i, t_j))}{t_j - t_i} \left(\frac{txs}{s} \right) \quad (1)$$

Here, TPS average values are derived using Equation 2 while considering the performance for N users.

$$\overline{TPS} = \frac{\sum u TPS_u}{N} \left(\frac{txs}{s} \right) \quad (2)$$

The consensus protocol used by ZK-CNNCHAIN will send and consume network data for blocks or additional transactions. Equation 3 monitors this network data stream consumption from time t_i to time t_j .

$$TPDN_u = \frac{Count(T_{xin}(t_i, t_j))}{\int_{t_i}^{t_j} Upload(t) + Download(t)} \left(\frac{txs}{kilobytes} \right) \quad (3)$$

Transactions per Unit of Network Data (TPND) is used here. DOWNLOAD(t) is the size of the download stream, and UPLOAD(t) is the size of the data upload stream at point t in the network. Equation 4 yields the average overall data stream usage.

$$\overline{TPDN} = \frac{\sum u TPDN_u}{N} \left(\frac{txs}{kilobytes} \right) \quad (4)$$

Latency (Response Time): Measures the time taken from vote submission to its validation in the blockchain. Memory and CPU Utilization: This metric analyzes the resource consumption of the CNN classification model and blockchain

validation process. Experiments showed that the system maintained stable TPS and response time up to 5000 simultaneous users, after which performance degradation was observed due to network bandwidth limitations.

Figure 8 illustrates the processing throughput relative to the data input rate.

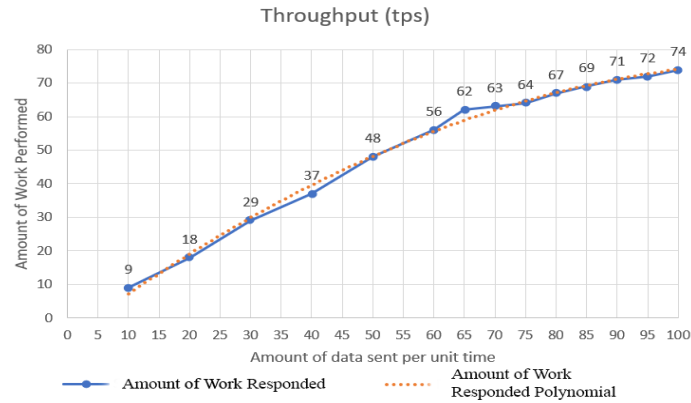


Fig.8. Processing throughput of the data recording process

Considering the amount of work sent per unit time in the performance test environment to determine the limits of the system, and considering the security contribution obtained, the latency is within an acceptable range.

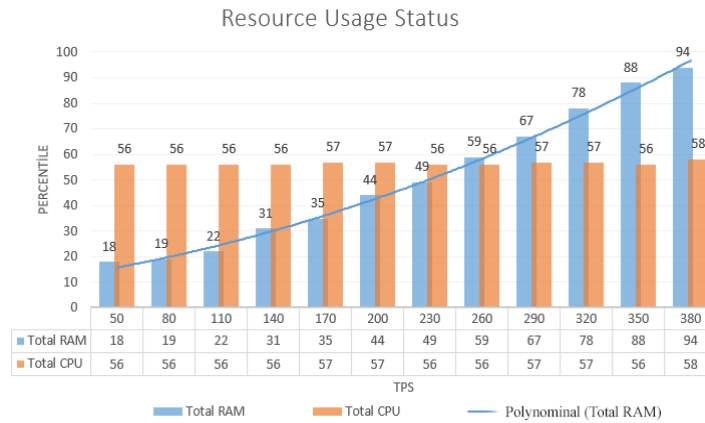


Fig.9. Resource usage of the data recording process

Figure 9 shows the resource utilization rates of the test computer during blockchain transaction processing. In our computer, which has strong processing power and RAM capacity, we attempted to measure the system's upper limits by increasing the amount of work demand per unit time. In the results obtained, it was determined that the CPU capacity remained constant and the RAM usage increased polynomially up to 380 TPS.

Figure 10 shows the confusion matrix of the system in a voting process with 4 different options. As can be seen from here, the system exhibits full stability and accurate performance.

