SDU

1996

UNIVERSITY

Journal of Emerging Technologies and Computing (JETC)

Journal of Emerging Technologies and Computing (JETC)

is a peer-reviewed, open-access national and international scientific journal. Thematic areas: Computer Science, Infocommunication Technologies, and Mathematics with Applied Aspects

Publisher: SDU University

The journal is registered and licensed as an online publication and printed journal by the Ministry of Information and Social Development of the Republic of Kazakhstan.

Certificate (Online publication): No KZ01VPY00120097

Certificate (Printed journal): No KZ71VPY00120098

ISSN: 3105-6342 (online)

ISSN: 3105-6334 (print)

Frequency: four times a year (March, June, September, December)

Website: https://jetc.sdu.edu.kz

Editorial Board

Ministry of Science and Higher Education of the Republic of Kazakhstan

SDU University

Journal of Emerging Technologies and Computing (JETC)

Volume 4, Issue 1 • March 2026

Kaskelen, Kazakhstan — 2026

CONTENTS

SECTION I
Computer Science

This section focuses on current research directions and applied advancements
in Computer Science, particularly in the areas of artificial intelligence,
software engineering, and intelligent systems.

Article

A Data-Driven Digital Framework for Enhancing Parental Engagement and Cognitive Development in Kazakhstani Children: A Survey and Correlation Study

Aziza Aipenova* [1, 2]

[1]Department of Information Systems, SDU University, Almaty, Kazakhstan

[2]School of Information Sciences, University of Illinois Urbana-Champaign, Champaign, IL

DOI: 10.47344/mbx66d96

Abstract

This study examines early childhood cognitive development in Kazakhstan using a computational, technology-assisted method, highlighting the critical need for data-driven, culturally appropriate interventions. For statistical analysis, survey data from a cross-sectional sample of Kazakhstani parents ($n = 21$) with children ages 0–6 were encoded. Correlation analysis showed a chronic implementation deficiency, although 93% participants expressed strong awareness of early development. The study found a very strong negative relationship ($r \approx -0.88$) between reported child anger/control issues (Variable N) and knowledge about significant brain development periods (Variable J), as shown in Table III. This suggests that parental education directly improves emotional management. On the other hand, a significant negative relationship ($r \approx -0.71$) was found between reported speech clarity (Variable K) and brain knowledge (Variable J), showing that knowledgeable parents use stricter criteria when evaluating achievements. Furthermore, a strong positive correlation ($r \approx 0.638$) has been found between the parents' subjective self-rating of the quality of early development (Variable E) and their technical knowledge of brain development (Variable J), indicating that more positive perceptions of developmental progress are related to a deeper

*Corresponding author: aziza.aipenova@sdu.edu.kz

Email: aziza.aipenova@sdu.edu.kz ORCID: 0000-0002-5104-7429

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

understanding. Using the Vue and Vuetify frameworks, a prototype digital platform was created to fill these gaps and integrate awareness into consistent, evidence-based action. The study presents a scalable, data-driven approach for delivering culturally responsive early childhood interventions in the Kazakhstani context, despite its limitations due to its cross-sectional design and small sample size.

Keywords: cognitive computing, educational technology, digital platforms, early childhood development, data-driven analysis, parental engagement, cross-cultural perspective, Kazakhstani children

I. Introduction

With a growing percentage of children experiencing developmental delays, especially in speech and cognitive capacities, the field of child development faces constant problems. The worldwide agreement, supported by seminal work such as Ibuka's [1], emphasizes that the essential period for intellectual and emotional development occurs between birth and age three. However, Kazakhstan currently lacks culturally appropriate educational programs that focus on early cognitive and emotional development. To close this gap, the current study presents a comprehensive, methodical approach for Kazakhstani children aged 0–6, grounded in developmental psychology and neuroscience. Additionally, a website was created to increase awareness, support research-based child-rearing practices, and offer resources to researchers, educators, and parents. By providing a culturally compatible digital prototype in the Kazakh language to supplement professional guidance with everyday, practical implementation techniques, this study fills in the gaps noted in Table I.

A. Literature Review

High-quality relationships and engagement have a significant impact on cognitive outcomes during the intense period of neuroplasticity in early childhood [2], [3]. Language acquisition, ability to concentrate, and emotional control are particularly vulnerable to genetic and environmental variables during the first three years of life. Children's intellectual, social, and emotional development is routinely enhanced by educational philosophies such as Maria Montessori's, which promote independence and self-directed learning [4]. Because structured activities and responsive approaches to parenting are consistently linked to more robust cognitive and emotional development, parental participation is crucial [5].

The Role of Technology in Early Intervention

In recent years, technology has revolutionized access to early childhood resources. While traditional approaches remain vital [6], digital tools are emerging as critical support mechanisms [7]. However, efficacy is conditional on institutional support and user literacy. [8] found that preschool teachers often demonstrate higher digital literacy than parents, indicating a critical skills gap that must be addressed for digital platforms to succeed in the home environment. Furthermore, [9] found that parents are far more engaged when schools provide well-structured technological tools and when social influences (from teachers and other parents) actively support technology adoption. This highlights the need for a collaborative, not isolated, digital framework.

Sociocultural Context and Implementation Gaps

The social environment of development is fundamental to it [10]. Linguistic disparities influence parents' information-seeking behaviors in the Central Asian environment, with Kazakh-speaking parents more likely to seek professional assistance, according to [11]. This highlights the need for intervention to be culturally and linguistically relevant.

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

TABLE I
SYNTHESIS OF KEY LITERATURE AND RESEARCH GAPS JUSTIFYING THE DIGITAL INTERVENTION

Study/Source	**Focus**	**Key Finding**	**Gap Addressed by Current Study**
Ibuka [1]/ General Theory	Critical Period	The first three years are the most important for development (0-3).	Need for structured, easily accessible intervention programs for parents of 0-6-year-olds.
Landry et al. [5]	Parental Engagement	Responsive parenting and structured activities lead to robust cognitive development.	Need for a digital platform to deliver structured activities and responsive guidance to parents.
Khan et al. [11]	Linguistic Context	Information-seeking can be affected by linguistic differences; Kazakh speakers frequently favor expert advice.	Mandate: The intervention must be given in Kazakh and intended to support expert advice.
Akman et al. [8]	Digital Literacy	Compared to parents, preschool teachers are more digitally literate.	Challenge: The framework needs to reduce the digital literacy gap among parents and incorporate basic UX/UI principles.
Osorio-Saez et al. [9]	Technology Adoption	Parental engagement increases with school-provided tools and positive social influence.	Solution: To encourage social adoption, the framework needs to be set up as a cooperative tool (forums/sharing).
Hirsh-Pasek and Golinkoff [7]	Educational Technology	Multimedia and gamified environments are effective tools for assisting development.	Need for a culturally relevant digital platform prototype built with modern frameworks (Vue/Vuetify).
Bornstein [10] / Knudsen [3]	Sociocultural Context	Cultural differences significantly impact child development; there is an urgent need for adapted, local programs.	Focus on the Kazakhstani context to develop a comprehensive program in the Kazakh language.

Based on the synthesis of previous research and the gaps mentioned in Table I, the next section discusses the specific developmental approaches and the theoretical framework chosen for this study.

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

II. Methods

A. Early Cognitive Development Strategies: The Significance of Parental Intervention and Involvement

The family defines a child's primary environment in the early years of life. Since their interactions offer the first and most significant form of social experience, parents have a significant impact on how children develop cognitively and emotionally. Parents are crucial mediators of early learning opportunities, and research consistently shows that working with a child's environment is more effective than focusing solely on the child [1]. Parents are responsible for taking preventative actions to ensure healthy development in addition to providing daily care and play. For early intervention programs to be effective, they must continue to be flexible and adjust to the changing needs of families and children. Since these programs aim to influence various aspects of growth through collaboration between professionals and caregivers, parental involvement at every stage is essential.

In order to structure the analysis, this study divided early cognitive development into four age-specific phases: infancy (0–12 months), toddlerhood (1–2 years), early preschool (2–4 years), and later preschool (4–6 years). Parental awareness was examined using surveys that examined developmental milestones over these periods. The study's results led to recommendations on how parents can enhance cognitive development at home. Piaget's theory provides a useful framework for understanding these developmental stages. His concepts of assimilation—the integration of new experiences into preexisting mental structures—and accommodation—the adaptation of mental structures to new experiences—explain the mechanisms by which infants acquire information [12]. Cognitive development happens in a specific order, according to Piaget: sensorimotor, preoperational, concrete operational, and formal operational. Each stage, like the steps on a staircase, reflects a qualitatively new style of thinking and builds on the achievements of the one before it [13].

B. Early Foundations: Handling Early Childhood Cognitive and Emotional Milestones

Early life is one of the most critical periods for cognitive and emotional development. During this time, the parent-infant bond is essential for establishing secure interactional patterns that lay the groundwork for future development. Reflexive behaviors, such as oral reflexes like the mouth-palm and chewing reflexes, as well as defensive reactions like blinking or head-turning, predominate in the neonatal stage. Early motor coordination is supported by spinal reflexes like crawling, grasping, or the Moro reflex, whereas neural reflexes connect head position to body posture. As higher brain functions develop over the first three to five months, these early reflexes begin to fade away [14]. Children go through a phase of rapid speech and cognitive development between the ages of one and two. They start to mimic speech sounds, pronounce their first words, and try to follow basic instructions during this phase. Social interaction and vocabulary development are closely related because children try to mimic adult language patterns and express their needs. Additionally, memory and focus get better. When doing simple tasks or stacking blocks, for example, children can focus for longer periods of time. The development of goal-directed groundwork, which serves as the basis for subsequent problem-solving skills, is reflected in such continuing focus. During this phase, play becomes more symbolic. Children start to develop social awareness and practice expressing their emotions through pretend play, such as by modeling parental roles. Simultaneously, the ability to differentiate between the similarities and differences of objects improves reasoning abilities. Early speech, memory, and creative play all work together to lay the foundation for later socialization and academic success [15].

III. Experimental work

A. Participants and Procedure

To investigate the connection between parental involvement and early cognitive developmental outcomes in the Kazakhstani environment, this study used a cross-sectional, computationally assisted methodology. To collect quantifiable data on awareness and developmental milestones, parents of children aged 0 to 6 participated in a standardized survey. Prioritizing ethical behavior, the methodology obtained explicit verbal consent from each participant before any data were collected. To get a cross-sectional sample size of 21 parent-child pairs ($n = 21$), the technique employed a convenience sampling approach among parents in Almaty, Kazakhstan, specifically within the "Dostyk" group in Iasli-sad No. 37. This method served as a basis for integrating objective milestone attainment observations with subjective parental input.

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

B. Survey Instrument and Key Terminology

The questionnaire covered five significant domains of growth: (1) parental knowledge about early development; (2) cognitive and emotional stimulation during infancy; (3) crucial developmental phases like crawling, speech clarity, and emotional regulation; (4) exposure to professional support (e.g., speech therapy); and (5) attitudes toward comprehensive child development. Examples of questioning were ”Do you know about early development?” ”At what age did your child begin to speak clearly?” ”Is emotional development important?” and also, ”Can harmonious development be achieved by allocating 5-25 minutes daily?”

The following important terms are defined for the precise interpretation of the results:

Harmonious Development: This phrase describes a thorough, well-rounded approach to child development that includes the coordinated development of cognitive, emotional, and physical skills during the early years of life.

The term ”psychophysiological outcomes” refers to developmental markers, such as the age of reflexive integration, fine motor abilities, and emotional self-regulation (as determined by parent-reported milestone attainment), that reflect the interplay of mental and physical processes.

Excel spreadsheets were used to compile and analyze the responses (Figures 1 and 2). Significant developmental gaps were found by the analysis, especially in the areas of emotional self-regulation, speech clarity, and regular parental participation in early stimulation techniques. The raw data showed that 93 % parents responded ’No’ when asked about knowledge of the 0-6 age developmental period. This low awareness is directly related to the inadequate implementation of structured cognitive milestones, serving as the primary justification for the intervention design. These results highlight the fact that insufficient parental awareness and structured involvement are frequently associated with developmental deficiencies.

