IRSTI 81.93.29 **https://doi.org/10.58805/kazutb.v.2.31-1562**

HYBRID MODEL OF MULTI-FACTOR AUTHENTICATION BASED ON DETERMINISTIC AUTOMATA AND STREAM CIPHERING

[1]A.A. Kulzhanova, [2]V.A. Zhmud

[1]al-Farabi Kazakh National University, Almaty, Kazakhstan,
[2]Novosibirsk State Technical University, Novosibirsk, Russia

Correspondent-author: e-mail: akbota.kulzhanova1594@gmail.com

In this paper, proposed a hybrid multi-factor authentication (MFA) method to secure and enhance performance in resource-constrained environments, such as IoT and embedded devices. The strategy combines deterministic finite automata (DFA) for formal state-based control of authentication, chaotic key generation based on the Lorenz dynamical system, and the ChaCha20 stream cipher for lightweight encryption. In research, security threats are rapidly increasing with distributed deployments, and traditional MFA models, which often lack formal verification mechanisms and impose computationally heavy complexities, are inadequate. The proposed model overcomes these limitations by introducing a deterministic authentication flow, ensuring strict state transitions and resistance to replay attacks. This approach deals with formally modeling the authentication mechanism via DFA, numerically simulating Lorenz to compute cryptographic key generation for, and implementing ChaCha20. Experimental results confirm the proposed solution provides an extremely low execution time and faster throughput than the AES-based approach, thus is suitable for low-power devices. Furthermore, chaotic systems improve entropy and provide robustness to brute-force attacks. This research confirms that this hybrid model balances security, computing efficiency, and formal verification requirements. This method is promising for IoT, mobile authentication, and distributed secure systems.

Keywords: multi-factor authentication, deterministic finite automaton, ChaCha20, Lorenz system, IoT security, stream cipher.

ДЕТЕРМИНДЕЛГЕН АВТОМАТТАР ЖӘНЕ АҒЫНДЫҚ ШИФРЛАУ НЕГІЗІНДЕГІ КӨПФАКТОРЛЫ АУТЕНТИФИКАЦИЯНЫҢ ГИБРИДТІ МОДЕЛІ

[1]А.А. Кульжанова, [2]В.А. Жмудь

[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан,
[2]Новосибирск мемлекеттік техникалық университеті, Новосибирск, Ресей,
e-mail: akbota.kulzhanova1594@gmail.com

Бұл мақалада ресурстары шектеулі ортада, мысалы, IoT және интеграцияланған құрылғыларда қауіпсіздік пен өнімділікті арттыру үшін гибридті көпфакторлы аутентификация (MFA) әдісі ұсынылады. Стратегия аутентификацияның формалды күй негізіндегі бақылау үшін детерминдік шекті автоматтарды (DFA) біріктіреді, Лоренц динамикалық жүйесіне негізделген хаотикалық кілт генерациясын және жеңіл шифрлеу үшін ChaCha20 ағын шифрын қолданады. Зерттеулерде қауіпсіздік қаупі тарату орындары көбейген сайын тез артуда, ал дәстүрлі MFA модельдері көбінесе формалды тексеру механизмдерінен жетіспейді және есептеу ауырлығымен күрделі болады, бұл оларды жеткіліксіз етеді. Ұсынылған модель аутентификацияның детерминдік ағынын енгізу арқылы осы шектеулерді жеңеді, қатаң күй ауысуларын және қайта ойнату шабуылдарына қарсы төзімділікті қамтамасыз етеді. Бұл тәсіл аутентификация механизмін DFA арқылы формалды моделдеуді, криптографиялық аутентификация үшін криптографиялық кілт генерациясын есептеу үшін Лоренцті сандық түрде модельдеуді және ChaCha20-ны жүзеге асыруды қамтиды. Эксперименттік нәтижелер ұсынылған шешімнің AES негізіндегі тәсілмен салыстырғанда орындалу уақытының едәуір төмен және өткізу қабілетінің жылдамырақ екенін көрсетеді, бұл оны төмен қуатты

құрылғыларға жарамды етеді. Бұдан басқа, хаотикалық жүйелер энтропияны арттырып, brute-force шабуылдарына қарсы төзімділік береді. Бұл зерттеу осы гибридтік модельдің қауіпсіздік, есептеу тиімділігі және формалды тексеру талаптарын теңестіретінін растайды. Бұл әдіс IoT, мобильді аутентификация және таратылған қауіпсіз жүйелер үшін перспективалы.

Түйін сөздер: көпфакторлы аутентификация, детерминирленген ақырлы автомат, ChaCha20, Лоренц жүйесі, IoT қауіпсіздігі, ағындық шифр.