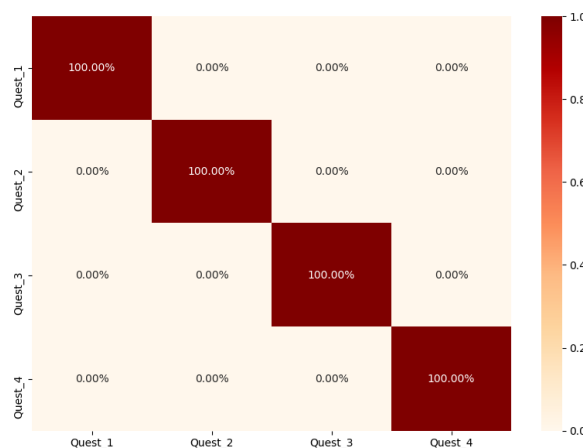


Fig.10. Confusion matrix for a voting process with 4 options

Figure 11 shows the confusion matrix of the system in a voting process with 12 different options. As can be seen from here, the system exhibits high stability and accurate performance.

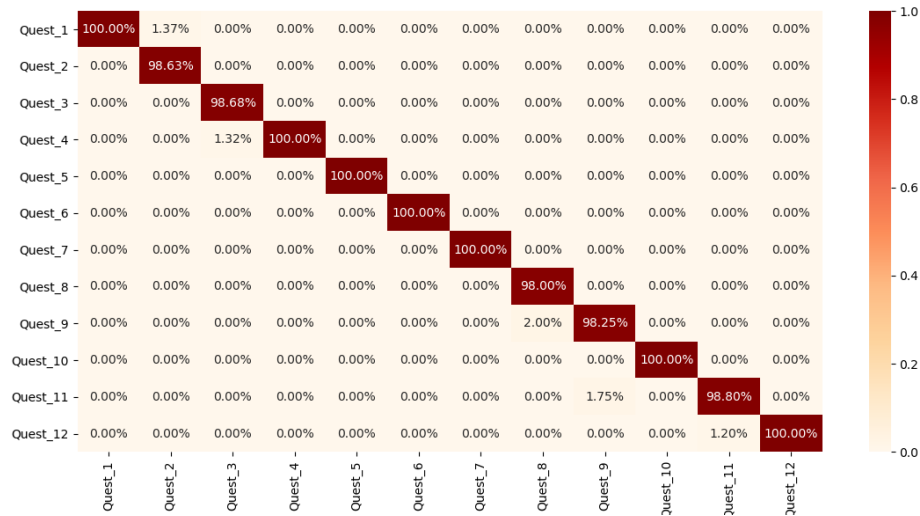


Fig.11. Confusion matrix for a voting process with 12 options

To evaluate the system's performance under simultaneous usage, we conducted a test scenario, resulting in the graph shown in Figure 12. The applied test scenario simulates the simultaneous operation of 1 to 10,000 users on the system. Under normal conditions, the duration of user operations on the system was measured as 57-62 ms on average. This number increases depending on the increase in the number of people on the system.

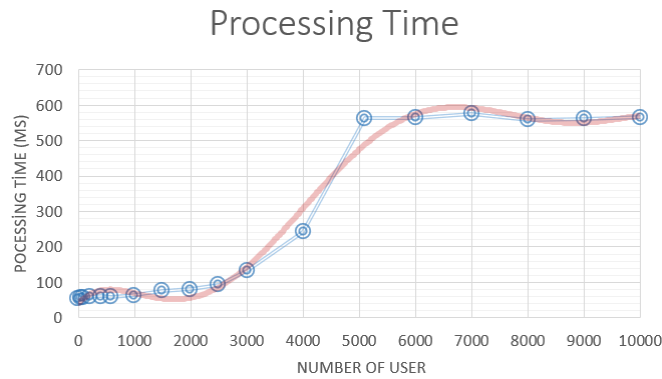


Fig.12. Performance under multiple simultaneous users (simulating a DDoS attack scenario)

Since the proposed blockchain-based voting system is based on a decentralized structure, it offers higher scalability compared to traditional electronic voting systems. This scalability is provided by the blockchain's data sharing mechanism between nodes. In particular, the fact that the data is not stored on a central server ensures that the system does not experience bottleneck problems even under high user numbers.

The system maintains stable performance up to 5000 users, after which the response time stabilizes at a constant average value. It is thought that the slowdown in this transaction processing time and the stabilization of the increasing trend is related to the bandwidth of the network on which the current system is running. This limitation of the current situation can be solved by performing the necessary tests at different bandwidths. This testing process simulates conditions similar to a Distributed Denial of Service (DDoS) attack. The aim of these experiments is to determine the upper limits of the proposed system.