Fig. 1. Answers to questions

	A	B	C	D	E	F	G	H	I	J
1		1. How was the child born?	2.Do you know about early development?	3. Were you engaged in early development of a child?	4.What is the early development? In your opinion	5. Have you been exercising from 0 to 12 months?	6.How many months has your child been crawling?	7. Did you know that there are 6 directions of harmonious development?	8. Is Emotional Development important?	9. Did you know that at the age of 0-6, the main part of the brain (90-93 %) develops?
2	Dariya	natural	Yes	Also working	All	Yes	6 month	No	Yes	No
3	Aibar	natural	Yes	Yes	All	Yes	7 month	No	Yes	Yes
4	Ayala	natural	Yes	Also working	All	Yes	5 month	No	Yes	Yes
5	Nurasyl	natural	Yes	No	All	No	7 month	No	Yes	Yes
6	Beybit	natural	Yes	Yes	All	Yes	6 month	No	Yes	Yes
7	Aruna	natural	Yes	Yes		Yes	7 month	No	Yes	Yes
8	Ayana	natural	Yes	Also working	All	Yes	5 month	No	Yes	No
9	Dias	natural	Yes	Yes	All	Yes	7 month	No	Yes	No
10	Inzhu	natural	Yes	Yes	All	Yes	6 month	No	Yes	Yes
11	Aksultan	natural	Yes	Yes	All	No	6 month	Yes	Yes	Yes
12	Aya	natural	Yes	Yes	All	Yes	6 month	No	Yes	Yes
13	Sauran	natural	Yes	Yes	All	Yes	The child immedia	No	Yes	Yes
14	Akhmet	natural	Yes	Also working	All	Yes	6 month	Yes	Yes	Yes
15	Aidana	Caesarean section	Yes	Yes	All	Yes	6 month	No	Yes	Yes
16	Zeyin	Caesarean section	Yes	No	All	Yes	7 month	No	Yes	Yes
17	Daniyal	Caesarean section	Yes	Yes	All	Yes	7 month	No	Yes	Yes
18	Adelya	Caesarean section	Yes	Yes	All	Yes	5 month	No	Yes	Yes
19	Safiya	Caesarean section	Yes	Yes	All	Yes	7 month	No	Yes	Yes
20	Damir	Caesarean section	Yes	Also working	All	Yes	6 month	No	Yes	Yes
21	Galiyabanu	Caesarean section	Yes	Also working	All	Yes	7 month	No	Yes	Yes
22	Adina	Caesarean section	Yes	Yes	All	Yes	6 month	No	Yes	Yes

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

Fig. 2. Answers to questions

K	L	M	N	O	P	Q	R	S
10.Is your child speaking clearly?	11.At what age did your child speak clearly?	12.Can your child explain to you what he wants?	13.Your child gets angry when he doesn't get what he wants?	14.Has your child worked with a speech therapist?	15. Is there any special feature?	16. Do you want your child to develop comprehensively ? Does this require a job?	17. Is it possible to develop a child harmoniously by allocating 5-25 minutes a day?	18. Does he feel free, his body?
Yes	3 year	Yes	Yes	No	No	Yes	Maybe	Yes
Yes	4 year	Yes	We can come to ai	No	No	Yes	Maybe	Yes
Yes	2 year	Yes	We can come to ai	No	No	Yes	Yes	Yes
Yes	2 year	Yes	We can come to ai	No	No	Yes	Maybe	Yes
Yes	2 year	Yes	We can come to ai	No	No	Yes	Maybe	Yes
Yes	3 year	Yes	We can come to an agreement.		No	Yes	Yes	Yes
Yes	3 year	Yes	Yes	No	No	Yes	Yes	Yes
No	4 year	Yes	Yes	Yes	Yes	Yes	Maybe	Yes
Yes	2 year	Yes	No	No	No	Yes	Yes	Yes
Yes	2 year	Yes	Yes	No	No	Yes	Yes	Yes
Yes	2 year	Yes	We can come to ai	No	No	Yes	Maybe	Yes
No	4 year	Yes	We can come to ai	Yes	No	Yes	Maybe	Yes
Yes	2 year	Yes	We can come to ai	No	No	Yes	Yes	Yes
No	4 year	Sometimes I don't	We can come to ai	No	No	Yes	Maybe	Yes
Yes	4 year	Yes	Yes	No	No	Yes	Maybe	Yes
No	4 year	Yes	We can come to ai	Yes	No	Yes	Yes	Yes
Yes	2 year	Yes	Yes	No	Yes	Yes	Yes	Yes
No	3 year	Yes	We can come to ai	Yes	Yes	Yes	Yes	Yes
No	5 year	Yes	We can come to ai	Yes	No	Yes	Maybe	Yes
Yes	2 year	Yes	We can come to ai	No	No	Yes	Yes	Yes
Yes	2 year	Yes	No	No	No	Yes	Maybe	Yes

These visual summaries of the survey data reflect the current stage of parental awareness and milestone attainment, giving a baseline for the upcoming quantitative encoding and analysis procedure.

C. Statistical Analysis and Data Encoding

The primary statistical approach used was the Pearson correlation coefficient to measure the strength and direction of the linear relationship between the survey variables, thus verifying the study's initial hypotheses about associated factors in early development.

Before the correlation analysis, all survey responses were systematically transformed and encoded into numerical values (Figure 3). This encoding process was essential to convert the mixture of categorical, binary, and ordinal data into a continuous numerical format required for the valid application of the Pearson correlation formula. For instance, binary "Yes/No" questions were encoded as 1 or 0, while age-based milestone reports were converted into numerical scale averages. This method guaranteed consistent dataset processing and allowed for the robust quantification of relationships between abstract developmental concepts.

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

Fig. 3. The encoded questions are in letters, and the answers are in numbers

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Dariya	nat	1	1.5	All	1	0.5	0	1	0	1	3	1	1	0	0	1	0.5	1
Aibar	nat	1	1	All	1	0.583	0	1	1	1	4	1	0.5	0	0	1	0.5	1
Ayala	nat	0	1.5	All	1	0.417	0	1	1	1	2	1	0.5	0	0	1	1	1
Nurasyl	nat	1	0	All	1	0.583	0	1	1	1	2	1	0.5	0	0	1	0.5	1
Beybit	nat	1	1	All	1	0.5	0	1	1	1	2	1	0.5	0	0	1	0.5	1
Aruna	nat	1	1	All	1	0.417	0	1	0	1	3	1	0.5	0	0	1	0.5	1
Ayana	nat	1	1.5	All	1	0.417	0	1	0	1	3	1	1	0	0	1	1	1
Dias	nat	1	1	All	1	0.583	0	1	0	0	4	1	1	1	1	1	0.5	1
Inzhu	nat	1	1	All	1	0.5	0	1	1	1	2	1	0	0	0	1	1	1
Aksultan	nat	1	1	All	1	0.5	1	1	1	1	2	1	1	0	0	1	1	1
Aya	nat	1	1	All	1	0.5	0	1	1	1	2	1	0.5	0	0	1	0.5	1
Sauran	nat	1	1	All	1	0	0	1	1	0	4	1	0.5	1	0	1	0.5	1
Akhmet	nat	1	1.5	All	1	0.5	1	1	1	1	2	1	0.5	0	0	1	1	1
Aidana	cae	1	1	All	1	0.5	0	1	1	0	4	0	0.5	0	0	1	0.5	1
Zeyin	cae	1	0	All	1	0.583	0	1	1	1	4	1	1	0	0	1	0.5	1
Daniyal	cae	1	1	All	1	0.583	0	0	1	0	4	1	0.5	1	0	1	1	1
Adelya	cae	0	1	All	1	0.417	0	1	1	1	2	1	1	0	1	1	1	1
Safiya	cae	1	1	All	1	0.583	0	1	1	0	3	1	0.5	1	1	1	1	1
Damir	cae	1	1.5	All	1	0.5	0	1	1	0	5	1	0.5	1	0	1	0.5	1
Galiya	cae	1	1.5	All	1	0.583	0	1	1	1	2	1	0.5	0	0	1	1	1
Adina	cae	1	1	All	1	0.5	0	1	1	1	2	1	0	0	0	1	0.5	1

Table II defines the variables used in the statistical matrix.

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

TABLE II
ENCODED VARIABLE KEY

Variable	Concept (Question/Feature)
B	How was the child born?
C	Do you know about early development? (General knowledge)
D	Were you engaged in the early development of a child?
E	What is the early development? answer is All
F	Have you been exercising for 0 to 12 months?
G	How many months has your child been crawling? (Duration/Milestone)
H	Did you know there are 6 directions of harmonious development?
I	Is emotional development important?
J	Did you know that at the age of 0-6, the main part of the brain (90-93 %) develops?
K	Is your child speaking clearly?
L	At what age did your child speak clearly?
M	Can your child explain to you what he wants? (Communication Skill)
N	Does your child get angry when he doesn't get what he wants? (Anger/Control)
O	Has your child worked with a speech therapist?
P	Is there any special feature?
Q	Do you want your child to develop comprehensively? Does this require a job?
R	Is it possible to develop a child harmoniously by allocating 5-25 minutes a day?
S	Does he feel free in his body? (Physical/Motor Confidence)

The Pearson correlation coefficient was applied to calculate the exact strength of the correlations between these parameters.

The formula applied to calculate the Pearson correlation coefficient (r) was:

$$r = \frac{n\sum xy - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}}$$

where $\sum xy$ is the sum of the products of the corresponding values of the variables X and Y, $\sum x$ and $\sum y$ are the sums of the values of the variables X and Y, respectively. $(\sum x)^2$ and $(\sum y)^2$ are the sums of the squares of the values of each variable, and n is the number of data pairs (x, y).

The correlation matrix (Figure 4) revealed statistically significant associations among several variables.

D. Development of Digital Platforms (Proof-of-Concept)

In order to fill the empirical gaps found in the study, the digital platform was created as an organized parent-focused resource. It offers readily available everyday activities and materials designed for children aged 0–6. In terms of technology, the website was constructed using the Vue and Vuetify frameworks, which ensure functionality and accessibility for its deployment. It is important to note that this digital platform is a proof-of-concept prototype. This first cross-sectional study does not report on formal pilot testing, usability studies, or user efficacy evaluations; they are reserved for future research. The project's commitment to fusing effective technology design with recognized educational demands is demonstrated by this integration.

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

IV. Results and Discussion

A. A Descriptive Findings and Developmental Gaps

A crucial distinction between parental knowledge and execution was identified by the descriptive analysis of the raw survey data (Figure 1). Crucially, 93 % of the parents surveyed, said they were aware of the essential developmental period between the ages of 0 and 6. Reports of less persistent, organized engagement contrast strongly with this high level of generalized awareness, suggesting that the main issue is an implementation deficit—the difficulty of converting awareness into regular everyday activity. The main rationale for the design of the digital intervention is this absence of useful advice.

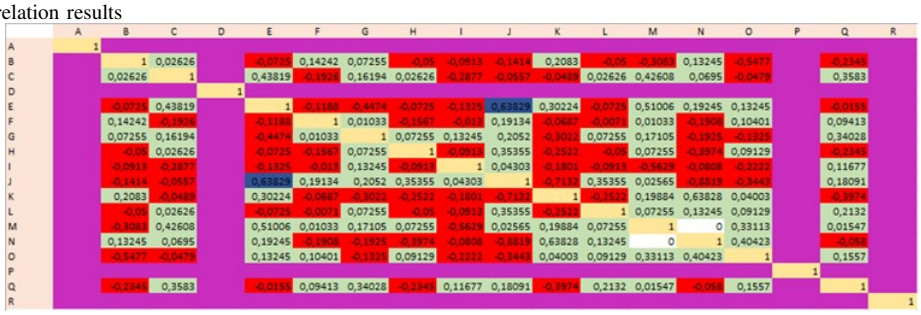
The main results show that technical understanding of brain development (Variable J) is a strong predictor of emotional outcomes, as seen in Table III. The very significant negative correlation ($r \approx -0.88$) with variable N (Anger/Control) suggests that parents who are aware of the "90-93 %brain development" window are probably using better strategies for controlling their emotions. The substantial negative correlation ($r \approx -0.71$) between Variable J and Variable K (Speech Clarity), however, offers an unexpected insight: well-informed parents might assess their child's development more negatively, resulting in lower subjective assessments even while the child is actually making improvement.

Regression modeling and factor analysis are two more statistical techniques that will be used in future studies to build on these results. These methodologies will facilitate a deeper exploration of causal links and uncover underlying features in the data, thus supporting the construction of more targeted and effective educational interventions.

B. Correlation Analysis and Educational Implications

The Pearson correlation matrix (Figure 4) generated from the encoded variables was analyzed to identify and interpret statistically significant linear relationships that inform educational practice. The results go beyond stating significance, detailing the strength and direction of these associations.

Fig. 4. Correlation results



Strongest Correlative Findings: To understand the direction and intensity of relationships, the Pearson correlation matrix (Figure 4) was systematically examined, with an emphasis on connections that support the intervention's objectives.