ГИБРИДНАЯ МОДЕЛЬ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ДЕТЕРМИНИРОВАННЫХ АВТОМАТОВ И ПОТОКОВОГО ШИФРОВАНИЯ

[1]А.А. Кульжанова✉, [2]В.А. Жмудь

[1]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан,
[2]Новосибирский государственный технический университет, Новосибирск, Россия,
e-mail: akbota.kulzhanova1594@gmail.com

В данной работе мы предлагаем гибридный метод многофакторной аутентификации (MFA) для обеспечения безопасности и повышения производительности в ресурсно ограниченных средах, таких как IoT и встроенные устройства. Стратегия сочетает детерминированные конечные автоматы (DFA) для формального управления аутентификацией на основе состояний, хаотическую генерацию ключей на основе динамической системы Лоренца и шифр потока ChaCha20 для легкого шифрования. В исследованиях угрозы безопасности быстро растут с распределенными развертываниями, и традиционные модели MFA, которые часто страдают от недостатка формальных механизмов верификации и накладывают вычислительно тяжелые сложности, оказываются недостаточными. Предложенная модель преодолевает эти ограничения, вводя детерминированный поток аутентификации, обеспечивая строгие переходы состояний и устойчивость к атакам воспроизведения. Подход включает формальное моделирование механизма аутентификации через DFA, численное моделирование Лоренца для вычисления генерации криптографических ключей для криптографической аутентификации и реализацию ChaCha20. Экспериментальные результаты показывают, что предложенное решение приводит к значительно меньшему времени выполнения и более высокой пропускной способности по сравнению с подходом на основе AES, что делает его подходящим для маломощных устройств. Более того, хаотические системы увеличивают энтропию и обеспечивают устойчивость к атакам грубой силы. Это исследование подтверждает, что данная гибридная модель балансирует безопасность, вычислительную эффективность и требования формальной верификации. Этот метод является многообещающим для IoT, мобильной аутентификации и распределенных защищенных систем.

Ключевые слова: многофакторная аутентификация, детерминированный конечный автомат, ChaCha20, система Лоренца, безопасность IoT, потоковый шифр.

Introduction. The rise of the digital era and the proliferation of Internet of Things (IoT) systems mean that information infrastructures have been revolutionized today. Smart equipment, embedded systems, and distributed networks are already part of the industrial, medical, and consumer environment. However, all this technological advance is also bringing about great expansion of cybersecurity threats, the most relevant in authentication systems that are the point of defense against unauthorized hacking. Multi-factor authentication (MFA) is established as a common method to improve security by integrating several separate checklists (e.g., knowledge, token, identity) [1].

Modern MFA systems, despite their popularity, suffer from a number of serious problems. For one, most current solutions depend on a static authentication workflow and have weak adaptive features or are susceptible to replay attacks. Second, no existing implementations are capable

of providing formal models for authentication correctness verification systems, therefore, system reliability under adversarial scenarios is difficult to guarantee. Third, commonly implemented cryptographic techniques, such as the Advanced Encryption Standard (AES), may impose an undue computational burden, which restricts their implementation in resource-limited environments [2].

These constraints are especially pronounced in IoT systems, where devices typically meet the strictest limitations in processing strength, memory and energy consumption. In such scenarios it becomes necessary to develop authentication mechanisms not only secure but also lightweight and scalable, and verifiable in formal terms [3].

To deal with the above issues, this paper proposes a hybrid Multi-Factor Authentication Model that introduces deterministic finite automata (DFA), chaotic key generation by using the Lorenz system and ChaCha20 stream cipher. A key concept of this approach is to formalize authentication as a deterministic state machine, ensuring strict control over the sequence of authentication action. The approach allows for fine-tuning authentication logic and removing uncertainty in verification in authentication mechanisms [4].

The application of deterministic finite automata provides a neat method to model authentication state modeling through mathematically based and orderly control mechanisms. The authentication factors are connected to a particular transition process in the automaton, and any change that does not occur in the expected path of process means instant rejection. This method not only improves security but also supplies a conceptual basis to consider the behavior in a system [5].

The model uses the stream cipher for encryption, ChaCha20, as it is efficient and can be implemented as a program. This is because ChaCha20 is less expensive compared to traditional block ciphers and it’ s faster and better in response time, which proves attractive for an IoT and embedded system implementation [6].

The union of these components leaves us with a single authentication architecture to integrate formal verification, robustness and computational cost. Instead of the traditional MFA systems, the proposed model guarantees deterministic authentication flow, minimizes the replay attacks via state-enforcement, and minimizes the computational burden. To address the shortcomings on the current MFA systems, this paper presents a hybrid approach to authentication which combines deterministic finite automata (DFA), Lorenz-style chaotic key generation and ChaCha20 stream cipher.

The primary contribution of the proposed method is to abstract the entire authentication process to a deterministic state-transition process, which keeps control over the execution of authentication, and avoids vagueness in the verification logic. This leads to inherent defenses against replay attacks and provides better overall performance for the authentication mechanism.

