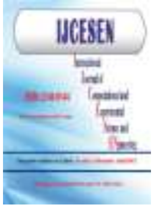
*International Journal of Computational and Experimental Science and ENgineering*
*(IJCESEN)*

*Vol. 10-No.4 (2024) pp. 1041-1049*
http://www.ijcesen.com



**ISSN: 2149-9144**

**Research Article**

# Blockchain-Enhanced Multi-Factor Authentication for Securing IoT Children's Toys

**Ahmad Alkhatib[1]*, Layla Albdour[2], Seraj Fayyad[3], Hussien Ali[4]**

[1]Alzaytoonah University of Jordan, , Faculty of Science and Information Technology, Cyber Security Department, 11733, Amman-Jordan
*** Corresponding Author Email:** Ahmad.Alkhatib@zuj.edu.jo - **ORCID:** 0000-0002-1369-1184

[2]Alzaytoonah University of Jordan, , Faculty of Science and Information Technology, Cyber Security Department, 11733, Amman-Jordan
**Email:** l.albdour@zuj.edu.jo - **ORCID:** 0000-0001-5088-2724

[3]Alzaytoonah University of Jordan, , Faculty of Science and Information Technology, Cyber Security Department, 11733, Amman-Jordan
**Email:** s.fayyad@zuj.edu.jo - **ORCID:** 0000-0002-3882-5310

[4]Alzaytoonah University of Jordan, , Faculty of Science and Information Technology, Computer Science Department, 11733, Amman-Jordan
**Email:** Husseinalimohammed6@gmail.com - **ORCID:** 0000-0002-3944-0320

**Article Info:**

**DOI:** 10.22399/ijcesen.417
**Received :** 13 August 2024
**Accepted :** 05 November 2024

**Keywords**:

Internet of Things (IoT),
Children's toys security,
multi-factor authentication,
QR code,
Blockchain

**Abstract:**

The rapid expansion of Internet of Things (IoT) devices underscores the critical importance of robust security protocols, particularly in the realm of children's toys. This study introduces an innovative multi-factor authentication strategy integrating Quick Response (QR) codes with Blockchain technology to fortify the security of IoT toys designed for children. The primary objective is to safeguard young users against potential threats stemming from unauthorized access, thereby ensuring a secure interaction with IoT-enabled toys. By amalgamating authentication factors, including QR codes, the proposed approach establishes a multilayered security framework. Leveraging the inherent immutability and transparency of Blockchain, the system verifies the authenticity of IoT toys by scanning a unique QR code, thus mitigating risks associated with malwares and unauthorized access. The decentralization of Blockchain ensures no single point of failure, enhancing resilience against cyber threats. Extensive usability studies underscore the efficacy and practicality of the advanced multi-factor authentication solution, poised to elevate the safety standards of IoT toys in the digital age. Furthermore, the study identifies potential avenues for future research, including the exploration of enhanced scalability, interoperability with various IoT ecosystems, and the integration of additional authentication mechanisms to adapt to evolving security challenges. This innovative approach not only bolsters security but also fosters trust among users, enabling seamless and worry-free interaction with IoT-enabled toys for children worldwide

## 1. Introduction

The Internet of Things (IoT) is the most emerging technology in which all the objects in the real world can use the Internet to communicate with each other as parts of a single unified system. The development of many smart applications such as games, homes, healthcare, transportation, cities and some technologies built on AI systems etc [1]. Furthermore, current IoT systems suffer from critical weaknesses in the information security system, including the possibility of identifying infected devices, the deposition of hackable data or services and accessible users affected by this information security breach. The cybersecurity challenge in IoT systems is to find solutions that can deal in a simple way with users' identity and devices in a simple and secure way and when looking at internet-connected children's toys where they are a subset of IoT devices that deserve special attention from the security community. The 2015 Hello Barbie hack, in which security researchers were able to remotely access the doll's microphone and record children's conversations [2], clearly demonstrates the importance of securing IoT toys. This research proposes an effective multifactor authentication solution based on robust combiners of the unique QR code printed on the toy using a companion mobile application. The proposed solution mitigates the authentication vulnerabilities of IoT and defends against several types of attacks.

The Federal Trade Commission's Children's Online Privacy Protection Rule (COPPA) places specific requirements on these services, including that they must "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children" [3]. In addition to mandated COPPA compliance, manufacturers of IoT toys provide their privacy policies to indicate data handling practices and security measures specific to their products. However, consumers have no way to verify whether IoT toys follow COPPA regulations or manufacturer privacy policies. Recent high-profile hacks of IoT devices give reason to doubt the security claims of these products [4,5,6].