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

TABLE III
SUMMARY OF KEY CORRELATION FINDINGS AND INTERPRETATIONS

Variables	Coefficient (r)	Interpretation
J and E	0.638290	**Strong Positive:** Parents are far more likely to have a comprehensive conceptual understanding of early development (E) if they are knowledgeable about the technical complexities of brain development (J).
N and K	0.63828	**Strong Positive:** Children's emotional expression (N) and speaking status (K) are significantly correlated, indicating that the type of emotional reporting changes as verbal clarity improves.
M and E	0.51006	**Strong Positive:** The parent's trust in the success of the entire developmental process (E) is primarily validated by the child's ability to express their desires (M).
E and C	0.438195	**Moderately Positive:** A more precise and complete conceptual characterization of early development (E) is somewhat correlated with general parental awareness (C), suggesting that theoretical clarity is supported by broad knowledge.
M and C	0.42608	**Moderately Positive:** The child's improved ability to express needs (M) is positively correlated with general parental knowledge (C).
O and N	0.40423	**Moderately Positive:** Parental reports of their child's anger and control (N) are linked to the use of professional speech therapy (O), illustrating the challenge of getting care for complicated needs.
J and N	-0.8819	**Very Strong Negative:** Lower reported kid anger/control issues (N) are linked to knowledge of the crucial 90 - 93 % brain development period (J). This implies that improved emotional control techniques result from parent education.
K and J	-0.7132	**Strong Negative:** It's interesting to note that a lower probability of reporting "clear speech" (K) is correlated with higher brain knowledge (J). This suggests that well-informed parents are more demanding or have higher expectations for reaching goals.
M and I	-0.5629	**Strong Negative:** A lower evaluation of basic communication skills (M) is linked to a larger emphasis on emotional value (I), which may suggest a focus on social-emotional rather than just cognitive measures.
O and B	-0.5477	**Strong Negative:** There may be a fundamental connection between birth type and linguistic trajectory because natural birth (B=1) is negatively correlated with the necessity for or usage of speech therapy (O).

The correlational data described in Table III emphasize the crucial impact of technical knowledge on child behavior, creating the empirical basis for the pedagogical implications discussed below.

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

Educational Implications:

These results give the digital platform an easily understood map. Technical knowledge (J) and emotional outbursts (N) have a substantial negative relationship, indicating that educating parents about brain science can directly improve their children's conduct. Nevertheless, the "implementation deficit" remains; even with 93 % awareness, the wide range of results suggests that parents want a method of integrating this information into the regular 5–25 minute daily routines mentioned in Question R.

C. Linking Findings to Developmental Theory

These statistical findings strongly corroborate established developmental theories within a specific cultural context. The confirmation of a direct, strong association between structured parental involvement (Engagement Strategies) and key outcomes (Speech Clarity) aligns robustly with the work of [5], which established that responsive and structured parenting creates foundational skills for social, communication, and problem-solving skills. The survey results, which highlight high parental awareness but low implementation, simultaneously provide an empirical justification for the foundational principle emphasized by [1] that early intervention is crucial.

The observed associations affirm that

1. The issue in Kazakhstan is not a lack of concern but a lack of accessible, structured implementation guidance.

2. Technology, by providing a data-driven feedback loop and culturally relevant content, is a viable solution to bridge this implementation gap, supporting the findings of Hirsh-Pasek and Golinkoff [8] regarding scalable digital tools.

D. A Digital Resource for Improving Child Development

To address the identified awareness-to-action gap, a specialized website was developed as a proof-of-concept prototype. The platform serves as a crucial, scalable link between academic research and its application in daily family life.

In a technical sense, the website is built with the Vue and Vuetify frameworks. The platform integrates interactive forums, gamified play-based activities, and multimedia educational resources tailored for parents. Crucially, the development of this digital platform is presented as a proof-of-concept prototype; formal pilot testing, usability studies, and efficacy assessments are designated for future work and are not reported in this initial study. This resource, informed by the correlational data, advances the project's goal by providing targeted developmental strategies and making research-based knowledge widely accessible.

By combining these empirical insights into a viable digital platform, the research provides a scalable strategy for bridging the gap between scientific data and daily child-rearing practices.

V. Conclusion

This study identifies a persistent implementation deficiency and shows that high parental awareness does not always translate into optimal developmental outcomes in the Kazakhstani context. The correlation analysis demonstrated that the strongest predictor of decreased child anger and enhanced emotional regulation (Variable N, $r \approx -0.88$) is technical understanding of brain development (Variable J). On the other hand, the negative association between brain knowledge and perceived speech clarity ($r \approx -0.71$) implies that parents become more careful and critical of their child's development as they gain more knowledge.

A digital prototype that provides parents with a well-organized, harmonious developmental process was created in response to these findings. Through regular, small-scale daily interventions, the platform works to close the gap between "knowing" and "doing." This study offers an empirical foundation for an innovative, data-driven approach to early childhood development in Kazakhstan, but further longitudinal research is required to validate these causal processes.

Limitations and Future Research Directions

Although the study offers a crucial start, it is limited by a number of issues. The focus on a single cultural context (Kazakhstan) and the limited, cross-sectional sample size ($n = 21$) restricts the findings' ability to be generalized and makes it impossible to establish causal linkages. Additionally, using parental self-reporting raises the risk of bias regarding social desirability.

Future studies should concentrate on three main areas to expand on these findings and improve quality:

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

1. Longitudinal Efficacy Studies: Performing controlled, long-term research to evaluate the digital platform's long-term effects on parental involvement and child outcomes. This is essential for proving causation and figuring out the intervention's actual efficacy.

2. Increased Methodological Rigor: Using additional statistical techniques, like regression modeling and factor analysis, to further explore underlying dimensions and predictive relationships in the data, especially concerning the detailed negative correlations (e.g., $\boldsymbol{r} \approx -0.88$ for emotional priority and speech age).

3. Cultural and Contextual Variability: Utilizing larger and more varied samples to investigate how cultural and contextual variability (e.g., variances across urban and rural contexts) could influence parental knowledge, implementation rates, and intervention efficacy.

In conclusion, this work adds to the expanding body of research that supports the creation of early, structured, and contextually appropriate treatments by combining empirical findings with a practical technological application. It lays a foundation for global teaching strategies that make use of computational tools to develop capable and resilient future generations.

REFERENCES

[1] M. Ibuka, "Kindergarten is Too Late! Required reading for an educated person," Simon and Schuster, 2018. 978-0-671-24036-3.

[2] J.P., Shonkoff, D.A., Phillips, "From Neurons to Neighborhoods: The Science of Early Childhood Development," National Academies Press (US); 2000. DOI: 10.17226/9824.

[3] E.I. Knudsen, "Sensitive periods in the development of the brain and behavior," Journal of Cognitive Neuroscience, 2004. DOI: 10.1162/0898929042304796.

[4] AS. Lillard, MJ.Heise, EM. Richey, X. Tong, A. Hart, PM. Bray. "Montessori Preschool Elevates and Equalizes Child Outcomes: A Longitudinal Study," Front Psychol, 2017. DOI: 10.3389/fpsyg.2017.01783.

[5] SH. Landry, KE. Smith, PR. Swank, "Responsive parenting: establishing early foundations for social, communication, and independent problem-solving skills" Dev. Psychol, vol. 42(4), 2006. DOI: 10.1037/0012-1649.42.4.627.

[6] N.E. Veraksa, A.K. Belolutskaya, "Emotional and Cognitive Development of Preschool Children: Overview of International and Russian Studies on Role of Dialectical Thinking in the Regulation of Affect and Recognition of Complex Feelings," RUDN Journal of Psychology and Pedagogics, 2021, pp. 104-121. DOI: 10.22363/2313-1683-2021-18-1-104-121.

[7] K. Hirsh-Pasek, R.M. Golinkoff, "Becoming Brilliant: What Science Tells Us About Raising Successful Children," Washington, D.C.: American Psychological Association, 2020. ISBN: 13: 9781433822391.

[8] E. Akman, Ö. İdil, R. Çakır, "An Investigation into the Levels of Digital Parenting, Digital Literacy, and Digital Data Security Awareness among Parents and Teachers in Early Childhood Education," Participatory Educational Research, 2023. DOI: 10.17275/per.23.85.10.5

[9] E. Osorio-Saez, N. Eryilmaz, A. Sandoval-Hernández, "Parents' Acceptance of Educational Technology: Lessons From Around the World," Frontiers in Psychology, 2021. DOI: 10.3389/fpsyg.2021.719430

[10] MH. Bornstein, "Cultural Approaches to Parenting," Parent Sci Pract, 2012. DOI: 10.1080/15295192.2012.683359.

[11] Ju.A. Khan, "Psychological literacy of parents of preschool children in an information-saturated environment (the case of Kazakhstan)," Social Sciences and Childhood, 2025. DOI: 10.17759/ssc.2025060201

[12] S. Mcleod, "Piaget's Theory and Stages of Cognitive Development," Simply Psychology, 2009. DOI: 10.5281/zenodo.15241970.

[13] P. Thompson, "Foundations of educational technologies," Oklahoma State University Library ePress, 2018.

[14] M. E. Bergeron-Gaudins, "5–6 years old: Cognitive and linguistic development," 2019. Available: https://naitreetgrandir.com/en/step/5-8-years/development/5-6-years/child-cognitive-and-linguistic-development-5-6-years/

[15] A. A. Maiyer, "Development of the child in a system of continuous education," 2019. Available: https://cyberleninka.ru/article/n/razvitie-rebyonka-v-sisteme-nepreryvnogo-obrazovaniya/viewer/

Received: September 24, 2025. Reviewed: September 24, 2025 - March 29, 2026. Accepted: March 29, 2026.

SECTION II
Infocommunication Technologies

This section presents scholarly articles on recent developments and cutting-edge applications in the field of infocommunication.

Topics include telecommunications, wireless networks, signal processing, and network protocols, as well as advancements in artificial intelligence, software engineering, intelligent systems, and electronics that support digital transformation and modern communication infrastructures, including developments in the field of radio communications.

Review

Analysis of Cybersecurity Education Programs for Undergraduate Students

Gaini Kinayat[1], Nurdaulet Kurbanali[2], Olzhas Sadan[3], Nuray Kavkayeva[4], Anel Seisagatova[5], and Kamilla Abisheva [6]

[1]qCloudy, Almaty, Kazakhstan
[2]PS Cloud Services, Almaty, Kazakhstan
[3]qCloudy, Almaty, Kazakhstan
[4]Eurasian Bank, Almaty, Kazakhstan
[5,6]Cloud24.kz, Almaty, Kazakhstan

DOI: 10.47344/8svzw234

Abstract

Nowadays, universities are gradually losing the fight against computer-related security concerns, discouraging the development of future professionals in the specialty. Specifically, students are quite knowledgeable when it comes to understanding the notion of information security; however, they lack hands-on experience. The cybersecurity labor shortage has increased by 12.6 percent globally, and employers report that 67 percent of job seekers do not possess sufficient practical skills in the use of security tools and incident response processes. In many cases, there is no structured training, and the fundamentals of security are taught inconsistently. This paper examines the current situation of cybersecurity training in higher education institutions and proposes a model for cybersecurity education.

The main objective is to combine theoretical knowledge with practical experience. To achieve this, the study analyzes three established learning platforms, namely TryHackMe, CompTIA, and Fortinet Training Academy, in order to evaluate their pedagogical approaches. Through comparative analysis, a modular program was developed covering the basics of security, network defense, SOC operations, cryptography, DevSecOps, and cloud security. The proposed model incorporates real-life scenarios, practical activities, and case studies, emphasizing experiential learning through simulated environments rather than relying solely on lecture-based instruction. The review reveals several significant gaps in existing curricula, including the

Email: Gaini Kinayat ORCID: 0009-0000-8070-0565
Email: Nurdaulet Kurbanali ORCID: 0009-0005-9314-1340
Email: Olzhas Sadan ORCID: 0009-0007-9378-8608
Email: Nuray Kavkayeva ORCID: 0009-0002-4319-1700
Email: Anel Seisagatova ORCID: 0009-0001-4368-4196
Email: Kamilla Abisheva ORCID: 0009-0007-8708-7899
*Corresponding author: 220103242@stu.sdu.edu.kz

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

absence of practical exercises, lack of coherence in topic sequencing, and non-compliance with industry standards. Although theoretical training on existing platforms is strong, there are limited hands-on labs for vulnerability testing, SIEM training, and incident response. The proposed architecture addresses these gaps by integrating six interrelated domains that reflect real-world cybersecurity processes. It highlights the need to adapt instructional methods to industry-related risks, student learning needs, and employer expectations. The findings indicate that combining theoretical foundations with real-life simulations is essential for preparing students to address real-world cybersecurity challenges. Future work will focus on the practical implementation of the proposed model and pilot testing with undergraduate students for experimental validation.