Moreover, the model includes chaotic key generation for stronger cryptographic robustness by the high entropy and initial-condition sensitivity. In this respect, the ChaCha20 stream cipher is computationally efficient, enabling the solution to be suitable in resource-constrained environments such as IoT and embedded systems. Security and performance of the proposed framework are verified with stronger advantages from conventional AES based solutions along with a strong approach to traditional attack vectors. This creates an ideal-balanced framework, combining both formal approaches and lightweight cryptography which is both theory-based and practically relevant.

Materials and Methods. The proliferation of distributed computing systems, cloud infrastructures, and, in general, IoT environments has enormously expanded connected devices and the amount of data transmitted. They are prevalent in applications such as healthcare, industrial automation, smart cities, and financial technologies. Nevertheless, the increase in size of such infrastructures has also resulted in a corresponding increase of cyber-threats with authentication systems emerging as one of the most

common targets of attacks [7].

Multi-factor authentication (MFA) has become an important improvement for system security by making several independent verification criteria including knowledge, possession, and biometric components. While most traditional MFA methods are convenient and efficient, we know of limitations. A main problem is the lack of formal verification mechanisms, complicating the assurance of correct and consistent authentication processes under the various operational scenarios. Authentication logic is defined procedurally and not formally in many implementations, and can therefore lead to potential system behavior vulnerabilities [8].

Yet another disadvantage is the susceptibility common to mainstream MFA systems to replay attacks. In a replay attack the adversary intercepts valid authentication data to obtain unauthorized access. In distributed or asynchronous environments, the current work is time-based or token-based, which provides no strong safeguards. However, the absence of rigorous authentication step ordering can lead to vulnerabilities in protocol design [9].

There is the issue that the computational efficiency of the system is less than acceptable, especially in resources where such networks are limited as in IoT devices, embedded systems and mobile platforms. Conventional cryptographic algorithms with high processing and energy overhead are typically used, e.g. block ciphers used everywhere. This limits their practicality into low-power devices, where performance and energy saving can prove crucial [10].

In the face of these challenges, it is apparent that authentication models should strike high security and a low computational cost, while affording formal guarantees of correctness. This study seeks to fill this gap by proposing a hybrid multi-factor authentication model that provides deterministic finite automata (DFA), chaotic key generation, and lightweight encryption.

The implementation of deterministic finite automata represents modeling of the authentication process as a formal state-transition system, which ensures a stricter control over the authentication stages of the sequence of steps to be done. This allows to remove ambiguity in the authentication logic and allow to be resilient against replay attacks through not using invalid state transitions. Simultaneously, through the introduction of chaotic key generation on nonlinear dynamical systems, the entropy and unpredictability of the cryptographic process are brought in and they become stronger than brute force, especially from statistical attacks [11].

Furthermore, the lightweight stream cipher encryption enables the proposed model to retain its computational feasibility and is more suitable for use in low-resource scenarios. These elements are merged to create a single architecture solution that tackles the security as well as performance issue.

Accordingly, the research problem posed in this study is to construct a secure, efficient, and formally verifiable MFA model to support modern distributed and low-resource systems.

System Architecture. The proposed system is deployed on a distributed architecture comprising authentication logic, cryptographic processing, and verification, with the overall architecture of this application as well and illustrated in Figure 1.

This is a distributed architecture system, meaning there are many integrated modules that are implemented as a part of one large system to provide secure authentication processing.

The process starts with the User Device, which collects user authentication factors (password, biometric). Inputs are sent to the Secure Enclave (TEE) that keeps the sensitive processing area in isolation, thereby preventing compromise to sensitive data.

In the secured environment, authentication logic is processed by the DFA Authentication Module which takes a deterministic finite automaton approach for verifying steps. It guarantees authentication factors are not executed in an arbitrary order and that the transitions are not erroneous.

Once those state transitions are completed successfully, the system utilizes the Lorenz Key

Generator to generate a cryptographic key with chaotic dynamics. The key produced is then executed again to the ChaCha20 Encryption Module and authentication data (such as a one-time password) is encrypted.