There are many weaknesses, including lack of data encryption (HTTP instead of HTTPS), lack of authentication to access personally identifiable information (PII), re-use of POST code, asymmetric HTTP responses that allow unique identity mining, and PI as shown in several studies that touched on privacy breaches in children's games and violations of both COPPA and individual game privacy policies. Despite its potentially serious impact, all these weaknesses can be easily corrected. Their presence refers to a major developer error, indifference or ignorance of privacy and best security practices that we can deal with for the purposes of developing the right security practices, applying rigour in privacy to children's games, defending consumer rights and privacy, and practices that lead to development by IoT game manufacturers [5].

A blockchain is essentially a distributed ledger technology that records transactions across multiple nodes in a way that makes them tamper-resistant and transparent. It consists of blocks of data linked together in a chronological chain, with each block containing a list of transactions. Each block also includes a unique cryptographic hash of the previous block, ensuring that any alteration to a previous block would be evident in subsequent blocks, thereby preserving the integrity of the data. This decentralized structure makes blockchain ideal for applications such as cryptocurrency, supply chain management, security, and more [7].

Blockchain technology offers several security benefits to provide integrity, transparency, decentralization, and resistance to tampering. Those benefits are:

**Immutability:** Once a transaction is recorded on the blockchain, it is extremely difficult to alter or delete it. Each block contains a cryptographic hash of the previous block, creating a chain of blocks that makes tampering evident.

**Decentralization:** Blockchain operates on a decentralized network of computers (nodes), which means there's no single point of failure. This reduces the risk of attacks that target centralized systems.

**Transparency:** Blockchain transactions are transparent and verifiable by anyone on the network. This transparency fosters trust among participants and makes it easier to detect and prevent fraudulent activities.

**Encryption:** Blockchain uses advanced cryptographic techniques to secure transactions and data. Private keys and digital signatures ensure that only authorized parties can access and modify the data.

**Consensus Mechanisms:** Blockchain networks rely on consensus mechanisms (e.g., Proof of Work, Proof of Stake) to validate and confirm transactions. These mechanisms ensure that the majority of nodes agree on the state of the blockchain, making it difficult for malicious actors to manipulate the network.

In this work we will propose a multi-factor authentication based blockchain using the online code and the toys with QR Code technology to give approval for the use of games associated with the Internet of Things technologies (IoT). The remainder of this paper is organized as follows: Section 2 provides an overview of related work. Section 3 introduces the proposed blockchain-based authentication framework, detailing its architecture, components, and operational principles. In Section 4, we present a comprehensive analysis and discussion of the framework's security features, including its resilience against common cyber threats. Finally, Section 5 concludes the paper with a summary of our findings and insights into future directions for enhancing the framework's scalability, interoperability, and efficiency in diverse IoT environments."

## 2. Literature Review

This section requires a review of many previous studies that addressed security weaknesses and privacy policy violations, and there is a need to develop a special mechanism to protect children from unsafe Internet-related toys and develop technology that is linked to parents and decentralized surveillance to monitor and maintain children's privacy.

The breaches that gained widespread attention involving internet-connected toys emphasize the financial worth of children's data within the framework of surveillance capitalism. These breaches encompass notable incidents such as the unauthorized access to Mattel's Wi-Fi Hello BarbieTM (November 2015) [2], VTech's Learning LodgeTM (November 2015) [8], and CloudPetsTM (2017) [9]. Various other breaches were executed by both consumer groups and ethical hackers ('white hat' hackers), who underscore the inadequate data security embedded within connected toys and their supporting structures. Research carried out by the Norwegian Consumer Council on two connected toys, My Friend Cayla™ and iQue Intellegeny Robot™ [10], as well as children's smartwatches [11], shed light on these vulnerabilities. Furthermore, the German government classified the My Friend Cayla™ doll (a toy similar to Hello BarbieTM) as an "illegal espionage apparatus" due to its breach of German law, which prohibits the manufacture, sale, or possession of surveillance devices camouflaged as other objects [12]. In the same year, the government prohibited the use of children's smartwatches because "through an app, parents can surreptitiously listen to the child's surroundings via such children's watches, classifying them as an unauthorized transmitting system" [13].