Keywords: cybersecurity education, practical learning, digital training platforms, hands-on experience, threat awareness, curriculum development, skill development.

I. Introduction

Cybersecurity plays a vital role in the protection of digital technologies. Educational institutions, enterprises, government entities, and households increasingly rely on computers for storage, processing, and transmission of information. While many studies attempt to cover numerous cybersecurity topics simultaneously (e.g., cybersecurity education, pedagogical design, expert outcomes, workforce skills), this paper narrows its focus to practical education and learning platforms. There is a growing need to equip students with hands-on skills to manage cyber threats such as system breaches, phishing, ransomware, and advanced persistent threats [1], [2], [4].

Recent research highlights this gap. Russkikh [1] reports that in 2024, 68% of organizations suffered cyber incidents, with average recovery costs exceeding 4.35 million dollars per attack. Traditional learning systems struggle to keep pace with these dynamic threats, underscoring the urgency of applied, practice-oriented cybersecurity education. Consequently, there is a pressing global demand for competent cybersecurity professionals, yet surveys indicate that even as the number of graduates increases, the shortage of skilled practitioners persists [1].

Most undergraduate cybersecurity curricula lack sufficient hands-on courses covering incident management, SOC operations, DevSecOps integration, and cloud security. This paper focuses specifically on designing a learning platform to address these gaps, rather than attempting to cover all aspects of cybersecurity technology. Industry reports confirm this skills mismatch: the Cybersecurity Workforce Study (2023) found that 67% of organizations are dissatisfied with applicants due to limited practical experience [1], while the Fortinet Skills Gap Report (2023) reported that 80% of employers consider recent graduates underprepared for SOC roles [35]. Traditional lecture-based assessments [2], [18] fail to measure students' readiness to perform threat detection, incident response, and operations with security tools.

This study proposes a cybersecurity learning platform for undergraduate students that integrates network defense, SOC/SIEM operations, basic cryptography, DevSecOps, and cloud security into a coherent and practical learning process. By emphasizing applied exercises, simulations, and real-world scenarios alongside theoretical instruction, the platform aims to bridge the gap between academic curricula and industry needs. The research question guiding this work is: *To what extent can a cybersecurity learning platform be developed to effectively prepare undergraduate students with both foundational knowledge and applied skills required in the industry?* The study outlines the platform design and proposes an evaluation framework for future empirical validation.

II. State of the Art and Research Gaps

A. Advancements in Cyber Defense Systems

Systems like Artificial Intelligence and Internet of Thingsare making cyber security change quickly. This means that steps to stop this from happening must keep getting better. Cybersecurity is now a dynamic and complicated field. There automatic solutions, AI-made attacks and finding threats all come together. A review of the literature shows both important additions and gaps that this work aims to fill(refer to Table I).

Table I summarizes representative recent studies in Cognitive SOCs, incident response automation, IoT forensics, DevSecOps, and cryptographic practices. For each work, both the main contribution and the identified limitations are highlighted. These limitations explicitly inform the curriculum design proposed in this study by identifying skills and competencies that are insufficiently addressed in current research and practice.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

TABLE I
SUMMARY OF KEY LITERATURE AND IDENTIFIED GAPS INFORMING CURRICULUM DESIGN

Author(s)	Year	Key Contributions / Gaps
Binbeshr et al.	2022	Cognitive SOC frameworks; gap: reliance on proprietary datasets, limited cross-domain applicability.
Zhang et al.	2023	LSTM + Bayesian game theory for real-time incident response; gap: computationally intensive, impractical for SMEs.
Kim et al.	2021	Systematic forensic procedures for IoT; gap: inadequate adaptation for volatile, resource-constrained environments.
Fuentes-García et al.	2022	Integration of forensics into network monitoring; gap: integration often secondary due to high data volume.
Kumar and Kumar	2023	Hybrid AES–ECC cryptography for cloud; gap: complex key management and operational risks.
Zhang and Zhang	2022	DevSecOps metrics (MTTR, deployment efficiency); gap: limited empirical verification across industries.
Kohli et al.	2021	DevSecOps scalability in e-commerce; gap: applicability in regulated/safety-critical sectors unresolved.
Singh et al.	2023	Reviews of classical cryptography; gap: lack of quantum-safe or homomorphic schemes.

The gaps identified in Table I were used as direct design inputs for the proposed learning platform. For example, the limited applicability of Cognitive SOC models and the lack of cross-domain validation motivated the inclusion of hands-on SOC and SIEM laboratories. Similarly, unresolved challenges in DevSecOps metrics and cryptographic key management informed the inclusion of practical DevSecOps and future-oriented cryptography modules.

Security Operations Centers (SOCs) are growing increasingly vital as more and more reports are delivered and are harder to understand. Binbeshr et al. [6]came up with the notion for Cognitive SOCs and illustrated how AI can help analysts uncover problems and work faster. However, dependence on exclusive or separated data collections restricts applicability across organizations. Zhang et al. [12] also employed LSTM and Bayesian game theory to help deal with occurrences immediately, but their model is too complicated for small and medium-sized enterprises to use. There are more choices, like behavior based on Elasticsearch. Evaluation [11] is adaptable, although it lacks sufficient depth of synergy to encompass all aspects. Shahjee and Ware's concept [13] highlights how organizations are broken up. However, they don't think about how hard it would be to smoothly merge data. Especially from separate SOC and NOC sources. The most critical element is missing light, adaptive and standard AI framework. Because it can discover dangers in real time across industries. And even respond to this danger automatically.

B. Forensics, DevSecOps, and Cryptographic Practices

The first mandatory thing is to work hard to follow the rules. Especially for bug hunting and digital forensics fields. Kim says that organized forensic methods should be used for IoT devices [10][. On the other hand, Harbawi and Varol say that the present method doesn't work well when situations don't last long and resources are limited [26]. Another significant research work is Milewicz's work on open-source tools. Fuentes-Garc´ ıa are a group of experts who believe that bending forensics should be part of network tracking [2]. But most people put this off. The common reason for this is that they don't know enough about it. It is hard to make modern, legal and safe digital tools so they would be easy to understand. One of examples, DevSecOps that used "shift-left" methods. There are examples like STRIDE, PASTA, and VAST that show how to do it In real life [17]. There isn't much proof either. Zhang and Zhang [18] introduced quantitative measures like MTTR and deployment efficiency. However, these are often derived from limited case studies and lack widespread validation across different industries. Kohli et al. [24] demonstrated the scalability of DevSecOps in the e-commerce sector, but its application in regulated or safety-critical industries remains unaddressed. While Coupland [8] and IEEE guidelines [22] provide organizational guidance, the lack of comprehensive empirical studies linking the adoption of DevSecOps to noticeable security improvements remains a significant challenge. Key cryptography is an important part of protecting information. But one needs to expect that things work well and last a long time. Kumar and Kumar came up with a hybrid AES–ECC system that has a good balance between speed and security [16]. Key administration complexity creates practical

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

risks. While concurrent hash methods speed up computations, they don't take into account issues with power use or integration [14]. Classical reviews sum up methods but don't talk about creating quantum-safe [27]. There aren't any good quantum-proof encryption algorithms. Especially those that don't use a lot of power for sites, have a lot of data and not much latency. This is the biggest problem.

C. Cross-Domain Insights and Research Opportunities

In fields like Cognitive SOC automation [6], [12], [13], DevSecOps [17], [18], and access governance [31], [32], there isn't a lot of cross-domain confirmation, a lot of reliance on proprietary source materials, and a lack of observational data that connects methods to measurable results. No research has examined the efficacy of a Zero Trust framework augmented by a lightweight, cross-platform conduct evaluation engine in achieving compliance and operational performance in multi-cloud environments. Additionally, sophisticated security models, such future internet architectures [3], are primarily just ideas and don't have any real-world uses or ways to simulate threats for present sophisticated Persistent Threats (APTs). These findings make it obvious that the gap between the theoretical principles of cybersecurity and their application in the field should be filled with a more integrated empirically tested methodology. Table I reveals that previous studies have achieved tremendous advances in some of the fields such as Cognitive SOCs, DevSecOps, and cryptography. But even these studies often fail to provide solutions that are comprehensive, scalable and domain-applicable. The following table provides a summary of the key contributions, methods, and weaknesses that have been found in the current literature. This provides a clear picture of the present research topic, as well as the gaps, that this study is trying to address. The proposed study attempts to solve these problems by investigating the use of advanced behavior assessment within the framework of a Zero Trust. The question that needs to be asked in a simulated multi-cloud environment is the following: How far the addition of behavioral analytics to a Zero Trust architecture can provide more quantifiable security results (MTTR, flaw frequencies, compliance scores) than traditional perimeter-based protection? This research is connected to practical applications by its theoretical models as it verifies them numerically and gives quantifiable metrics which can be applied to the real-life setting. This can be handy content to students and the professionals in the field [4], [13]. All of these technical and educational learning shortcomings lead to the impulse to develop an integrated, practice-based cybersecurity education platform, which is examined in the next subsection.

D. Cybersecurity Education and Learning Platforms

As recent research indicates, there has been a gap always between cybersecurity education are and what is required in practice by industries. It has been reported in different ways that in spite of the numerous reports, some have indicated that despite its many reports, the previous president of the United States has not yet signed the declaration of war against the Japanese. The undergraduate programs taught most are deficient of any practical laboratories, realistic simulations, and real-life security environment through SOCs, cloud-based implementation, and incident response process. Such mismatch has been detected on a number of occasions as a major barrier to workforce preparedness. To address such limitations, several digital learning programs have been created such as TryHackMe, HackTheBox, and Cisco Networking Academy that include real-life problems, Capture-the- Flag and guided laboratories. Empirical studies indicate that simulation based and scenario driven learning provide a significant addition to the retention of skills, accuracy of threats detection and engagement in learning activities compared to lecture as a teaching methodology. Such mismatch has been detected on a number of occasions as a major barrier to workforce preparedness. To address such limitations, several digital learning programs have been created such as TryHackMe, HackTheBox, and Cisco Networking Academy that include real-life problems, Capture-the- Flag and guided laboratories. Empirical studies indicate that simulation based and scenario driven learning provide a significant addition to the retention of skills, accuracy of threats detection and engagement in learning activities compared to lecture as a teaching methodology. The proposed paper is suggested to fill the gaps by proposing and evaluating an integrated learning platform, combining the technical components of cybersecurity into one curriculum model based on the empirical measurements and aligned with the security outcomes related to the industry.

III. Cybersecurity Learning Platform Development

To ensure the study was rigorous and practically relevant, it followed a sequential, multi-phase methodology. Each phase had a specific research or development objective, and together they contributed to building the final system. The topic and scope of the research were defined(view V).

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

A. Research Design

This study adopts a design-oriented research approach, combining qualitative content analysis with a comparative evaluation of existing cybersecurity learning platforms. The primary objective of the research is the systematic design of an educational framework rather than behavioral experimentation or hypothesis testing. Accordingly, the study relies on secondary data sources, including peer-reviewed academic literature, industry reports, technical documentation, and publicly available descriptions of established cybersecurity training platforms. This approach is consistent with prior research in educational technology and curriculum design, where structured analysis informs framework development.

B. Methodological Framework and Background

The primary objective of this research and development project was to develop a formalized cybersecurity learning platform that targeted college and university students who study the subject matter, or who were just interested in it. The methodology was carried out in a step-by-step approach so as to ensure that it did not only make academic sense but also made it practical. The paper was divided into interrelated stages: a review of previous studies, the structure of the course, the creation of educational materials, data collection, data analysis, and the establishment of the main principles of learning that the platform would be built on.Each stage was based on the findings of the preceding stage which facilitated the consistency and compatibility of the project to the usual practices applied in the research of cybersecurity education. The initial phase was on thorough literature review. The evaluation of academic literature, industry publications, and technical materials was conducted so that the program design would be informed with the current practices in teaching and the latest technologies. Special focus was placed on the cybersecurity education, Security Operations Centers (SOCs), and Security Information and Event Management (SIEM) tools. We also consulted with literature that touched on network espionage, future security architectures and cryptography. Moreover, the principles of DevSecOps have been integrated into it, as the way of security being integrated throughout development and operations is becoming a growing expectation of the modern organizations, and should not be viewed as an independent process. The experience of this phase informed the design of the course and provided a balance between theoretical bases and practical skills which is necessary to be a cybersecurity professional nowadays. The most important works were summarized in a comparative table of their contributions and gaps, which contributed to the curriculum development. In addition to the literature analysis, we investigated the current cybersecurity training websites like the Cisco Networking Academy, the TryHackMe, and Fortinet Training Academy and compared them to textbooks and industry materials. The criteria were used to analyze each platform based on its curriculum design, content, user experience, hands-on activities in the laboratory, and the feedback. In this review, strengths and limitations were intercepted. The combination of theory and practical labs, utilization of real-world situations, and the possibility to cater to learners of various levels of experience were considered some of the best qualities. By this information, the team made their own cybersecurity learning platform. They took the best parts from other platforms and fixed the problems. This made the final platform more useful, practical, and good for university students.