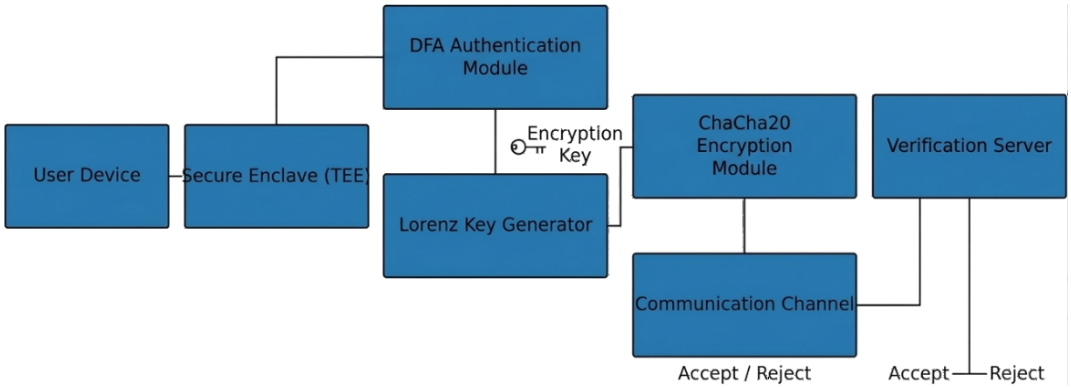


Fig.1 - General Architecture of the Proposed MFA System

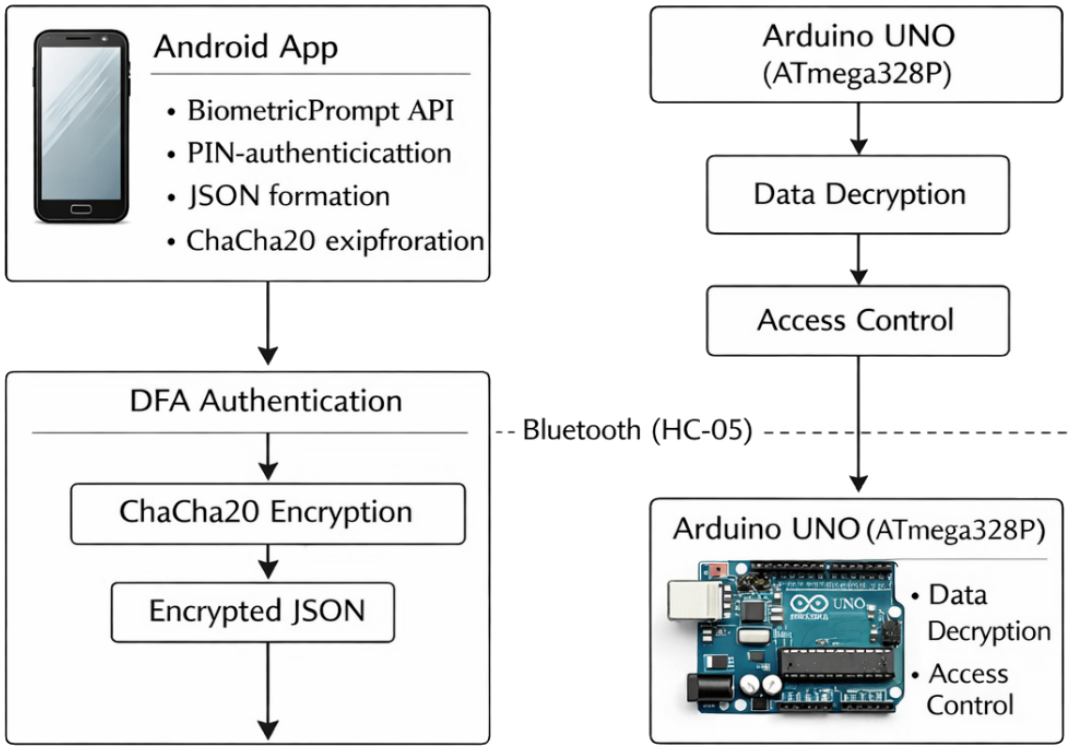


Fig.2 - Hardware–software implementation of the proposed MFA system

The encrypted data propagates over the Communication Channel to the Verification Server which processes that authentication decision. The server validates the accepted responses and verifies that they match with the expected authentication status.

In this process a feedback loop also exists in which the server returns Accept/Reject to the user device. This completes the authentication cycle and synchronizes client with server state.

The modular architecture allows distinct concerns of authentication control, key generation,

and encryption, both in terms of scalability and security.

Implementation. For the testing and validation of the proposed model, an initial prototype solution was built on a mobile client and an embedded device.

The mobile module obtains the authentication factors, performs DFA-based validation, and performs ChaCha20 encryption. The embedded module collects the encrypted data, verifies the integrity, and makes decisions on access control.

As a result, the components communicate with a lightweight structured data format for effective data transmission in resource-poor settings.

Figure 2 shows the actual implementation of the proposed system, including a mobile user interaction with the embedded device. The mobile application handles authentication and encryption and the embedded system processes the received data and controls access.

Moreover, its practical implementation demonstrates that the authentication model can work in a practical IoT environment under resource-constrained environments. This work tested a working prototype and verified it experimentally.

Research Methods. First, formal modelling is used to describe the authentication process with deterministic finite automata (DFA). This method lets us model the authentication logic as a state-transition system with some clear states, input and transition functions. Formal modeling guarantees the identity authentication process is deterministic, unambiguous, and verifiable. Furthermore, this method lays a great foundation for evaluating system correctness and resistance to logical attacks, e.g. replay and sequence manipulation. This way, this chaotic setup adds a new dimension of uncertainty, and makes the system more resistant to brute-force and statistical attacks. Mathematical modeling is applied to specify system parameters, initial cases, transformational changes, necessary for transforming the continuous chaotic signals into discrete binary sequences.