Upon publicizing IoToys data breaches, it becomes evident how extensive and vital the data held by IoToys manufacturers and their service providers truly is. For instance, during the 2015 VTech breach, it was revealed that "approximately 2.2 million parents had registered and set up accounts on Learning Lodge for almost 3 million children" [8]. A more recent breach of CloudPetsTM' database exposed over 820,000 user accounts, making them susceptible to theft. These user profiles contained sensitive information like pictures and names of children, in addition to their birthdates. Moreover, the profiles disclosed the child's connections to authorized adults, such as parents, grandparents, and aunts, who could share messages with the child [14]. At this juncture, it seems that certain toy manufacturers lack the essential technical expertise or are hesitant to either employ or contract this expertise to adequately safeguard children's data. Furthermore, there is a noticeable lack of transparency and impartial oversight concerning children's data in the online domain at this stage.

CloudPetsTM experienced a data breach, where unauthorized access to their database was discovered by security expert Troy Hunt [14], creator of 'Have I Been Pwned?'—a website allowing individuals to check if their personal information has been compromised. CloudPetsTM, produced by Spiral Toys in California, are internet-connected plush toys that facilitate voice messaging between parents and children. These toys use Bluetooth Low Energy (BLE) technology to connect with parents' smartphones, enabling family members to exchange voice messages with the toy. The associated app also allows the toys to play lullabies and narrate stories via the toy's speakers [9]. To receive and record messages, children interact with the toy's paws (left paw for receiving, right paw for recording), and the messages are stored and transmitted via cloud storage to designated family members.

Troy Hunt identified that the CloudPetsTM database was inadequately secured, specifically a publicly accessible MongoDB without authentication, indexed by Shodan—a search engine for connected devices (2017). Disturbingly, this unsecured database contained over 2,182,337 voice recordings, encompassing both children and adults. Unauthorized parties accessed and interacted with the CloudPets data, often holding it for ransom. Despite multiple attempts through various channels, including email, phone calls, Facebook, and Twitter, to alert Spiral Toys of this critical breach, there was no response. Moreover, Spiral Toys failed to inform parents about the breach—a mandatory requirement under Californian government regulations, where the company is situated [14].

Hunt was alerted about the breach by a contact involved in data breach trading circles, which involve the distribution of stolen databases for financial gain or personal interest. These breached databases can spread widely once exposed due to the ease and speed of digital information replication across the globe [15]. Hunt highlighted in his testimony to the US House Committee on Energy and Commerce that the surge in affordable cloud services and the rapid growth of the "Internet of Things" have amplified the risk of data breaches, as new types of information are digitized and made vulnerable [15].

Up to this point, toy manufacturers like Spiral Toys have been responsible for regulating their data privacy and safety practices. However, the CloudPetsTM incident reveals a significant flaw in this approach. The prevalent use of insecure, inexpensive cloud-based database platforms is a major part of the issue, making these databases easily susceptible to hacking. Some toy companies, such as Cognitoys, prioritize responsible practices by integrating current best security practices into their toy design and infrastructure. Conversely, others like Spiral Toys lack the required skills and technical infrastructure to navigate the IoToys space independently. Given the prevalent vulnerability of

IoToys to hacking at both Bluetooth and database levels, it is evident that the current self-regulatory environment is insufficient [16,17].

"An Analysis of Security and Privacy Vulnerabilities in Internet of Things Toys" by Egelman et al., [18] - This study used penetration testing, code review, and network traffic analysis to identify security vulnerabilities in a variety of internet-connected toys. The study found that many of the toys had poor security practices, such as weak encryption and easily guessable passwords, which put the personal information of children at risk.

"A Study of Privacy Risks in Children's Smart Toys" by Kao et al., [19] this study used a combination of code review, user surveys, and interviews with developers to investigate the privacy risks in children's smart toys. The study found that many of the toys had poor privacy practices, such as collecting sensitive personal information without adequate disclosure or consent, and storing it in a way that was not secure.

"IoT Toy Hack: Investigating the Security of IoT Toys for Children" by R. J. [20]- This study used a combination of penetration testing and code review to investigate the security of IoT toys for children. The study found that many of the toys had poor security practices, such as weak encryption and poor access controls, which put the personal information of children at risk.

The paper presents a systematic literature review conducted by Almadani et al., [7] on blockchain-based multi-factor authentication (MFA). The authors aim to provide insights into the current state of research in this area by analyzing existing literature. The systematic review examines various aspects of blockchain-based MFA, including its implementation, effectiveness, security implications, and applications. By synthesizing findings from relevant studies, the paper offers a comprehensive understanding of the opportunities and challenges associated with deploying blockchain-based MFA solutions. Additionally, the review identifies research gaps and suggests directions for future research in this domain. Overall, the paper contributes to advancing knowledge in the field of blockchain-based authentication and provides valuable insights for researchers and practitioners working on securing digital systems using multi-factor authentication techniques.