While blockchain and Zero-Knowledge Proof (ZKP) enhance privacy and security in electronic voting, potential threats such as Sybil attacks, replay attacks, 51% attacks, and validator collusion remain concerns. To mitigate these risks, our system implements permissioned blockchain models to prevent majority control, ZKP-based authentication to ensure unique voter identities without revealing personal data, and timestamping with nonce verification to prevent vote duplication. Additionally, consensus-based validation mechanisms safeguard vote integrity, and zk-SNARKs reduce communication overhead while maintaining privacy. Future improvements will focus on post-quantum cryptographic enhancements to strengthen resistance against emerging security threats.

5. Conclusions and Future Work

Decision-making in large groups is facilitated by methods such as voting, referendums, and elections. Voting reliability, counting honesty and time cost are important processes during the realization and evaluation process of these events.

Through the interfaces developed in this study, users can design their own surveys, referendums and voting processes. They can vote electronically on these designed election procedures. Evaluation of the votes, that is, the counting process, is carried out with high accuracy by the CNN machine learning algorithm, preventing manipulation and bias. At the same time, evaluation processes are supported by blockchain and zero-knowledge proof-based infrastructures, contributing to voting privacy, data security and transparency processes.

Two different election scenarios were prepared in the vote counting tests. There are different numbers of output values in these scenarios. While the developed selection evaluation system achieved 100% success in a four-option system, it showed an average of 99% success in a twelve-option system. When the transaction time costs of the working mechanism are evaluated, the system operates without disruption for 2000 to 5000 users in multi-user scenarios. In this scenario, it is determined that the response times of the transaction process are fixed after 5000 users, and it is concluded that this is due to the network performance in which the system is running. In the measurements performed for the data recording and transaction processes of the proposed model, the amount of work that can be performed against the transaction requests sent per second has been evaluated. With this measurement, we attempted to measure the operational efficiency of the system. As a result of the values we have obtained, the general architecture can operate with full efficiency up to 65 transactions per second. The system throughput gradually decreases for transaction requests exceeding 65 TPS. In the tests performed up to 100 tps, the response rate remains at the level of 70. Although this is not seen as a problem, it can be solved with a simple queue structure. The resource usage of the systems running during the testing phase of the scenarios was also emphasized. Our results in this regard, while CPU usage remained constant at 57%–58%, RAM usage increased to 95% as the TPS increased. RAM usage reached 95% when 380 simultaneous requests were submitted from a voting device. Since such a scenario is unlikely to occur in real-world applications, the system's upper limits were thoroughly tested. As a result, it can be said that it performed quite successfully.

In future studies, it is planned to develop the system in a way that will accommodate a larger user base by considering its functionality and prevalent potential. In addition, micro-queuing structures will be integrated to provide a higher response to all concurrent tasks coming to the architecture.

All the Declarations and Statements

Author Contributions Statement

Remzi Gürfidan – Conceptualization, Methodology, and Supervision: proposed research ideas, constructed the overall framework, and supervised project execution.

Bekir Aksoy – Data Curation and Software Implementation: handled data acquisition and implemented the research model.

Mevlüt Ersoy – Model Training, Validation, and Performance Evaluation: Led the model training process, validated results using standard metrics, and benchmarked performance against existing methods.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

None

Data Availability Statement

None

Ethical Declarations

None

Acknowledgments

Not Applicable

Declaration of Generative AI in Scholarly Writing

The authors did not use AI or AI-assisted methods in any part of the study.

Abbreviations

The following abbreviations are used in this manuscript:

AI – Artificial Intelligence
 ANN – Artificial Neural Network
 API – Application Programming Interface
 BAN – Burrows–Abadi–Needham Logic
 BC – Blockchain
 CNN – Convolutional Neural Network
 CPU – Central Processing Unit
 CPS – Cyber-Physical System
 DDoS – Distributed Denial of Service
 DL – Deep Learning
 ECNN – Enhanced Convolutional Neural Network
 GDPR – General Data Protection Regulation
 GKR – Goldwasser–Kalai–Rothblum Protocol
 IoT – Internet of Things
 MPC – Multi-Party Computation
 NLP – Natural Language Processing
 NP – Nondeterministic Polynomial Time
 QAP – Quadratic Arithmetic Program
 RAM – Random Access Memory
 RICS – Rank-1 Constraint System
 SNARG – Succinct Non-Interactive Argument
 SNARK – Succinct Non-Interactive Argument of Knowledge
 STARK – Scalable Transparent Argument of Knowledge
 TPS – Transactions Per Second
 TPND – Transactions per Unit of Network Data
 VPD – Verifiable Polynomial Delegation
 ZKP – Zero-Knowledge Proof
 zk-SNARKs – Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge
 zk-STARK – Zero-Knowledge Scalable Transparent Argument of Knowledge

References

- [1] S. D. Ayyıldız and D. Arda, “Güvenli elektronik seçim için sır paylaşım şemalarının uygulanması,” M.S. thesis, Trakya Üniversitesi Fen Bilimleri Enstitüsü, 2021.
- [2] N. Aydın, “Klasik oylama yönteminin elektronik oylama yöntemlerine evrilmesi,” *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, vol. 12, no. II, pp. 711–744.
- [3] Ö. Ü. Polat, “Blok zincir teknolojisi ve vergileme,” in *Sosyal Bilimler Alanında Teori, Uygulama, Tarihsel ve Güncel Tartışmalar*, 2022, p. 115.
- [4] N. Kahraman, “Blokzincir teknolojisinin yerel yönetimlerde kullanımı,” in *21. Uluslararası Kamu Yönetimi Forumu Tam Metinler Kitabı*, 2022, p. 77.
- [5] V. G. Demirci, “Dijital reklamcılıkta makine öğrenmesi ve veri gizliliği,” *Kent Akademisi*, vol. 15, no. 3, pp. 1455–1474.
- [6] Ö. Özkaya and İ. Toprak, “Türkiye’de güvenlik faaliyetleri kapsamında kişisel verilerin işlenmesi,” *MANAS Sosyal Araştırmalar Dergisi*, vol. 11, no. 3, pp. 1291–1305, 2022.
- [7] X. Yang and W. Li, “A zero-knowledge-proof-based digital identity management scheme in blockchain,” *Computers & Security*, vol. 99, Art. no. 102050, 2020.
- [8] M. K. Hasan, A. Alkhalifah, S. Islam, N. Babiker, A. K. M. Habib, A. H. M. Aman, and M. Hossain, “Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations,” *Wireless Communications and Mobile Computing*, vol. 2022, 2022.
- [9] J. J. Bambara and P. R. Allen, *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*. New York: McGraw-Hill Professional, 2018.
- [10] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.
- [11] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng, “A survey on zero-knowledge proof in blockchain,” *IEEE Network*, vol. 35, no. 4, pp. 198–205, 2021.
- [12] M. D. V. Barros, F. Schardong, and R. F. Custódio, “Leveraging self-sovereign identity, blockchain, and zero-knowledge proofs to build a privacy-preserving vaccination pass,” *arXiv preprint arXiv:2202.09207*, 2022.
- [13] J. Zhang, T. Xie, Y. Zhang, and D. Song, “Transparent polynomial delegation and its applications to zero-knowledge proof,” in *Proc. IEEE Symp. Secur. Privacy*, May 2020, pp. 859–876.
- [14] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, “Federated learning for healthcare informatics,” *Journal of Healthcare Informatics Research*, vol. 5, no. 1, pp. 1–19, 2021.