Secondly, dynamics modeling through nonlinear processes using the Lorenz system are used to model the random system for creating the chaotic keys. The Lorenz system, which is characterized by a set of nonlinear differential equations, has a delicate dependence on initial conditions and the dynamics are often intricate. These properties are exploited to generate very high entropy. The approach and method of this study is a set of formal, mathematical, algorithmic as well as experimental methods to build and test a secure and efficient multi-factor authentication model. These two-fold methods integrate not only with theoretical strength, but they also guarantee practical implementation.

Third, formalization of algorithm design is undertaken to organize the authentication process and key generation. The proposed model provides a step-by-step algorithm and is done in the form of each layer, making it easy to understand and implement. Algorithmic formalization eliminates ambiguity in system behavior and enables the authentication workflow can be systematically evaluated and rationalized.

Fourth, numerical simulation is performed to simulate the Lorenz system, and to draw chaotic sequences in a discrete environment. Since Lorenz was continuous in nature, numerical methods are needed to approximate its function. The simulation consists of iterative computation, normalization of values and quantization into the discrete units needed for cryptographic purpose.

Fifth, a comparative performance evaluation of experimental results is performed to understand the effectiveness of the proposed model versus conventional cryptographic approaches. Performance measures (how long it takes to execute, throughput, computational overhead, etc.) The evaluation is conducted under scenarios, which are representative of resource-constrained environmental conditions, making the results applicable to IoT and embedded systems.

Lastly, comparative analysis is applied to assess whether the proposed model is beneficial in comparison to the state-of-the-art multi-factor authentication mechanisms. Comparison encompasses characteristics of security (replay, brute force attack resistance), as well as performance (computation cost and memory usage

etc). This allows the advantages and disadvantages of the suggested method to be evaluated in a complete manner. Such a framework can form an effective structure for constructing, codifying, and validating the hybrid MFA model.

To do so, the study combines formal validation methodologies with the practical performance characterization process, so that the solutions presented are both theoretically robust and practical.

Research Stages. To ensure methodical development and testing of the proposed model, a series of stepwise phases were followed throughout the implementation of the study:

1. Analysis of existing MFA methodologies and their flaws in security, computation, and lack of formal verification.

2. Design of a DFA-based authentication model with clearly defined state transitions.

3. The Lorenz dynamical system is used for the chaotic key generation implementation.

4. Introduction of lightweight encryption mechanisms based on the ChaCha20 stream cipher.

5. Analysis of system performance in resource-constrained conditions.

6. Comparative analysis of baseline authentication and encryption methods.

Evaluation Metrics. This hybrid MFA model is reported with performance and security metrics:

1. Execution time - to measure computational efficiency.

2. Throughput - to evaluate system performance under load.

3. Resistance to repay attacks ensured through deterministic state transitions.

4. Resistance to brute-force attacks - enhanced by chaotic key generation.

5. Computational complexity - reflecting resource consumption.

6. Suitability for resource-constrained environments - particularly for IoT and embedded systems.

Metrics are a set of quantifiable measurements that are used to evaluate the overall security robustness and performance of a system.

DFA-Based Authentication Model. The deterministic finite automaton used in the proposed system is formally defined as a 5-tuple [12]:

$$DFA = (Q, \Sigma, \delta, q_0, F), \quad (1)$$

where:

1. $Q$is a finite set of states.

2. $\Sigma$is the input alphabet.

3. $\delta : Q \times \Sigma \to Q$is the transition function.

4. $q_0 \in Q$is the initial state.

5. $F \subseteq Q$is the set of accepting states.

State transitions:

1. $q_0 \to q_1$— first factor verified.

2. $q_1 \to q_2$— second factor verified.

3. $q_2 \to q_3$— authentication success.

4. any failure $\to q_{fail}$.

The authentication process follows a strictly defined sequence of transitions and was illustrated in Figure 3.

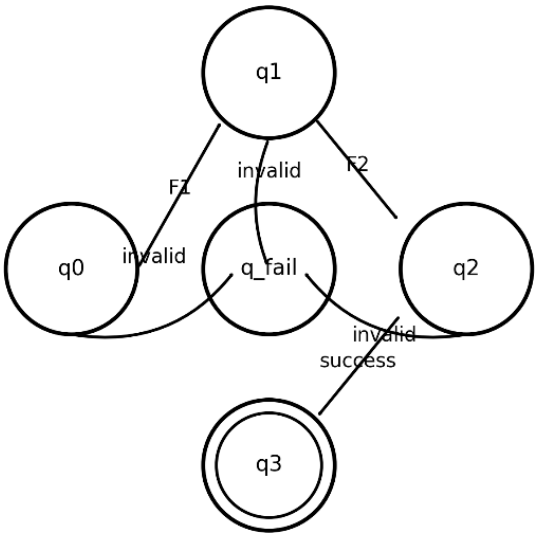


Fig.3 - DFA State Transition Diagram

The first authentication factor (e.g., password or biometric data) triggers a transition from $q_0$to q_1. The second factor leads to a transition from $q_1$to q_2. Successful completion of all required steps results

in the final accepting state q_3. Any incorrect input or violation of the sequence results in a transition to the rejection state q_{fail}.