A New Blockchain-Based Authentication Framework for Secure IoT Networks" proposes. an innovative authentication framework leveraging blockchain technology to enhance security in IoT networks by Al Hwaitat et al., [21]. This framework aims to address the vulnerabilities present in traditional authentication methods by leveraging the decentralized and tamper-resistant nature of blockchain. Through the use of cryptographic techniques and distributed consensus mechanisms, the proposed framework ensures the integrity and authenticity of transactions within IoT networks. By integrating blockchain into the authentication process, the framework offers enhanced security measures, thereby mitigating the risks associated with unauthorized access and tampering.

Li et al. [22] discusses the proliferation of connected edge devices in smart city environments, driven by advancements in the Internet of Things (IoT) and cloud computing, underscores the critical need for robust authentication mechanisms to bolster security. With billions of devices interconnected, ensuring their protection against potential threats is paramount. However, securing these devices can pose significant challenges, particularly for resource-constrained devices. To address these challenges, researchers have turned to decentralized solutions such as blockchain technology, with Ethereum emerging as a popular choice due to its programmable smart contracts. In this study, we propose an enhanced authentication mechanism designed to bolster security while improving performance. Leveraging the unique properties of the Neo blockchain platform, known for its enhanced security features and faster transaction execution, our research presents a novel approach to authentication. Comparative analysis against existing algorithms demonstrates notable improvements, with the proposed mechanism exhibiting a 20% to 90% enhancement in execution time and a reduction of 30% to 70% in registration and authentication processes.

Kotel et al. [23] advocates for the utilization of Hyperledger Fabric to bolster the security of smart home systems through blockchain technology. The proposed approach aims to address the security limitations commonly encountered in existing permissioned blockchain methodologies. Central to the architecture is a multi-layered framework comprising the Cloud Storage Layer, Blockchain Platform Layer, Application Layer, and IoT Devices Layer. Notably, the integration of a cloud storage layer is strategically employed to leverage its inherent advantages in terms of efficiency and availability. Given that smart home devices often necessitate significant computing resources and storage capacity, the cloud presents an ideal solution to meet these demands effectively.

Traditional Multi-Factor Authentication (MFA) often falls short in these settings, prompting the exploration of blockchain-enhanced solutions [24]. Blockchain-Enhanced Multi-Factor Authentication (BEMFA) integrates blockchain's decentralized, tamper-resistant capabilities with MFA to address access control, data integrity, and security concerns in IoT. Internet-connected children's toys represent a unique segment within IoT devices that requires heightened attention from the security community [25]. If these toys are compromised, cyber-predators could potentially gather private information or interact with children remotely, posing serious safety risks. Effective user authentication is critical for all applications connected to the internet; however, single-factor authentication is widely considered insufficient, especially for applications aimed at children. Kids often use simple, easily guessed passwords in IoT-connected applications associated with these toys. Authors proposed implementing multi-factor authentication (MFA) in IoT-connected toys using companion applications. When unusual behavior, such as a change in IP address, GPS location, OS version, or browser, is detected, the system should prompt two-factor authentication to verify the child's identity and safeguard their security and privacy. They presented a multi-authentication approach that incorporates a password alongside additional verification methods, such as SMS, security tokens, digital certificates, or biometric authentication. Kaspersky [26] have uncovered vulnerabilities in a popular smart toy robot that could expose children to cybercriminals, allowing unauthorized users to secretly communicate with them through video chat without parental consent. The Android-based toy, designed for kids and equipped with a camera and microphone, uses AI to interact with children. However, during initial setup, a security flaw in the responsible API enables cybercriminals to intercept sensitive information such as the child's name, age, and IP address, posing significant risks. Additionally, attackers can exploit the toy's functionalities to initiate calls with children directly, bypassing parental controls. The security weaknesses extend to the parent's mobile application, where attackers can use brute-force methods to gain control over the robot, allowing them to link the device to their own accounts. Kaspersky [26] emphasizes the importance of prioritizing safety and security features when purchasing smart toys, urging parents to research products thoroughly, keep devices updated, limit app permissions, and use reliable security solutions. The findings were presented at Mobile World Congress 2024, and Kaspersky reported the vulnerabilities to the vendor, who has since issued patches[26].