- [15] T. Feneuil, A. Joux, and M. Rivain, "Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs," *Cryptology ePrint Archive*, 2022.
- [16] T. Feng, P. Yang, C. Liu, J. Fang, and R. Ma, "Blockchain data privacy protection and sharing scheme based on zero-knowledge proof," *Wireless Communications and Mobile Computing*, vol. 2022, Art. no. 1040662, 2022, doi: 10.1155/2022/1040662.
- [17] Y. Fan, B. Xu, L. Zhang, J. Song, A. Zomaya, and K. C. Li, "Validating the integrity of convolutional neural network predictions based on zero-knowledge proof," *Information Sciences*, 2023, doi: 10.1016/j.ins.2023.01.036.
- [18] M. Babel and J. Sedlmeir, "Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs," *arXiv preprint arXiv:2301.00823*, 2023, doi: 10.48550/arXiv.2301.00823.
- [19] A. Goel, M. Agarwal, M. Vatsa, R. Singh, and N. Ratha, "Securing CNN model and biometric template using blockchain," in *Proc. 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, Tampa, FL, USA, 2019, pp. 1–7, doi: 10.1109/BTAS46853.2019.9185999.
- [20] J. A. Alzubi, O. A. Alzubi, A. Singh, and M. Ramachandran, "Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1080–1087, Jan. 2023, doi: 10.1109/TII.2022.3189170.
- [21] T. Usuzaki, K. Takahashi, K. Umemiya, M. Ishikuro, T. Obara, M. Kamimoto, and K. Majima, "Augmentation method for convolutional neural network that improves prediction performance in the task of classifying primary lung cancer and lung metastasis using CT images," *Lung Cancer*, vol. 160, pp. 175–178, 2021, doi: 10.1016/j.lungcan.2021.06.021.
- [22] I. E. Livieris, N. Kiriakidou, S. Stavroyiannis, and P. Pintelas, "An advanced CNN-LSTM model for cryptocurrency forecasting," *Electronics*, vol. 10, no. 3, Art. no. 287, 2021.
- [23] A. B. Pawar, M. A. Jawale, P. William, G. S. Chhabra, D. S. Rakshe, S. K. Korde, and N. Marriwala, "Implementation of blockchain technology using extended CNN for lung cancer prediction," *Measurement: Sensors*, vol. 24, Art. no. 100530, 2022.
- [24] M. Ramanan, L. Singh, A. S. Kumar, A. Suresh, A. Sampathkumar, V. Jain, and N. Bacanin, "Secure blockchain-enabled cyber-physical health systems using ensemble convolution neural network classification," *Computers and Electrical Engineering*, vol. 101, Art. no. 108058, 2022.
- [25] M. U. Mia, M. Rahman, A. Elbeltagi, A.-A. Mahbub, G. Sharma, H. T. Islam, *et al.*, "Sustainable flood risk assessment using deep learning-based algorithms with a blockchain technology," *Geocarto International*, pp. 1–29, 2022.
- [26] P. Li, W. Ou, H. Liang, W. Han, Q. Zhang, and G. Zeng, "A zero trust and blockchain-based defense model for smart electric vehicle chargers," *Journal of Network and Computer Applications*, vol. 213, Art. no. 103599, 2023.
- [27] X. Xiang, J. Cao, and W. Fan, "Decentralized authentication and access control protocol for blockchain-based e-health systems," *Journal of Network and Computer Applications*, vol. 207, Art. no. 103512, 2022.
- [28] F. Ş. Hjalmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjalmtýsson, "Blockchain-based e-voting system," in *Proc. 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, Jul. 2018, pp. 983–986.
- [29] M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, "Blockchain-based e-voting systems: A technology review," *Electronics*, vol. 13, no. 1, Art. no. 17, 2023.
- [30] R. Hanifatunnisa and B. Rahardjo, "Blockchain-based e-voting recording system design," in *Proc. 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, Oct. 2017, pp. 1–6.
- [31] S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu, "Implementation of blockchain-based e-voting system," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 1449–1480, 2024.

Authors' Profiles



Dr. Remzi GÜRFİDAN is an Associate Professor of cybersecurity applications and research at Isparta University of Applied Sciences. He completed his master's degree in the Department of Electronics and Computer Engineering. He has experience in software development, cybersecurity, and deep learning. He is the author of two books on blockchain technologies. He has served as Editor-in-Chief for two international engineering journals.



Dr. Bekir AKSOY is an Associate Professor in the Department of Mechatronics Engineering at Isparta University of Applied Sciences. He focuses on image processing and artificial intelligence.



Dr. Mevlüt ERSOY is an Associate Professor in the Department of Computer Engineering at Süleyman Demirel University. His research interests include cybersecurity, artificial intelligence algorithms, and computer networks. Currently, he is actively conducting a TÜBİTAK project in software engineering and a BAP project related to development boards.

How to cite this paper

Remzi GÜRFİDAN, Bekir AKSOY, Mevlüt ERSOY, "Collecting Digital Data and Evidence with Zero Knowledge Based Smart Systems: Zk-CNNChain", International Journal of Information Technology and Computer Science(IJITCS), Vol.18, No.4, pp.17-31, 2026. DOI:10.5815/ijitcs.2026.04.02