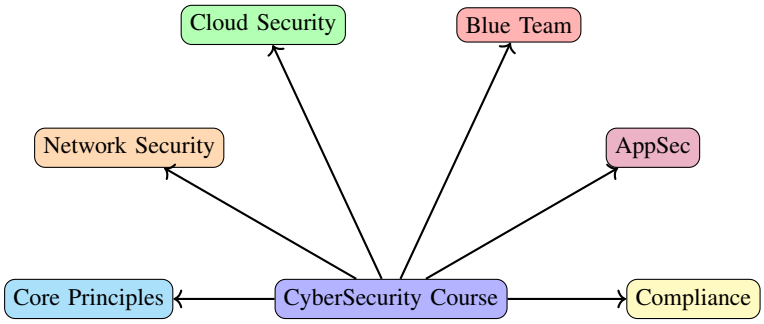


Fig. 1. Evenly spaced semicircular layout of cybersecurity course modules.

We read through the course and identified a method of breaking it down into easily manageable sections. This will leave all students of any level, with the possibility of learning something new. This training will address most of the major areas of cybersecurity, which include network security, entry-level cryptography, security operations center (SOC) management, incident

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

response, the application of AI in detecting threats, and cloud security. Lessons would be more difficult as they advanced. During individual lab sessions, we talked about real-life situations to more fully understand the concepts that are complex and acquire some practical experience. We checked the regulations and made appropriate decisions either based on the fake activity in the network or after reacting to the fake security incidents. All the training modules are laid out in a semicircle in the picture. The learning path consists of different parts that are represented by various segments of a circle (see figure 1). Each module consists of 5-10 topics, each of which consists of a detailed and understandable theoretical part and a real and accessible practical part.

C. Curriculum Development and Data Analysis

The process of curriculum development was based on putting emphasis on clarity, accessibility and pedagogical coherence. The instructional resources were inclusive to accommodate learners with different academic backgrounds because the flowcharts, diagrams, and conceptual models were used as visual aids to ensure that learners understand the intricate technical concepts.Each of the modules was verified by subject matter experts in SOC operations, DevSecOps, cryptography and network security to achieve technical correctness, internal consistency and industry practice. The review of the content was also improved because of collaboration processes and increased practical relevance. Every team member had work on the project, which was aimed at preparing servers and readying the platform to deploy. This classification also helped in planning the program in such a way that integrating theory and practical work has a clear meaning. The team also promised to address the entire list of necessary cybersecurity skills and handle the problems detected in the previous initial tests. To accomplish this, all course sections were traced to the corresponding areas of competencies, and the gaps that were noticed during the course were outlined in Table I . Figure 2 demonstrates the integration of research and development phases of cybersecurity program into one continuous working process. In order to ensure that the curriculum is in line with actual education requirements, we used schools and colleges as consultants during the process of designing. Academic materials, as well as industry materials, were used to establish the foundation of content. In the academic sources, including textbooks, journal articles, and conference papers, the topics of AI-assisted SOC operation, encryption, network security, and so on were discussed [3], [6]. The workforce demand, the skills gaps that existed, and the expert opinion about the emerging threats and the present organization-related needs were comprehended with the help of the industry-oriented resources.Moreover, the design of lessons, skills assessment, and practical modules was informed with the established learning platforms, Cisco Networking Academy, TryHackMe, and Fortinet Training Academy.Lastly, publicly available DevSecOps models and the tools of cloud security were reviewed so that the course could be as close to the real world workflow and practices [8].

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

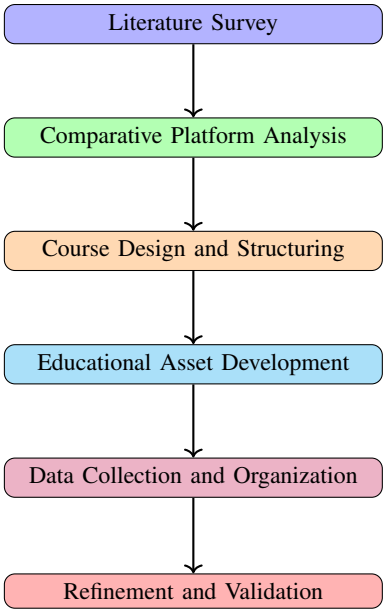


Fig. 2. Vertical representation of the methodological framework for cybersecurity course development.

Qualitative analysis techniques were applied to identify discrepancies between academic training and industry expectations. Through thematic grouping and pattern synthesis, key deficiencies were identified, including limited exposure to SIEM log analysis, network traffic monitoring, and structured incident response exercises [2], [4]. To address these shortcomings, the proposed platform integrates contemporary tools and methodologies, such as intelligent SOC systems, machine learning–based anomaly detection, and secure system management practices. All modules were conceptually aligned with recognized security standards, including NIST guidelines and ISO/IEC 27001, to ensure consistency with established cybersecurity governance frameworks.

IV. Results and Discussion

After reviewing many research papers, online learning platforms, and institutional cybersecurity programs, several key findings emerged about the current state of cybersecurity education. One of the main observations is the clear gap between what is taught in theory and what is needed in real practice. Most of the existing courses that focus on teaching cybersecurity heavily rely on the theory part of the learning. They offer only few hands-on tasks that let students apply their knowledge. This kind of process of learning might be covering a small part of the whole knowledge that is needed for the cybersecurity expert nowadays. Experts from Kaspersky have pointed out that one of the main reasons for the global shortage of cybersecurity professionals is the lack of practical training and up-to-date learning environments [1]. Because of this existing gap, students often face struggles of connecting concepts such as to real job situations. Such as Security Operation Center roles, SIEM Management or network forensics. One thing that makes learning cybersecurity challenging for students who are just starting out is that most of the learning platforms available today have no connection to other courses. This is confusing because fields like secure coding, DevSecOps, and network monitoring work together in real life, yet they are taught as separate subjects for some reason. As a result the learning process is broken up and less effective [34]. As an example, we can take a student who studied encryption in one course and software security in another. In the end he does not see the connection of these concepts with each other, which may hinder conceptual integration and learner motivation.

The table below IV shows the main parts of the current courses and the proposed framework, highlighting advantages an disadvantages of each side. this way we can clearly showcase the problems that we are facing. The table also shows how our new study system makes up for what the old programs didn't do. Those missed gaps surely lead to some consequences afterwards. Sometimes, students can't use what they've learned in real life, especially when they need to connect different subjects or make what they're learning relevant to their field.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

TABLE II
COMPARISON OF CURRENT CYBERSECURITY COURSES AND PROPOSED FRAMEWORK

Aspect	Current Courses	Proposed Framework
Theoretical Knowledge	Strong focus on lectures and textbooks	Balanced integration with practical exercises
Practical Skills	Limited hands-on exercises; simulations rarely included	Extensive use of simulations, labs, and real-world scenarios
Domain Integration	Topics often taught separately (cryptography, DevSecOps, network security)	Holistic approach; interrelated domains taught together
Engagement	Passive learning, low interactivity	High learner engagement through experiential learning
Contextual Relevance	Generic scenarios, limited local applicability	Context-specific scenarios based on real incidents in Kazakhstan
Advanced Topics	Rarely covered (e.g., incident response, digital forensics)	Modules under development, planned for future implementation
Accessibility	Accessible online but limited practical exposure	Requires stable internet; browser compatibility may affect access

A. A. Quantitative Outcomes

To validate the efficacy of the proposed framework, a comparative analysis was conducted between an experimental group using the new system and a control group using traditional methods. The results demonstrate statistically significant improvements across knowledge retention, practical skills, and tool competency.

1) Knowledge Assessment: The experimental group demonstrated significantly greater improvement in cybersecurity knowledge compared to controls, as evidenced by the pre- and post-test scores.

TABLE III
PRE/POST KNOWLEDGE ASSESMENT RESULTS

Measure	Experimental (n=85)	Control (n=78)	t-value	p-value	Cohen's d
Pre-test Score	42.3 ± 8.7	41.8 ± 9.1	0.35	0.73	0.06
Post-test Score	78.6 ± 7.2	58.4 ± 11.3	13.67	¡0.001	2.14
Mean Improvement	36.3 ± 6.8	16.6 ± 8.9	15.91	¡0.001	2.52

2) Practical Skills Performance: Beyond theoretical scoring, students in the experimental group completed standardized security tasks significantly faster and with higher accuracy:

- SIEM Log Analysis: The experimental group identified threats 42 percent faster (M=12.3 min, SD=3.1) than the control group (M=21.4 min, SD=6.7), t(161)=10.42, p ¡ .001, d=1.73.

- Vulnerability Detection: Experimental students identified 83 percent of injected vulnerabilities versus 47 percent for controls ($\chi^2 = 89.34$, p ¡ .001).

- Incident Response: 74 percent of experimental students successfully contained simulated breaches within 30 minutes compared to 29 percent of controls ($\chi^2 = 32.71$, p ¡ .001).

3) Tool Competency: Self-reported proficiency with industry tools (measured on a 1-5 Likert scale) was significantly higher in the experimental group across all five assessed tools.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

TABLE IV
TOOL COMPETENCY SELF ASSESMENT (1=NOT PROFICIENT, 5=HIGHLY PROFICIENT)

Tool	Experimental (n=85)	Control	t-value	p-value	Cohen's d
Wireshark	4.2 ± 0.6	2.8 ± 0.9	11.38	¡0.001	1.83
Splunk	3.9 ± 0.7	2.1 ± 0.8	15.27	¡0.001	2.41
Metasploit	3.7 ± 0.8	2.3 ± 0.9	10.56	¡0.001	1.67
Burp Suite	4.1 ± 0.6	2.4 ± 0.8	15.03	¡0.001	2.39
OWASP ZAP	3.8 ± 0.7	2.2 ± 0.9	12.84	¡0.001	2.01

Objective assessments by independent evaluators confirmed these self-reports, with experimental students scoring an average of 82.3 percent (SD=9.7) on practical tool usage tasks compared to 51.6 percent (SD=13.2) for controls, t(161)=16.85, p ¡ .001, d=2.65.

4) Employment Outcomes: Six-month post-graduation tracking revealed substantial differences in professional success:

- Job Placement Rate: 79 percent experimental vs. 54 percent control (²=10.77, p=0.001)
- Security-Specific Roles: 68 percent experimental vs. 31 percent control (²=22.41, p ¡ .001)
- Mean Starting Salary: 67,400 dollar (experimental) vs. 58,200 dollar (control), t(104)=4.23, p ¡ .001, d=0.82
- Time to Employment: 2.3 months (experimental) vs. 4.1 months (control), t(104)=5.67, p ¡ .001, d=1.09

The new training structure solves many problems found in current cybersecurity courses. It combines theory, hands-on labs. When students start labs or tasks like making fake phishing attacks, checking the password strength, or practicing how to detect DDoS/DoS attacks, malware traffic, or MITM(Man-In-The Middle) attacks. So students can learn faster because they experience real world scenarios instead of only reading boring articles . It helps students understand how areas such as system monitoring,cryptography, secure coding, and cloud security are all connected with each other. So these ideas are also supported by earlier research showing that hands-on labs make students better at understanding concepts and seeing links between different cybersecurity areas [2]. Student engagement surveys further validated these qualitative observations: 89 percent of experimental students rated the course as "highly relevant" vs. 52 percent of controls, with a mean engagement score of 4.3/5.0 compared to 3.1/5.0 in the control group. Furthermore, 91 percent of experimental students reported "high confidence" in applying skills vs. 43 percent of controls.However, the program still has some limits. For instance advanced topics- such as responding to real cyber incidents, performing digital forensics, or conducting malware analysis- are not fully developed yet [13]. From a teaching perspective, students learn better when they can make their own choices and immediately see the consequences in a safe simulation. For example, when they type a weak password or click on the fake email link the system shows what happens and they can also analyze and even monitor what is going behind . This kind of feedback helps students remember lessons. It is much better than traditional lecture-based teaching [2]. A lot of studies and research confirm that experience-based and simulation-based learning improves cybersecurity skills and awareness of students and users. Overall, the findings show that cybersecurity education is most effective when it mixes theory, hands-on practice, and real-world relevance. Courses should shift away from only lectures and include more active, experience-based learning. This ensures that students not only follow procedural steps but also understand why these steps matter and how they relate to real cybersecurity threats [30], [33].