## 3. Proposed Method

The user is required to scan a unique QR code printed on the toy using a companion mobile application, which then verifies the authenticity of the toy and establishes a secure connection. The authentication process incorporates factors such as possession of the physical toy, knowledge of the QR code, and the use of a trusted mobile application. By leveraging QR codes as part of the authentication process, the proposed approach offers a user-friendly and intuitive method for children to access their toys while mitigating security risks

***Figure 1:*** *propose a multi-factor authentication using the online code and the toys with QR Code technology to give approval for the use of games associated with the Internet of Things technologies (IoT).*

Authentication proposed system: Implementing blockchain in authentication systems can provide several advantages, primarily in terms of decentralization, immutability, and enhanced security. Security issues in kids' toys can pose significant risks, especially considering that children may not understand the implications of sharing personal information or interacting with connected devices. We used blockchain to authenticate the children's toys by scanning a QR code to validate the used toy and make sure no breaches or tampering have been made to avoid malwares and hackers from accessing these toys and miss use them (figure 1). The proposed system is demonstrated in figure 2.

In the first step a QR code is scanned using a mobile application to start verifying the smart toy. Upon the scanning process a new block is created as shown in step-2. Unlike traditional centralized systems, blockchain operates on a decentralized network of nodes (computers) where each node maintains a copy of the entire blockchain ledger. This decentralization eliminates the need for a central authority or intermediary to validate blocks.

Therefore, a copy of the generated block is broadcasted to the entire chain to start the validation process, as step-3 shows. Validation in blockchain refers to the process of verifying the integrity and authenticity of transactions- in our case the transaction is validating the toy- before adding them to the blockchain ledger. It ensures that only valid transactions are recorded, and the integrity of the blockchain network is maintained. Step-4 shows that each node independently verifies the transaction to ensure its validity. This verification typically involves checking the digital signatures of the transaction, ensuring that the sender has the authority to initiate the transaction. After initial verification, the transaction must be validated by the majority of nodes in the network to be added to the blockchain. Consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), or Delegated Proof of Stake (DPoS), are used to achieve agreement among network participants on the validity of transactions. Each consensus mechanism has its own rules and algorithms for determining which nodes are allowed to validate transactions and add new blocks to the blockchain. In step-5 Valid transactions are grouped together into blocks. Before a block is added to the blockchain, it undergoes further validation to ensure its integrity. Nodes compete to solve a cryptographic puzzle or mathematical problem (in the case of PoW) to create a new block. The first node to solve the puzzle broadcasts the solution to the network. Other nodes verify the solution and the validity of the transactions in the proposed block. If a consensus is reached, the block is added to the blockchain. Step-6 is the validation process that ensures the immutability and transparency of the blockchain ledger. Once a transaction is recorded on the blockchain, it cannot be altered or deleted without consensus from the majority of nodes.The transparency of the blockchain ledger allows anyone to verify the validity of transactions and track the entire transaction history to trace any breaches or alterations in the nodes.

## 4. Discussion

It is important to note that there have been several studies and reports in recent years that have highlighted security vulnerabilities and privacy policy violations in internet-connected children's toys. These studies have shown that these toys can be easily hacked, allowing unauthorized individuals to access sensitive information such as the child's name, location, and even hear and speak through the toy. Additionally, many of these toys have been found to have inadequate or non-existent privacy policies, which leaves children and their families at risk for data breaches and other privacy violations. It is essential for manufacturers and developers of internet-connected children's toys to prioritize security and privacy in the design and development of these products to protect the safety and well-being of children and their families. The main point of conducting a comprehensive, long-term study on the impact of security vulnerabilities and privacy policy violations in internet-connected children's toys on children and their families is to gain a better understanding of the full extent of the risks and potential long-term effects on children's safety and well-being. This information can be used to inform the development of solutions and best practices for addressing these issues in internet-connected children's toys. The proposed QR-based Blockchain for authentication framework presents a promising approach to address the security challenges faced by IoT networks. By integrating blockchain technology into the authentication process, the framework offers several advantages over traditional methods. Firstly, blockchain's decentralized nature ensures that there is no single point of failure in the authentication process. Each node in the network maintains a copy of the blockchain ledger, eliminating the risk of central authority compromise or single node failure. This decentralization enhances the resilience of the authentication system against various cyber threats and attacks. Moreover, blockchain's tamper-resistant properties enhance the integrity and transparency of the authentication process. Transactions recorded on the blockchain are immutable, making it extremely difficult for malicious actors to alter or tamper with authentication data. This immutability ensures the authenticity of user identities and device interactions within the IoT network, thereby reducing the risk of unauthorized access and data manipulation.