This deterministic structure prevents bypass or reordering of authentication. In addition, the DFA model protects against replay attacks by enforcing unique session parameters. Valid transitions are not created by repeated inputs, meaning that previously intercepted authentication data cannot be reused.

Chaotic Key Generation Method. The cryptographic key used in the authentication process is generated using the Lorenz chaotic system, defined by the following system of differential equations:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x) \\ \frac{dy}{dt} &= x(\rho - z) - y \\ \frac{dz}{dt} &= xy - \beta z \end{aligned} \tag{2}$$

where σ, ρ, and $\beta$are system parameters.

The key generation process consists of the following steps:

1. Initialization of system parameters and initial conditions.

2. Numerical iteration of the Lorenz system.

3. Extraction of the x-component sequence.

4. Normalization of values.

5. Quantization into discrete byte values:

The key is derived as:

$$k_i = \text{mod}(|\ x_i\ | \cdot 10^6, 256), \tag{3}$$

6. Construction of a binary sequence;

7. Formation of a 256-bit cryptographic key.

Encryption Method. To ensure confidentiality of authentication data, the ChaCha20 stream cipher is used. The encryption process is defined as:

$$C = M \oplus KS(K, nonce, counter), \tag{4}$$

where: M- plaintext data, K- secret key generated by the chaotic system, KS- keystream generated by ChaCha20, C- ciphertext.

ChaCha20 is selected due to its efficiency in software implementations and suitability for low-resource environments.

To ensure confidentiality of the generated OTP, the output of the DFA is encrypted using the ChaCha20 stream cipher before transmission [13].

The encryption process can be represented as:

$$C = OTP \oplus KS, \tag{5}$$

where: C is the ciphertext, $OTP$is the generated one-time password, KS is the keystream generated by ChaCha20.

Authentication Algorithm. The complete authentication procedure is formalized as follows:

Input: authentication factors $F1$, $F2$.

Output: authentication status.

The complete authentication workflow is shown in Figure 4.

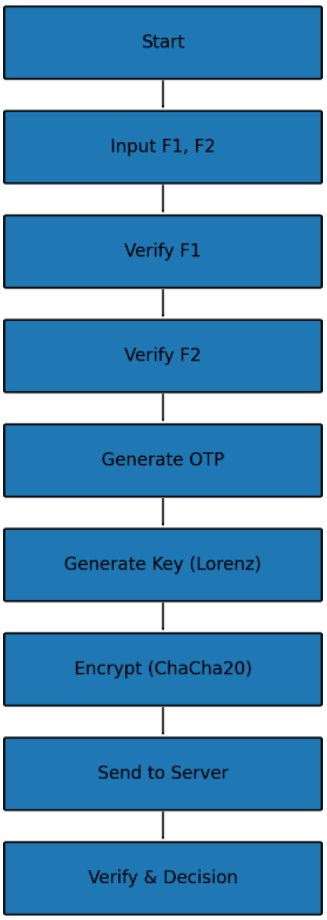


Fig.4 - Authentication Protocol Flow

Each step of the process-from factor verification to encrypted transmission—is presented sequentially:

1. Initialize state q_0.

2. Verify first factor:

I. if false → reject.

II. else → transition to q_1.

3. Verify second factor:

I. if false → reject.

II.else → transition to q_2.

4. Generate one-time authentication data.

5. Generate cryptographic key using the Lorenz system.

6. Encrypt data using ChaCha20.

7. Transmit encrypted data to the server.

8. Perform server-side verification.

9. Return authentication result (accept/reject).

To ensure reproducibility and eliminate ambiguity in the authentication process, the proposed model is formally specified using structured pseudocode. The following algorithm represents the complete authentication workflow, including DFA-based validation, chaotic key generation, and encrypted communication. The formal representation of the authentication process corresponding to the flowchart in Figure 3 is given in Algorithm 2.

Formal Authentication Algorithm Pseudocode:

Input: F1, F2

Output: Auth_Status

```
state = q0
if Verify(F1) == false:
    return Reject
state = q1
if Verify(F2) == false:
    return Reject
state = q2
Generate OTP
K = GenerateKey(Lorenz)
C = ChaCha20(OTP, K)
Send C to server
if ServerVerify(C) == true:
    return Accept
else:
    return Reject
```

Results and Discussion. In this research, a hybrid multi-factor authentication model based on deterministic finite automata (DFA), chaotic key generation (using the Lorenz system), and ChaCha20 stream cipher encryption was proposed.