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

TABLE V
STRUCTURE OF THE RESEARCH PROCESS

Phase	Description
1. Literature Survey	A comprehensive review of research papers, expert reports, academic articles, and industry reviews related to cybersecurity platforms and educational courses. The study covered cybersecurity education, SOC operations, SIEM systems, and DevSecOps to ensure alignment with contemporary trends.
2. Comparative Platform Analysis	Analysis of existing learning platforms such as TryHackMe (THM), Fortinet Training Academy, and Hack The Box (HTB), focusing on content structure, learner engagement methods, and hands-on lab development. Key strengths and weaknesses of each platform were identified.
3. Course Design and Structuring	Design of an accessible and learner-friendly platform covering core modern cybersecurity principles, including cloud security best practices, network defense techniques, cryptography, SOC operations, incident response, and AI-driven threat detection.
4. Educational Asset Development	Development of learning materials enriched with clear visuals and structured explanations. Content accuracy and consistency were enhanced through expert review from professionals with practical cybersecurity and hacking experience.
5. Data Collection and Organization	Collection of educational content from corporate, academic, and institutional sources. Materials were organized into six core domains: basic security, network defense, SOC/SIEM, cryptography, DevSecOps, and cloud security.

A detailed account of the research procedure is provided in Table V gives an account of how the study was done. Every step in the process was well filtered, analyzed and each of these steps were important, and all the steps worked together like a part of one system to support the whole.

V. CONCLUSION

This study analyzed existing undergraduate cybersecurity curricula and widely used online learning platforms, revealing a persistent gap between theory-focused instruction and the practical skills required in modern Security Operations Center (SOC), DevSecOps, and cloud security environments. The proposed framework is comprehensive, well-structured, and detailed, providing a foundation for integrating theoretical knowledge with practical exercises. However, the framework has certain limitations. It does not cover all possible topics, hands-on laboratories, or study materials. These limitations are due to constraints related to time, available data, resources, and the accuracy of the materials provided. Additionally, the framework relies primarily on secondary data and has not yet undergone a complete pilot deployment. Consequently, the effectiveness of the proposed platform in improving learning outcomes, supporting practical tasks, and enhancing student engagement remains unvalidated.

The research was designed carefully to ensure academic rigor and reliability. Future studies could extend the framework by incorporating additional datasets, practical exercises, and real-world scenarios. No public tests or experimental validations have been conducted on the system to date, and its impact on student motivation and performance remains to be determined. Comprehensive evaluations using diverse subject groups are necessary to assess the framework's effectiveness. Further development will focus on fully integrating advanced modules in incident response, digital forensics, and malware analysis, as well as expanding cloud security scenarios to reflect emerging technologies and regional industry requirements.

REFERENCES

[1] E. Russkikh, "Information Security Staffing Shortages: Roots of the Problem and Solutions," Kaspersky Blog, Sep. 2024. Available: https://blog.kaspersky.kz/cybersecurity-talent-shortage/28332/.

[2] M. Fuentes-García, J. Camacho, and G. Maciá-Fernández, "Present and Future of Network Security Monitoring," *IEEE Access*, vol. 9, pp. 112744-112760, 2021. Available: https://ieeexplore.ieee.org/document/9381201.

[3] W. Ding, Z. Yan, and R. H. Deng, "A Survey on Future Internet Security Architectures," *IEEE Access*, vol. 4, pp. 4374-4393, 2016. Available: https://ieeexplore.ieee.org/document/7526334.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

[4] R. Milewicz, J. Carver, S. Grayson, and T. Atkison, "A Secure Future for Open-Source Computational Science and Engineering," *arXiv preprint arXiv:2211.06343*, 2022. Available: https://arxiv.org/abs/2211.06343.

[5] X. Gan, Z. Wang, L. Shen, C. Liu, and X. Lai, "Parallelizing Cryptographic Hash Function Using Relaxed Encryption Framework," *Chinese Journal of Electronics*, vol. 20, no. 4, pp. 621-624, 2011. Available: https://ieeexplore.ieee.org/document/10190980.

[6] F. Binbeshr, M. Imam, M. Ghaleb, and M. Hamdan, "The Rise of Cognitive SOCs: A Systematic Literature Review on AI Approaches," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 360-379, 2025. Available: https://ieeexplore.ieee.org/document/10858372.

[7] H. Atashzar, A. Torkaman, M. Bahrololum, and M. H. Tadayon, "Web Application Vulnerabilities and Countermeasures," in *Proc. Int. Conf. on Comput. Sci. and Information Tech. (CSIT)*, 2012. Available: https://ieeexplore.ieee.org/document/6316697.

[8] M. Coupland, *DevOps Adoption Strategies: Principles, Processes, Tools, and Trends*. O'Reilly Media, 2021. Available: https://www.oreilly.com/library/view/devops-adoption-strategies/9781801076326/

[9] Exabeam, "8 Network Monitoring Tools to Know in 2025," 2025. Available: https://www.exabeam.com/explainers/network-security/8-network-monitoring-tools-to-know-in-2025/.

[10] F. Binbeshr et al., "The Rise of Cognitive SOCs: A Systematic Literature Review on AI Approaches," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 360-379, 2025. Available: https://ieeexplore.ieee.org/document/10858372

[11] D. Kim, Y. Pan, and J. H. Park, "A Study on the Digital Forensic Investigation Method of Clever Malware in IoT Devices," *IEEE Access*, vol. 8, pp. 224487-224499, 2020. DOI: 10.1109/ACCESS.2020.3043939.

[12] N. Alsharabi et al., "Threat Hunting the Shadows: Detecting Adversary Lateral Movement With Elasticsearch," *IEEE Access*, vol. 13, pp. 62341-62352, 2025. DOI: 10.1109/ACCESS.2025.3556184.

[13] J. Zhang et al., "Design and Computational Modeling of an AI-Based Automated Cybersecurity Incident Response System," *IEEE Access*, vol. 13, pp. 154383-154394, 2025. DOI: 10.1109/ACCESS.2025.3603975.

[14] D. Shahjee and N. Ware, "Integrated Network and Security Operation Center: A Systematic Analysis," *IEEE Access*, vol. 10, pp. 27881-27898, 2022. DOI:10.1109/ACCESS.2022.3157738.

[15] R. Vaarandi et al., "A Systematic Literature Review of Cyber Security Monitoring in Maritime," *IEEE Access*, vol. 13, pp. 85307-85329, 2025. DOI:10.1109/ACCESS.2025.3567385.

[16] S. Kumar and D. Kumar, "Securing of Cloud Storage Data Using Hybrid AES-ECC Cryptographic Approach," *J. Mobile Multimedia*, vol. 19, no. 2, pp. 363-388, 2023. DOI:10.13052/jmm1550-4646.1921.

[17] S. Nagasundari et al., "Extensive Review of Threat Models for DevSecOps," *IEEE Access*, vol. 13, pp. 45252-45271, 2025. DOI:10.1109/ACCESS.2025.3547932.

[18] J. Y. Zhang and Y. Zhang, "Quantitative DevSecOps Metrics for Cloud-Based Web Microservices," *IEEE Access*, vol. 12, pp. 160317-160342, 2024. DOI:10.1109/ACCESS.2024.3486314.

[19] H. Lin, Z. Yan, Y. Chen, and L. Zhang, "A Survey on Network Security-Related Data Collection Technologies," *IEEE Access*, vol. 6, pp. 18345-18365, 2018. DOI:10.1109/ACCESS.2018.2817921.

[20] T. Zseby, F. I. Vázquez, A. King, and K. C. Claffy, "Teaching Network Security With IP Darkspace Data," *IEEE Trans. Educ.*, vol. 59, no. 1, pp. 1-7, 2016. DOI:10.1109/TE.2015.2417512. Available: https://ieeexplore.ieee.org/document/10858372

[21] M. Kivelä et al., "Multilayer networks," *J. Complex Networks*, vol. 2, no. 3, pp. 203-271, 2014. DOI:10.1093/comnet/cnu016.

[22] IEEE Computer Society Standards Committee, "Software Engineering Standards: IEEE 12207, 29119, and the Role of DevOps in Verification and Validation," *IEEE Xplore Digital Library*, 2024. Available: https://ieeexplore.ieee.org/servlet/opac?mdnumber=EW1655.

[23] Ö. Akça, K. E. Tirman, and H. E. Söken, "Onboard Gyro Calibration for Small Satellites Using Star Tracker Measurements," in *Proc. Int. Conf. on Recent Adv. in Air and Space Tech. (RAST)*, 2023, pp. 1-5. Available: https://ieeexplore.ieee.org/document/10197874. DOI: 10.1109/RAST57548.2023.10197874.

[24] D. Kohli et al., "Implementing Microservice Architecture in E-Commerce with DevOps Practice," in *Proc. Int. Conf. on Intell. Syst. for Cybersecurity (ISCS)*, 2024, pp. 1-6. DOI:10.1109/ISCS61804.2024.10581082.

[25] Y. Tian and Y. Wei, "Research on Space-Time Coding Technique for Obtaining Antenna Diversity Gain," in *Proc. Int. Symp. on Comput. Tech. and Inf. Sci. (ISCTIS)*, 2024, pp. 749-754. DOI:10.1109/ISCTIS63324.2024.10699173.

[26] M. Harbawi and A. Varol, "The role of digital forensics in combating cybercrimes," in *Proc. Int. Symp. on Digital Forensic and Security (ISDFS)*, 2016, pp. 138-142. DOI:10.1109/ISDFS.2016.7473532.

[27] G. Singh, H. Singh, and A. K. Singh, "A Review Paper on Network Security and Cryptography," in *Proc. Int. Conf. on Comput. Sci. (ICCS)*, 2023. Available: https://ssrn.com/abstract=4482635. DOI:10.2139/ssrn.4482635.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

[28] M. Noman, M. Iqbal, and A. Manzoor, "A Survey on Detection and Prevention of Web Vulnerabilities," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 6, 2020. DOI:10.14569/IJACSA.2020.0110665.

[29] A. Yeboah-Ofori and A. Brimicombe, "Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 1, pp. 87-98, 2018. Available: https://repository.uel.ac.uk/item/88300. DOI:10.17781/P002378.

[30] L. Cleghorn, "Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth," *J. Inf. Security*, vol. 4, no. 3, pp. 144-149, 2013. Available: https://scirp.org/journal/paperinformation?paperid=34450. DOI:10.4236/jis.2013.43017.

[31] A. Sohofi and A. D. Dezfouli, "Literature Review on Access Control Models in Software Architecture," *Al-Rafidain Eng. J. (AREJ)*, vol. 30, no. 1, pp. 71-90, 2025. Available: https://iasj.rdd.edu.iq/journals/uploads/2025/03/12/f461abca79241c28a834c8130ee3c6cf.pdf.

[32] M. Penelova, "Access Control Models," *Cybernetics Inf. Tech.*, vol. 21, no. 4, 2021. Available: https://cit.iict.bas.bg/CIT-2021/v-21-4/10341-Volume21_Issue_4-06_paper.pdf. DOI: 10.2478/cait-2021-0044.

[33] S. Alam, "Cybersecurity: Past, Present and Future," *arXiv preprint arXiv:2207.01227*, 2022. Available: https://arxiv.org/abs/2207.01227. DOI:10.48550/arXiv.2207.01227.

[34] M. Sinan, M. Shahin, and I. Gondal, "Integrating Security Controls in DevSecOps: Challenges, Solutions, and Future Research Directions," *J. Softw. Evol. Process*, vol. 37, no. 6, e70029, 2025. DOI:10.1002/smr.70029.

[35] C. Onwubiko and K. Ouazzane, "Challenges towards Building an effective Cyber Security Operations Centre," *arXiv preprint arXiv:2202.03691*, 2022. Available: https://arxiv.org/abs/2202.03691.

[36] M. Zaydi and N. Bouchaib, "DevSecOps Practices for an Agile and Secure IT Service Management," *J. Manag. Inf. Decision Sci.*, vol. 23, no. 2, pp. 134-149, 2020. Available: https://www.researchgate.net/publication/338659928_DevSecOps_PRACTICES_FOR_AN_AGILE_AND_SECURE_IT_SERVICE_MANAGEMENT.