Additionally, the use of consensus mechanisms in blockchain ensures that only valid transactions are added to the blockchain ledger. Consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) enable network participants to collectively validate authentication transactions, further enhancing the security and trustworthiness of the authentication framework. Furthermore, the integration of cryptographic techniques in blockchain enhances the confidentiality and privacy of authentication data. Private keys and digital signatures ensure that only authorized parties can access and modify authentication information, protecting sensitive user and device data from unauthorized disclosure or manipulation. Overall, the blockchain-based authentication framework offers a robust and secure solution for IoT networks, mitigating the security risks associated with traditional authentication methods. By leveraging the decentralized, tamper-resistant, and transparent nature of blockchain technology, the framework provides enhanced security measures to safeguard IoT devices and networks against cyber threats and attacks. This technology is interesting and thus applied in some different fields in the literature [27-31].

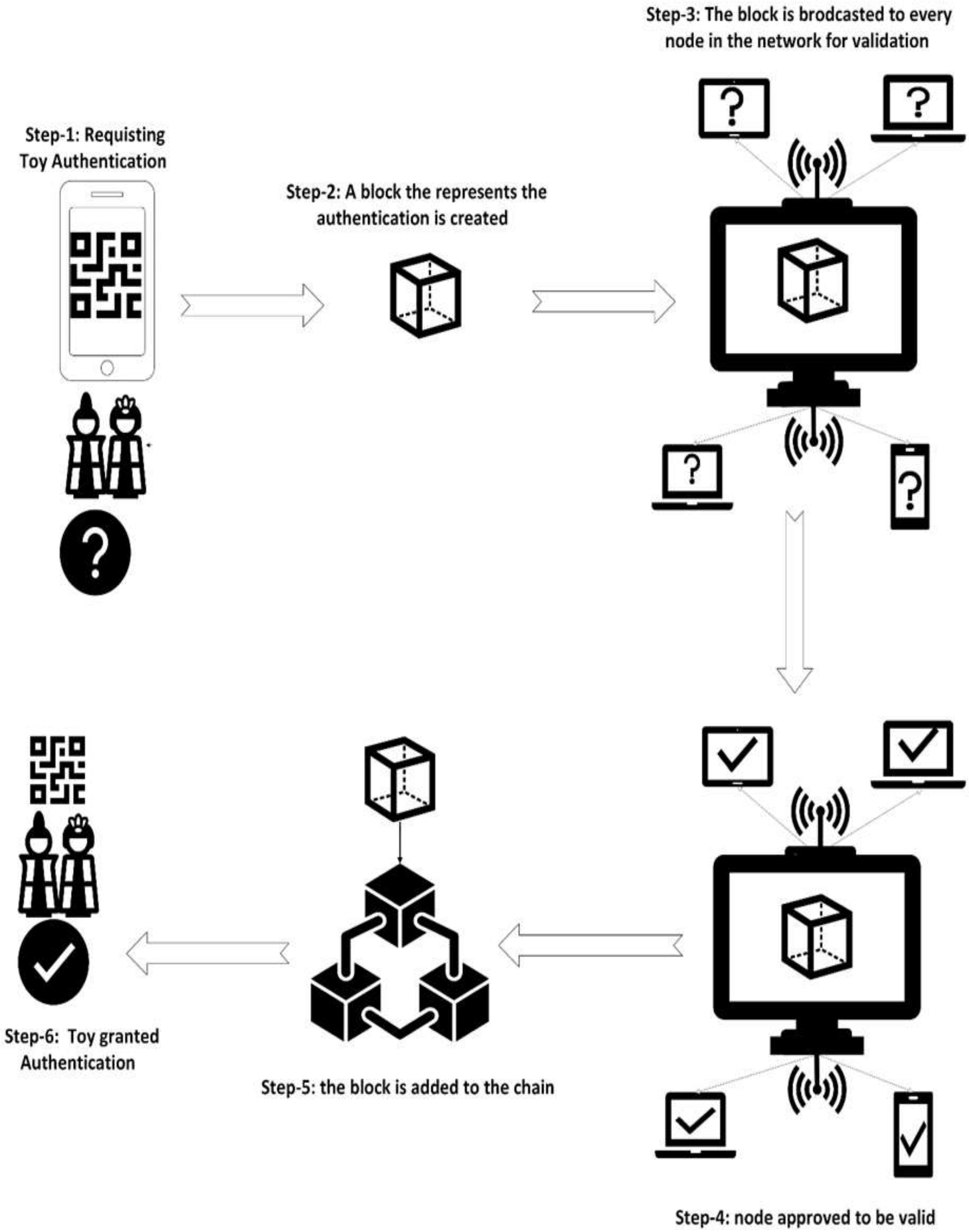

Step-1: Requisting Toy Authentication
Step-2: A block the represents the authentication is created
Step-3: The block is brodcasted to every node in the network for validation
Step-4: node approved to be valid
Step-5: the block is added to the chain
Step-6: Toy granted Authentication