Table 1 - Performance Comparison of Authentication Models

Metric	Proposed Model (DFA + ChaCha20 + Lorenz)	Traditional MFA (AES-based)
Execution Time	Low	High
Throughput	High	Medium
Computational Overhead	Low	High
Energy Consumption	Low	High
Suitability for IoT	High	Limited

This approach compensates for the limitations of conventional authentication systems by leveraging formal verification, improved security, and reduced computational overhead within a common architecture. Deterministic finite automata were used to formalize the authentication process, which

is one of our work's contributions.

In contrast to traditional MFA solutions, where authentication logic is normally executed in a procedural fashion, this architecture supports strict state transitions and removes the ambiguity from this process. It provides inherent resistance to replay attacks, as any departure from a predefined sequence leads to rejection.

A comparative analysis was performed with AES-based systems for MFA to assess the effectiveness of the proposed approach. Results are listed in Table 1.

The suggested model substantially outperforms conventional AES-based models based on execution time and computation efficiency, presented in Table 1.

Since the ChaCha20 stream cipher is optimized for software implementations and does not require complex block operations, it is mostly used to bypass all complexities. Beyond that, the proposed model has enhanced security characteristics. There is a comparative security analysis in Table 2.

Table 2 - Security Comparison of Authentication Approaches

Security Property	Proposed Model	Traditional MFA
Replay Attack Resistance	High	Medium
Brute-force Resistance	High	Medium
Formal Verification	Supported	Not supported
State Control	Strict (DFA)	Weak
Key Entropy	High (chaotic)	Medium

The findings in Table 2 demonstrate that the combination of DFA and chaotic key generation can considerably improve the security of the authentication process. Deterministic design ensures sequential order of the authentication steps, and Lorenz-based key generation introduces high entropy with non-trivial unpredictability.

Analytically, we can derive the performance of this proposed model from the synergy of components. The DFA guarantees logical accuracy and avoids any protocol-level vulnerabilities, the chaotic system boosts the cryptographic strength, and the ChaCha20 cipher is efficient computational material. This hybrid provides a complementary approach that satisfies the security and performance issues.

In addition, experimental testing indicated that the proposed model is able to keep its performance stable under the condition of resource constraint, so it is especially well-suited for IoT and embedded domains. Unlike the conventional MFA systems, which can lead to heavy latency and consume a lot of energy, the proposed method allows fast authentication with lower resource consumption.

This model has its drawbacks though and a few practicalities. In chaotic systems, parameters and numerical stability must be carefully chosen. Further, synchronization between client and server states must be considered to properly perform DFA operation. These issues deserve further investigation in the future.

Therefore, the hybrid MFA model presented offers a robust, formal and efficient authentication solution based on this data. Compared to conventional methods, it shows obvious strengths (both performance and security), hence could become a potential one of the next generation authentication systems in distributed and resource bound contexts.

Conclusion. This paper introduced a hybrid multi-factor authentication model based on DFA, Lorenz-based chaotic key generation, and ChaCha20 stream cipher under one unified structurally designed abstract environment. The

proposed method was inspired by the drawbacks of conventional MFA schemes, including their not having formal verification, replay attack, and heavy computational burden, especially in resource-constrained settings such as IoT and embedded devices.

The results indicate that the formal process of authentication based on deterministic finite automata offers the formalized and mathematically sound way of controlling the authentication logic. The model provides a strong enough mechanism to achieve state transitions so that authentication progresses linearly rather than having ambiguity created during steps and can prevent unauthorized bypass of verification. Since replay attacks continue to be a prominent threat in many of these distributed environments, this deterministic behavior drastically improves system reliability as well as inherent resistance.

Adding chaotic key generation on top of Lorenz system provides another layer of resilience to such attacks. The generated keys are therefore very high entropy and unpredictable, given the strong potential response of chaotic systems to initial conditions of the system and the non-linear dynamics of the system itself. This phenomenon increases sensitivity to brute-force and statistical attacks; hence, the proposed model is more resistant against such brute-force attacks than conventional key generation mechanisms.

Besides, the ChaCha20 stream cipher is computationally cheap and easy to implement in a software environment. When computing power and energy overheads are reduced, the experimental results confirm that the proposed model achieves lower execution time and a higher throughput than AES-based MFA systems. This makes the model especially convenient when applied to devices on low power and where real-time authentication is required. From an analytic perspective, the effectiveness of the proposed approach lies in the synergistic interaction of its components.

The DFA provides formal correctness as well as structural security, the chaotic system increases cryptographic unpredictability, and the stream cipher allows smooth processing of the data. This enables the model to achieve a proper trade-off between security and performance, essential for today's distributed systems.