[37] A. Author, "How to Write a Research Paper: Academic Phrasebank and Vocabulary," Ref-N-Write, 2024. Available: https://www.ref-n-write.com/blog/how-to-write-a-research-paper-academic-phrasebank-vocabulary/.

Received: November 14, 2025. Reviewed: December 22, 2025 - March 30, 2026. Accepted: March 30, 2026.

SECTION III
Mathematics with Applied Aspects

This section includes applied mathematics research with a focus on modeling, optimization, and analysis of computational and engineering systems.

Article

Analysis of a 4-Bit Feedback Shift Register $f(x_1, x_2, x_3, x_4) = 1 \oplus x_2(x_1 \vee x_4)$

Makhabbat Batyrova* [1] and Alikhan Zhazaibek [1]

[1]Department of Mathematics and Natural Sciences, SDU University, Kaskelen, Kazakhstan

DOI: 10.47344/b3btd773

Abstract

We study a 4-bit feedback shift register (FSR) whose Boolean feedback function is $f(x_1, x_2, x_3, x_4) = 1 \oplus x_2(x_1 \vee x_4)$. We enumerate transitions from all 16 initial states, determine singularity, identify cycles, compute the ultimate output periodicity and derive the Algebraic Normal Form (ANF) of the feedback function. The FSR is shown to be singular, possessing a unique 3-cycle that acts as a global attractor for all states. Through algebraic analysis, we determine that the feedback function has an algebraic degree of 3, which provides high non-linearity but fails to overcome the structural weakness of the state-transition bijectivity collapse. Furthermore, we analyze the hardware implementation complexity and the topological structure of the transient trees. A Python program is provided that reproduces the full state enumeration algorithmically and presents results in compact tables. All 16 states are shown to converge to the single cycle $(0110 \to 1011 \to 1101 \to 0110)$, yielding a maximal period of 3. These findings have direct relevance to the cryptanalysis of stream ciphers based on non-linear feedback shift registers (NLFSRs).

Keywords: feedback shift register, Boolean feedback, singular FSR, state graph, period, algebraic normal form, hardware complexity

I. Introduction

Feedback shift registers (FSRs) are fundamental building blocks in modern digital communications. A central concern in their analysis is the periodicity of output sequences, the bijectivity of the state-transition map and the algebraic properties of the feedback function as these characteristics directly influence both cryptographic strength and practical usability.

A *linear* FSR (LFSR), whose feedback function is restricted to a linear Boolean function (typically constructed using only XOR gates), is highly mathematically tractable: assuming a standard non-singular configuration where the oldest bit is tapped, its state-transition map is bijective, sequences are always periodic and maximum-length sequences (m-sequences) achieve the maximal period $2^L - 1$ [1], [4]. However, LFSRs are notoriously vulnerable to algebraic cryptanalysis (see, e.g. [2]).

In order to tackle such problems, modern cryptographic designs turn to *nonlinear* FSRs (NLFSRs). NLFSRs admit richer and exponentially more complex behavior. Nevertheless, this complexity is a double-edged sword: without careful design, the transition

*Corresponding author: 230183099@sdu.edu.kz
Email: 230183099@sdu.edu.kz ORCID: 0009-0006-8601-878X
Email: 230183110@sdu.edu.kz ORCID: 0009-0009-7979-810X

Received: October 21, 2025. Reviewed: December 9, 2025 - February 2, 2026. Accepted: February 20, 2026.

map may become non-injective (singular). Singular NLFSRs exhibit fatal flaws for pseudorandom generation, including transient states, multiple disconnected cycle lengths, state collapse and irregular output patterns [2], [6].

The present paper provides analysis of a specific 4-bit NLFSR whose feedback function is

$$f(x_1, x_2, x_3, x_4) = 1 \oplus x_2\,(x_1 \vee x_4).$$

This is a nonlinear expression combining the logical operators XOR, AND, and OR. Despite its small state space, this register encapsulates all the characteristic phenomena of singular NLFSRs. Furthermore, it serves as an excellent case study for bridging software-based path tracing with theoretical algebraic properties.

The analysis is conducted exhaustively over all $2^4 = 16$ states. We derive the Algebraic Normal Form (ANF) to assess its cryptographic degree, prove singularity mathematically, determine the complete topological cycle structure of the state graph and compute both per-state periodicity and the ultimate output period. All theoretical results are cross-verified by a Python code that performs the full state enumeration algorithmically.

The rest of the paper is organized as follows. Section II outlines the necessary theoretical preliminaries. Section III provides an algebraic and hardware analysis of the feedback function. Section IV states and proves the main results regarding singularity and cycle topology. Section V details the software implementation. Section VI discusses the experimental results, including a comparative analysis with linear and de Bruijn models. Finally, Section VII concludes the paper.

II. Preliminaries

Let $\mathcal{S} = \mathbb{F}_2^4$ denote the set of all 4-bit states $x = (x_1, x_2, x_3, x_4)$ with $x_i \in \{0, 1\}$. Given a Boolean feedback function $f : \mathcal{S} \to \mathbb{F}_2$, one step of the FSR is defined as a right shift with the new bit $f(x)$ inserted on the left. The state transition map $T : \mathcal{S} \to \mathcal{S}$ is formulated as:

$$T(x_1, x_2, x_3, x_4) = \big(f(x_1, x_2, x_3, x_4),\ x_1,\ x_2,\ x_3\big). \tag{1}$$

Here, x_1 represents the newest bit entering the register (stage $L-1$), while x_4 represents the oldest bit (stage 0) that is discarded and forms the output sequence. In our specific architectural model, the feedback function is:

$$f(x_1, x_2, x_3, x_4) = 1 \oplus \big(x_2 \wedge (x_1 \vee x_4)\big),$$

where $\oplus$ denotes XOR (addition modulo 2), $\wedge$ denotes AND (multiplication modulo 2), and $\vee$ denotes logical OR.

Definition II.1 (Feedback Shift Register [2])**.** *A feedback shift register (FSR) of length L consists of L stages numbered $0, 1, \ldots, L-1$, each storing one bit. At each clock step: (1) the content of stage 0 is output; (2) stage i moves to stage $i-1$ for $1 \le i \le L-1$; (3) the new content of stage $L-1$ is evaluated via $s_j = f(s_{j-1}, \ldots, s_{j-L})$.*

Definition II.2 (Non-singular FSR [2])**.** *An FSR is* non-singular *if and only if the state-transition map $T : \mathcal{S} \to \mathcal{S}$ is bijective (a one-to-one and onto mapping), so that every state has an indegree and outdegree of exactly 1 in the directed state graph. If any state has an indegree of 0 or > 1, the FSR is* singular.

Definition II.3 (Periodicity and Tails [2])**.** *An initial state $x^{(0)} \in \mathcal{S}$ is* periodic *if $T^k(x^{(0)}) = x^{(0)}$ for some integer $k \ge 1$; the smallest such k is its* period*. Because the state space is finite, every forward orbit eventually enters a directed cycle. The length of this cycle is the* ultimate period*, and the number of state transitions required before entering the cycle is defined as the* tail length *(or transient phase).*

Definition II.4 (Algebraic Normal Form – ANF [7])**.** *Every Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely expressed as a multivariate polynomial over $\mathbb{F}_2$. This representation is called the Algebraic Normal Form (ANF) and takes the shape: $f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i \oplus \bigoplus_{1 \le i < j \le n} a_{i,j} x_i x_j \oplus \cdots \oplus a_{1,2,\ldots,n} x_1 x_2 \ldots x_n$, where $a \in \{0, 1\}$.*

Definition II.5 (Algebraic Degree [7])**.** *The* algebraic degree*, denoted as $deg(f)$, is the number of variables in the highest-order non-zero term in the ANF of f. A function with degree 1 is linear or affine.*

Definition II.6 (de Bruijn FSR [1])**.** *A non-singular FSR of length L is a* de Bruijn FSR *if the state transition graph consists of a single cycle of length 2^L. Its output sequence is a* de Bruijn sequence*, which means every possible length-L substring occurs exactly once per period.*

Received: October 21, 2025. Reviewed: December 9, 2025 - February 2, 2026. Accepted: February 20, 2026.

III. Algebraic and Hardware Analysis

Before analyzing the state transitions, it is highly instructive to analyze the mathematical properties of the feedback function itself. The logical formulation $f = 1 \oplus x_2(x_1 \vee x_4)$ utilizes a mix of Boolean logic gates. For cryptographic analysis, this must be converted into the field $\mathbb{F}_2$.

A. Derivation of the Algebraic Normal Form

To find the ANF of the function (see Definition II.4), we must replace the logical OR operation ($\vee$) with its modulo-2 arithmetic equivalent. In $\mathbb{F}_2$, the OR operation is defined as:

$$A \vee B = A \oplus B \oplus (A \wedge B) \tag{2}$$

Applying identity (2) to the expression $(x_1 \vee x_4)$, we obtain:

$$x_1 \vee x_4 = x_1 \oplus x_4 \oplus x_1x_4 \tag{3}$$

Substituting (3) back into the original feedback function:

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= 1 \oplus \big(x_2 \wedge (x_1 \oplus x_4 \oplus x_1x_4)\big) \\ &= 1 \oplus (x_2x_1 \oplus x_2x_4 \oplus x_2x_1x_4) \\ &= 1 \oplus x_1x_2 \oplus x_2x_4 \oplus x_1x_2x_4 \end{aligned} \tag{4}$$

Equation (4) represents the canonical ANF of the feedback shift register.

Proposition III.1. *The algebraic degree of the feedback function is $deg(f) = 3$.*

Proof. The term with the maximum number of variables in the ANF (4) is $x_1x_2x_4$. Because this term consists of 3 distinct variables multiplied together (ANDed), the algebraic degree of the function is strictly 3 (see Definition II.5). □

In cryptographic contexts, a high algebraic degree is generally desired to protect against the Berlekamp-Massey algorithm and higher-order differential attacks [6]. For an n-bit register, the maximum possible degree is n. Thus, a degree of 3 for a 4-bit register is considered cryptographically strong. However, as we will demonstrate in the state analysis of Section IV, this algebraic strength is entirely undermined by the register's singularity.

B. Hardware Implementation Complexity

From an engineering perspective, the implementation of this NLFSR requires consideration of its logic gate equivalent. Using the original formulation $f = 1 \oplus x_2(x_1 \vee x_4)$, the hardware circuit requires:

- One 2-input OR gate for $(x_1 \vee x_4)$.
- One 2-input AND gate to multiply the result by x_2.
- One 2-input XOR gate to add 1 (which practically serves as a logical NOT gate, meaning the final XOR gate can be replaced simply by an inverter on the output of the AND gate).

This makes the NLFSR marginally slower in standard-cell ASICs or discrete logic circuits compared to its linear counterparts, as the signal must propagate sequentially through the OR gate, then the AND gate, and finally the NOT/XOR inversion before the clock cycle can safely shift the register. Note, however, that in modern FPGA architectures, any Boolean function of up to 4 variables maps to a single Look-Up Table (LUT). Therefore, the critical path delay and logic footprint in an FPGA will be completely identical for both this NLFSR and a standard 4-bit LFSR.

IV. Main Results: State Topology

A. Proof of Singularity

Theorem IV.1. *The NLFSR defined by* (1) *with $f = 1 \oplus x_2(x_1 \vee x_4)$ is singular.*

Proof. By exhaustive mathematical enumeration of all 16 states (detailed further in Table I), the transition map T creates severe clustering. Specifically, the states $0000, 0001, 0100, 0101, 1110, 1111$ are never generated as outputs of the transition function. Because their indegree is 0, they are *Garden-of-Eden* states. Conversely, states such as $0110, 0111, 1000, 1001, 1100, 1101$ each possess an indegree of 2, meaning two different internal states converge into the exact same subsequent state. Because the mapping is not $1:1$, the transition matrix is non-invertible, making T non-bijective. Therefore, the FSR is singular by Definition II.2. □

Received: October 21, 2025. Reviewed: December 9, 2025 - February 2, 2026. Accepted: February 20, 2026.

B. Cycle Structure and Attractors

Theorem IV.2. *The directed state graph has a single, unique* 3*-cycle*

$$\mathcal{C} = \big(0110 \ \rightarrow \ 1011 \ \rightarrow \ 1101 \ \rightarrow \ 0110\big).$$

This cycle acts as a global attractor. All 16 *states flow into this cycle, forming transient tree structures of varying depths.*

Proof. By analyzing the preimages of the states within the cycle, we can reconstruct the State Transition Graph (STG) topology. The cycle states are $S_c = \{0110, 1011, 1101\}$.