***Figure 2*** *Proposed Block chain Authentication system*

## 5. Conclusion and Recommendations

In conclusion, this study presents a blockchain-based authentication framework designed to bolster security in IoT networks by overcoming limitations inherent in traditional authentication systems. Utilizing blockchain's decentralized, tamper-resistant, and transparent properties, this framework fortifies IoT device and network security against cyber threats and unauthorized access.

Through blockchain integration, the proposed framework ensures data integrity, transparency, and privacy throughout the authentication process. Blockchain's decentralized nature reduces vulnerabilities associated with single points of failure, increasing the system's resilience to attacks. Additionally, blockchain's tamper-resistant features help maintain the immutability of authentication transactions, deterring unauthorized modifications.

The framework's use of consensus mechanisms guarantees that only legitimate authentication records are stored on the blockchain ledger, enhancing the system's reliability. Furthermore, cryptographic techniques like private keys and digital signatures add another security layer, safeguarding sensitive data against unauthorized access.

Looking ahead, future work should focus on enhancing the framework's scalability, efficiency, and interoperability to support the growing demands and complexity of IoT environments. Research could explore optimizing the framework for high-transaction environments and developing cross-platform compatibility to ensure seamless integration across diverse IoT ecosystems. Addressing these areas will ensure the framework remains adaptable to evolving security challenges in the digital landscape, providing an enduringly robust solution for IoT authentication.

## Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

## References

[1]AbdelQader, A., Lafi, M., Awad, K., & AbedelQader, M. A. (2023). A Novel Approach to Elicit Software Requirements for IoT Systems Using SVM Classifier. In 2023 *International Conference on Information Technology (ICIT) (pp. 779-782)*. Amman, Jordan. doi: 10.1109/ICIT58056.2023.10225969

[2]Gibbs, S. (2015, November). Hackers can hijack wi-fi Hello Barbie to spy on your children. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children

[3]Federal Trade Commission. (1998). Children's online privacy protection rule ("COPPA"). Retrieved from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[4]Munro, K. (2015, January). Making children's toys swear. Retrieved from https://www.pentestpartners.com/security-blog/making-childrens-toys-swear/

[5]Cooper, D. (2017). Researchers find another smart toy that's easy to hack. *Engadget*. Retrieved from https://www.engadget.com/2017/12/08/teksta-toucan-can-listen-to-kids-researchers-security/

[6]Franceschi-Bicchierai, L. (2017). Internet of things teddy bear leaked 2 million parent and kids message recordings. Motherboard. Retrieved from https://motherboard.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

[7]Almadani, M.S., Alotaibi, S., Alsobhi, H., Hussain, O.K., & Hussain, F.K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. *Internet of Things,* 23.

[8]Federal Trade Commission. (2018). Electronic Toy Maker VTech Settles FTC Allegations that it Violated Children's Privacy Law and the FTC Act.

[9]CloudPets (2017). Gold [app download page]. Retrieved from https://itunes.apple.com/au/app/cloudpets-gold/id976429128?mt=8

[10]EU & US (2016). consumer take action against flawed connected toys. BEUC NEWS. Brussels: *The European Consumer Organisation.*

[11]WatchOut (2017).: Analysis of smartwatches for children. Oslo: *Norwegian Consumer Council.*

[12]Walker, H. (2017). Terrified German parents urged to destroy doll 'that can spy on children. Daily Express. *London: Northern and Shell Media.*

[13]Wakefield, J. (2017). Germany bans children's smartwatches. BBC News. London: *British Broadcasting Corporation.*

[14]Hunt, T. (2017). Data from Connected CloudPets Teddy Bears Leaked and Ransomed, Exposing Kid's Voice Messages. *Troy Hunt.*

[15]Identity Verification in a Post-Breach World. (2017). House Committee on Energy and Commerce. Washington: *USA Government (testimony of Troy Hunt).*

[16]Knowles, B., Finney, J., Beck, S., et al. (2018). What children's imagined uses of the BBC micro: bit tells us about designing for their IoT privacy, security and safety. Living in the Internet of Things: *Cybersecurity of the IoT. London.*