Furthermore, the modular structure of the proposed system means that it can be easily scaled up or down. The components of these models (authentication control, key generation and encryption) can be individually customized or extended to adapt the model to different applications, such as IoT applications, mobile devices, and cloud services.

Notwithstanding the strengths, some limitations need to be considered. In practical practice, while challenging, chaotic key generation must be made, with the choice of system parameters and a stable numerical technique in order to not make randomness properties lose. In addition, the DFA-based approach necessitates a correct synchronization in the state of clients and servers, which further complicates the distributed systems. For real world deployment, overcoming these issues is crucial.

Thus, here we propose hybrid MFA to secure, efficient, and formally verifiable authentication on the best practices compared with the traditional model as a better-performing and safer solution. The findings of this work prove that we can employ formal automata theory in combination with lightweight and chaos-based cryptographic methods to reach an optimal path for next generation authentication.

In future works, it would also be useful to contribute the adaptation and context-based authentication model, the combined biometric and behavioural factors factor analysis, large experimental validation work in a real system. Further details on chaotic system optimization and hardware-based implementations may increase the practicality of the proposed method.

References

1. Ashok N., Judgi T. Optimized Multi-Factor Authentication Through Context-Aware Deep and Federated Learning Approaches//Mathematical Modelling of Engineering Problems. -2025.-Vol.12(12):4435-4442. DOI 10.18280/mmep.121232.

2. Nair V., Song D. Mfdpg: Multi-factor authenticated password management with zero stored secrets //arXiv preprint arXiv:2306.14746. -2023. DOI 10.48550/arXiv.2306.14746.

3. Khajehzadeh L., Barati H., Barati A. L2AI: lightweight three-factor authentication and authorization in IOMT blockchain-based environment //arXiv preprint arXiv:2407.12187.-2024. DOI 10.48550/arXiv.2407.12187.

4. Saukhanova Z., Shakhmetova G, et al. Identifying the efficiency of applying of finite automata in encryption and decryption//Eastern-European Journal of Enterprise Technologies. -2025.-Vol.3(9(135). -P.65-78.DOI 10.15587/1729-4061.2025.331044.

5. Vayadande K., Agarval K, et al. Cryptography using automata theory//ITM Web of Conferences. -2022. Vol.-50(1). DOI 10.1051/itmconf/20225001007.

6. Jammula M., Mani V.V, Kondoju S. K. Performance evaluation of lightweight cryptographic algorithms for heterogeneous IoT environment// Interconnection Networks. -2022.-Vol.22: 2141031. DOI 10.1142/S0219265921410310.

7. Suleski T.,Ahmed M, et al. A review of multi-factor authentication in the Internet of Healthcare Things //Digital health. -2023.-Vol.9.-P.1-20. DOI 10.1177/20552076231177144.

8. Modarres A. M. A., Sarbishaei G. An improved lightweight two-factor authentication protocol for IoT applications//IEEE transactions on industrial informatics. -2023.-Vol.19(5). -P.6588-6598. DOI 10.1109/TII.2022.3201971.

9. Fasila K., Mathew S. An efficient multilevel security architecture for blockchain-based IoT networks using principles of cellular automata //PeerJ Computer Science. -2022.-Vol.8: e989. DOI 10.7717/peerj-cs.989.

10. Sorescu T. G.Chiriac V.M., et al. Comparative Performance Analysis of Lightweight Cryptographic Algorithms on Resource-Constrained IoT Platforms+ //Sensors.-2025.-Vol.25(18): 5887. DOI 10.3390/s25185887.

11. Ihsan M., Madduri C, et al. Secure Authentication in IoT Devices Using Lightweight Multi-Factor Cryptographic Schemes//2025 International Conference on Intelligent Communication Networks and Computational Techniques (ICICNCT).-2025. DOI 10.1109/ICICNCT66124.2025.11233122.

12. Shakhmetova G., Saukhanova Z., et al. Ontological Model of Cryptosystems Based on the Theory of Finite Automata// IEEE, 2024 International Visualization, Informatics and Technology Conference (IVIT). -2024. DOI 10.1109/IVIT62102.2024.10692774.

Information about the authors

Kulzhanova A.A.-Lecturer at the International University of Engineering and Technology, Almaty, Kazakhstan, e-mail: akbota.kulzhanova1594@gmail.com.

Zhmud V.A.- Doctor of Technical Sciences, Professor, Novosibirsk State Technical University, Novosibirsk, Russia, email: oao_nips@bk.ru.

Сведения об авторах

Кульжанова А.А.-лектор МИТУ, Алматы, Казахстан, e-mail: akbota.kulzhanova1594@gmail.com.

Жмудь В.А.- доктор технических наук, профессор, Новосибирский государственный технический университет, Новосибирск, Россия, e-mail: oao_nips@bk.ru.