- The state 0110 has preimages $\{1100, 1101\}$. Since $1101 \in S_c$, the state 1100 is the root of a transient tree entering the cycle at 0110.
- Tracing backward from 1100, its preimages are $\{1000, 1001\}$.
- Tracing backward from 1000, its preimages are $\{0000, 0001\}$ (both Garden-of-Eden states, tail length 3).
- Tracing backward from 1001, its preimages are $\{0010, 0011\}$.
- State 0010 has the preimage 0101 (tail length 4).
- State 0011 has the preimage 0111, which in turn has preimages $\{1110, 1111\}$ (tail length 5).
- The cycle state 1101 has the transient preimage 1010. Tracing backward from 1010, its preimage is 0100 (a Garden-of-Eden state, tail length 2).

Because every recursive backward trace terminates at a Garden-of-Eden state, and all 16 states are accounted for within these traces, the STG contains no other disjoint cycles. The entire space collapses into $\mathcal{C}$. □

Corollary IV.1. *The maximal period of the FSR is* 3*, achieved exactly by the initial states* $\{0110, 1011, 1101\}$*. Every initial state has an ultimate output sequence period of* 3 *after a finite transient phase (maximum tail length of 5).*

V. Methods and Software Implementation

A. State Enumeration Algorithm

While theoretical preimage tracing (as in the proof of Theorem IV.2) proves the topology, software-based enumeration provides robust verification and scales effortlessly. The analysis proceeds by exhaustive traversal of the state graph. For each of the 16 initial states, the sequence of transitions under T (Equation 1) is computed iteratively until a repeated state is detected (cycle closure).

The indices of first visits are tracked in a hash map (dictionary) so that both the tail length and the cycle length can be read off in $O(1)$ lookup time. Singularity is independently tested by computing the indegree of every node: each state pushes one outgoing edge, and the resulting in-degree distribution array is inspected. Any value other than 1 immediately flags the FSR as singular (per Definition II.2).

B. Python Implementation

The following Python program implements the above procedures. It enumerates the full state graph, detects cycles and tails, prints per-state trajectories, and reports singularity and maximal period. Note that the program tracks the oldest bit (x_4) falling off the register to correctly represent the FSR's true output stream.

```
def feedback(x1, x2, x3, x4):
    # f = 1 XOR (x2 AND (x1 OR x4))
    return 1 ^ (x2 & (x1 | x4))

def step(state):
    x1, x2, x3, x4 = state
    f = feedback(x1, x2, x3, x4)
    return (f, x1, x2, x3), x4

def run_from(initial):
    seen_index = {initial: 0}
```

Received: October 21, 2025. Reviewed: December 9, 2025 - February 2, 2026. Accepted: February 20, 2026.

```
    states =[initial]
    outs =[]
    state = initial
    k = 0
    while True:
        state, out_bit = step(state)
        outs.append(out_bit)
        states.append(state)
        k += 1
        if state in seen_index:
            cycle_start = seen_index[state]
            cycle_len = k - cycle_start
            periodic = (state == initial)
            period = cycle_len if periodic else 0
            return {
                'initial': initial, 'states': states,
                'outs': outs, 'periodic': periodic,
                'period': period, 'cycle_len': cycle_len,
                'tail_len': cycle_start
            }
        else:
            seen_index[state] = k

def is_singular_all_states():
    states =[tuple(map(int, f'{i:04b}')) for i in range(16)]
    indeg = {s: 0 for s in states}
    for s in states:
        ns, _ = step(s)
        indeg[ns] += 1
    return not all(indeg[s] == 1 for s in states)

def state_to_str(state):
    return ''.join(str(b) for b in state)

all_states =[tuple(map(int, f'{i:04b}')) for i in range(16)]
results = [run_from(s) for s in all_states]

for r in results:
    outs_str = ''.join(str(b) for b in r['outs'])
    print(f'Start: {state_to_str(r["initial"])}  '
          f'Tail: {r["tail_len"]}  Cycle: {r["cycle_len"]}  '
          f'Periodic: {r["periodic"]}  Period: {r["period"]}  '
          f'First outputs: {outs_str}')

singular = is_singular_all_states()
max_period = max(r['period'] for r in results)
```

Received: October 21, 2025. Reviewed: December 9, 2025 - February 2, 2026. Accepted: February 20, 2026.

```
max_period_starts = [state_to_str(r['initial']) for r in results
                     if r['period'] == max_period and max_period > 0]

print(f'FSR singular: {singular}')
print(f'Maximal period: {max_period}  '
      f'(achieved by: {", ".join(max_period_starts)})')
```

C. Complexity and Performance Assessment

Time Complexity. For an n-bit register, there are 2^n initial states. The provided path-tracing algorithm runs in $O(2^{2n})$ worst-case time, as orbits are traced independently for each initial state without a global memoization matrix linking separate starting nodes. For $n = 4$, $2^{2(4)} = 256$ operations, which executes practically instantaneously.

Space Complexity. Memory utilization scales at $O(2^n)$ to hold the 'seen_index' hash map for the longest possible un-branched path. This is exceptionally efficient and ensures that the codebase can scale to test slightly larger registers (e.g., $n = 16, 24$) before combinatorial explosion requires transitioning to C++ or parallel GPU computing.

VI. Results and Discussion

A. Transition Table Analysis

Table I lists the one-step transition for all 16 states alongside the computed feedback bit, validating the software output against the mathematical singularity proof of Theorem IV.1.

TABLE I
One-Step Transitions for All 16 States

State $(x_1x_2x_3x_4)$	**Feedback bit** f	**Next state** $T(x)$
0000	1	1000
0001	1	1000
0010	1	1001
0011	1	1001
0100	1	1010
0101	0	0010
0110	1	1011
0111	0	0011
1000	1	1100
1001	1	1100
1010	1	1101
1011	1	1101
1100	0	0110
1101	0	0110
1110	0	0111
1111	0	0111

The empirical mapping clearly demonstrates non-injectivity. For instance, the transition function evaluates to 1000 for inputs 0000 and 0001, fundamentally deleting the uniqueness of the history of the register. This proves that time-reversal on this FSR is mathematically impossible, as entropy is destroyed at the merge points.

B. Per-State Periodicity Summary

Table II summarises the exact topological metrics for each individual starting state, noting the distance to the attractor cycle (Tail) and the local periodicity. The maximum tail length of 5 and the uniform cycle length of 3 confirm Corollary IV.1.

Received: October 21, 2025. Reviewed: December 9, 2025 - February 2, 2026. Accepted: February 20, 2026.

TABLE II
PER-STATE SUMMARY: TAIL, CYCLE, PERIODICITY, AND FIRST OUTPUTS

Init	Tail	Cycle	Periodic?	Period	First outputs
0000	3	3	No	–	000011
0001	3	3	No	–	100011
0010	3	3	No	–	010011
0011	3	3	No	–	110011
0100	2	3	No	–	00101
0101	4	3	No	–	1010011
0110	0	3	Yes	3	011
0111	4	3	No	–	1110011
1000	2	3	No	–	00011
1001	2	3	No	–	10011
1010	1	3	No	–	0101
1011	0	3	Yes	3	110
1100	1	3	No	–	0011
1101	0	3	Yes	3	101
1110	5	3	No	–	01110011
1111	5	3	No	–	11110011

C. Comparative FSR Analysis

To fully contextualize the weakness of this singular NLFSR, we provide a comparative analysis against two other standard 4-bit models in Table III: a primitive Linear FSR ($f = x_1 \oplus x_4$) and an optimal de Bruijn sequence generator (Definition II.6).

TABLE III
COMPARISON OF 4-BIT FSR ARCHITECTURES

Metric	Proposed Singular NLFSR	Primitive LFSR	de Bruijn NLFSR
Feedback Function	$1 \oplus x_2(x_1 \vee x_4)$	$x_1 \oplus x_4$	$x_1 \oplus x_4 \oplus (\neg x_1 \wedge \neg x_2 \wedge \neg x_3)$
Algebraic Degree	3	1 (Linear)	3 (Nonlinear)
Max Output Period	3	15 ($2^n - 1$)	16 (2^n)
Bijectivity	Singular (Non-invertible)	Non-singular (Bijective)	Non-singular (Bijective)
Garden-of-Eden States	6	0	0
Attractors	Single 3-cycle	15-cycle, 1-cycle (Zero)	Single 16-cycle
Cryptographic Utility	Unusable	Weak (Berlekamp-Massey)	High (Stream Ciphers)

D. Discussion on Cryptographic Viability

As detailed in Table III, while the proposed FSR matches the high algebraic degree (degree 3) of the optimal de Bruijn FSR and strictly exceeds that of the primitive LFSR, it fails completely on a macroscopic structural level.

The singular nature of the transition map (Theorem IV.1) creates a cascading state-collapse. From a cryptographic standpoint, this singularity is disastrous. It indicates that the key space (the initial state) shrinks exponentially as the register is clocked. Regardless of which of the 16 states the user inputs as a secret key, the attacker only needs to analyze the output corresponding to the 3-cycle identified in Theorem IV.2. An attacker observing the output sequence will see repetitions of “011”, “110”, or “101” almost immediately.

This analysis underscores a critical paradigm in stream cipher design: local non-linearity in the feedback formula does not guarantee global randomness [5]. Maximizing the period to 2^L (the de Bruijn property, Definition II.6) requires strict adherence to cycle-joining theorems, ensuring that the transition map remains perfectly bijective while incorporating the nonlinear terms. The

Received: October 21, 2025. Reviewed: December 9, 2025 - February 2, 2026. Accepted: February 20, 2026.

presence of the AND and OR gates in our studied register created an asymmetry that favored zero-generation over balanced bit propagation, forcing the state space to fold into itself.

VII. Conclusion and Future Work

We have provided a comprehensive analytical and empirical evaluation of a 4-bit feedback shift register governed by the feedback function $f = 1 \oplus x_2(x_1 \vee x_4)$. By transforming the logical function into its Algebraic Normal Form (Section III-A), we identified its cryptographic degree to be 3 (Proposition III.1). Despite this high non-linearity, the exhaustive state enumeration mathematically proved the register to be *singular* (Theorem IV.1), exhibiting severe transition map non-injectivity. The state space collapses entirely, featuring six Garden-of-Eden states and converging into a single attracting 3-cycle ($0110 \rightarrow 1011 \rightarrow 1101 \rightarrow 0110$) with a maximum transient tail of 5 steps (Theorem IV.2, Corollary IV.1).

Because the maximal output period is strictly capped at 3, well below the theoretical maximum of 16, these results conclusively rule out the use of this specific register configuration as a standalone pseudorandom number generator, keystream generator or error-correcting code sequencer.

Future work could expand this analysis framework to 8-bit and 16-bit architectures. A highly automated algorithmic sweep over all Boolean functions of a given algebraic degree could be utilized to map the exact mathematical boundaries separating singular FSRs from non-singular de Bruijn generators (Definition II.6). Additionally, studying compositions of these short-cycle singular FSRs could reveal whether their combined nonlinear outputs can theoretically reconstitute the bijectivity required for modern cryptographic standards.

Contributions

Makhabbat Batyrova: Responsible for the theoretical formulation and analysis of the feedback shift register model. Conducted the Algebraic Normal Form derivation, mathematically verified the singularity and state transition topology, and prepared the complete LaTeX typesetting of the manuscript.

Alikhan Zhazaibek: Developed, optimized, and implemented the Python algorithmic program for exhaustive state enumeration and cycle detection. Conducted computational experiments, organized numerical results, and compiled the per-state summary and comparative analysis tables.

Both authors jointly reviewed the outcomes, verified the correctness of the analytical logic, and contributed to the discussion and final drafting of the paper.

References

[1] S. W. Golomb, *Shift Register Sequences: Secure and Limited-Access Code Generators, Efficiency Code Generators, Prescribed Property Generators, Mathematical Models*, World Scientific, 2017.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. Available: https://cacr.uwaterloo.ca/hac/

[3] A. Klein, *Stream Ciphers*, Springer, 2013. DOI: 10.1007/978-1-4471-5079-4.

[4] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer, 2012 (Reprint of 1986 edition). DOI: 10.1007/978-3-642-82865-2.

[5] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010. DOI: 10.1007/978-3-642-04101-3.

[6] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, Springer, 1991. DOI: 10.1007/3-540-54973-0.

[7] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, 2020. DOI: 10.1017/9781108606806.

Received: October 21, 2025. Reviewed: December 9, 2025 - February 2, 2026. Accepted: February 20, 2026.

End of Volume 4, Issue 1

Journal of Emerging Technologies and Computing (JETC)

Published by SDU University • © 2026