[17]Masoud, M., Jaradat, Y., Manasrah, A., & Jannoud, I. (2019). Sensors of smart devices in the Internet of Everything (IoE) era: Big opportunities and massive doubts. *Journal of Sensors*, 2019;6514520, 26 pages. https://doi.org/10.1155/2019/6514520

[18]Egelman, S., Herrmann, M., Tripp, J., Haney, A., King, J., & Roesner, F. (2018). Security and privacy risks in internet of things toys. *Proceedings of the ACM Conference on Computer and Communications Security, pp. 835–847.*

[19]Kao, M. K., Sun, X., & Han, C. (2019). Children's smart toys: An investigation of security and privacy risks. *IEEE Pervasive Computing*, 18(2), 34–41.

[20]Hao, R. J., Chen, Y. H., & Chen, Y. T. (2020). IoT Toy Hack: Investigating the Security of IoT Toys for Children. *In Proceedings of the 2020 IEEE International Conference on Internet of Things (IoT) (pp. 1-5).*

[21]Al Hwaitat, A.K.; Almaiah, M.A.; Ali, A.; Al-Otaibi, S.; Shishakly, R.; Lutfi, A.; Alrawad, M. A New Blockchain-Based Authentication Framework for Secure IoT Networks. *Electronics*, 12(3618).

[22]Li, D., Peng, W., Deng, W., & Gai, F. (2018). A Blockchain-Based Authentication and Security Mechanism for IoT. In 2018 *27th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-6). Hangzhou, China: IEEE. DOI: 10.1109/ICCCN.2018.8487449.

[23]Kotel, S., Sbiaa, F., Kamoun, R. M., & Hamel, L. (2023). A Blockchain-based approach for secure IoT. *Procedia Computer Science*, 225.

[24]Eddy, A., Guillan, B. Z. A., Elias, E. K., Aniell, E., Simon, S. B., & Faisal, M. (2024). Blockchain-enhanced multi-factor authentication for securing IIoT. *International Journal of Electrical Engineering, Mathematics and Computer Science*, 1(3), 1-24. doi:10.62951/ijeemcs.v1i3.16

[25]M. Alanazi and M. Aborokbah, "Multifactor Authentication Approach on Internet of Things: Children's Toys," 2022 *2nd International Conference on Computing and Information Technology (ICCIT)*, Tabuk, Saudi Arabia, 2022, pp. 6-9

[26]Kaspersky, 2024. Smart toy vulnerabilities could let cybercriminals video chat with kids. [online] Available at: https://usa.kaspersky.com/about/press-releases/smart-toy-vulnerabilities-could-let-cybercriminals-video-chat-with-kids?srsltid=AfmBOoraBnsV3cSt7dnM09aAIXUTi17IV-_7eQuQO1doARq0i7PQ2J3a [Accessed 31 October 2024].

[27]P., V., & A., M. R. (2024). A Scalable, Secure, and Efficient Framework for Sharing Electronic Health Records Using Permissioned Blockchain Technology. *International Journal of Computational and Experimental Science and Engineering*, 10(4);827-834. https://doi.org/10.22399/ijcesen.535

[28]Prasada, P., & Prasad, D. S. (2024). Blockchain-Enhanced Machine Learning for Robust Detection of APT Injection Attacks in the Cyber-Physical Systems. *International Journal of Computational and Experimental Science and Engineering*, 10(4);799-810. https://doi.org/10.22399/ijcesen.539

[29]M, P., B, J., B, B., G, S., & S, P. (2024). Energy-efficient and location-aware IoT and WSN-based precision agricultural frameworks. *International Journal of Computational and Experimental Science and Engineering,* 10(4);585-591. https://doi.org/10.22399/ijcesen.480

[30]S, P. S., N. R., W. B., R, R. K., & S, K. (2024). Performance Evaluation of Predicting IoT Malicious Nodes Using Machine Learning Classification Algorithms. *International Journal of Computational and Experimental Science and Engineering,* 10(3);341-349. https://doi.org/10.22399/ijcesen.395

[31]S, P., & A, P. (2024). Secured Fog-Body-Torrent : A Hybrid Symmetric Cryptography with Multi-layer Feed Forward Networks Tuned Chaotic Maps for Physiological Data Transmission in Fog-BAN Environment. *International Journal of Computational and Experimental Science and Engineering,* 10(4);671-681. https://doi.org/10.22399/ijcesen.490