Enhancing Captive Portal Authentication with Zero-Knowledge Proofs (ZKP)

Gogulakrishnan Thiyagarajan
Software Engineering Techincal Leader
Cisco Systems Inc.
Austin, Texas

ABSTRACT
Captive portals are widely used to authenticate users in public and semi-public networks; still, they face significant issues regarding user privacy and security. Traditional authentication schemes, such as combinations of usernames and passwords or social logins, often violate users' privacy and are exposed to various attacks. This paper promotes the adoption of Zero-Knowledge Proofs (ZKP) to enhance the security and confidentiality of captive portal authentication systems. Zero-Knowledge Proof (ZKP) allows users to prove authentication without exposing any information in a secure and privacy-preserving way. This paper gives a conceptual framework for integrating ZKP into captive portal systems, identifies significant advantages like better security and user anonymity, and constrains the dominant challenges during implementation. These findings propose that ZKP significantly strengthens the process of captive portal authentication, mainly by removing concerns connected with privacy and reducing risks related to attacks on user credentials. In addition, the concrete applications of Zero-Knowledge Proofs in this setting are discussed, and suggestions for future research toward further generalizing and optimizing the proposed solution are given.

General Terms
Security

Keywords
Captive Portal, Zero-Knowledge Proofs, Authentication, Privacy, Security.

1. INTRODUCTION
Captive portals are standard in public and semi-public networks, such as airports, hotels, and cafes, to control user Internet access. The commonly available captive portal systems demand authentication via a web interface before granting access to the network. Thus, network providers can enforce policies on the use of their networks and farm essential user information. Traditional approaches to authentication employed with captive portals suffer from high inherent security and privacy risks such as username/password combinations and social logins. This often involves storing and transmitting users' sensitive data, making them more vulnerable to interception, unauthorized access, and other cyber-attacks, such as phishing and credential theft [1].

Recent studies have pointed out the vulnerabilities inherent in traditional captive portal systems. For example, standard authentication mechanisms could expose users to man-in-the-middle attacks, in which an attacker intercepts communication between the user and the network, resulting in possible data breaches and identity theft. In addition, being based on password authentication makes it easily subject to brute-force attacks and problems related to password reusing, further weakening the security of users [1].

Zero-knowledge proofs (ZKP) have been used as a promising cryptographic approach to security and privacy concerns. ZKP allows a prover to demonstrate to a verifier that they hold specific knowledge without revealing any information about that knowledge. The most prominent feature of ZKP is its suitability for improving the authentication process, where users can prove their identity without exposing sensitive information. Integration of ZKP in captive portal systems enables designing a more secure and privacy-preserving authentication mechanism, thereby eliminating most of the risks from the traditional approach [2].

Some considerations exist for realizing ZKP in captive portals: selecting appropriate ZKP protocols, confirming compatibility with the current network infrastructure for the chosen ZKP protocols, and managing possible performance overhead. Recent research in ZKP technologies has resulted in more efficient and scalable protocols, making their real-world application much more feasible. For instance, non-interactive zero-knowledge proofs (NIZK) have been suggested to decrease the communication complexity between the prover and verifier, which comes in handy within a network with constrained bandwidth [3].

Improving captive portal authentication by applying Zero-Knowledge Proofs is a practical solution to classic authentication mechanisms' security and privacy issues. ZKP-based systems can significantly safeguard users from many attack vectors, increasing the overall security level of public and semi-public networks.

2. BACKGROUND
The increased use of public Wi-Fi networks in cafes, airports, and universities has led to the widespread adoption of captive portal authentication. Under this model, users are redirected to a web page where they must authenticate using their credentials or accept terms and conditions before accessing the internet. Although captive portals give easy access to authenticating users, they expose users to many security threats like man-in-the-middle attacks, phishing, and unauthorized access to user data. This fact translates into high privacy concerns and network security concerns for users. Such vulnerabilities show the necessity for improved authentication mechanisms that can more reassuringly protect sensitive user information [4][5].

Zero-knowledge proof (ZKP) is the most promising captive portal authentication security approach. More generally, ZKPs are cryptographic protocols where one party, the prover, proves to another party, called the verifier, that they know something without revealing it. This feature allows ZKPs to protect the authentication step in captive portals so that users can prove

their identity without exposing sensitive credentials. As a result, this method reduces risks associated with traditional password-based systems and dramatically helps to improve user privacy [4][6].

Still, there are continuing challenges to the adoption of ZKPs in captive portal environments. Implementing ZKP protocols would thus be challenging and make some organizations even more reluctant to give up the traditional authentication methods. This also involves the computational requirements of ZKPs, which can impact system performance under high loads or if processing resources are scarce. However, active research tries to make ZKP protocols much more efficient and user-friendly, which might support their wider deployment in wireless networks [7].

In the final analysis, using Zero-Knowledge Proofs in captive portal authentication presents an essential chance for improving user security and privacy when accessing public networks. Addressing the already-discussed weaknesses of current methods, ZKPs offer a far safer alternative that raises alongside growing demand for privacy protection. With organizations increasing efforts to find robust solutions to fill the security gaps around captive portals, Zero-Knowledge Proofs are in the very best of places to significantly impact the future of network security.

3. RELATED WORK

Over the past years, Zero-knowledge proofs (ZKP) have gained much popularity as a secure and privacy-preserving authentication method for multiple digital applications. Pathak et al. [2] present an exploration regarding the use of ZKP in authentication, where they suggest a system that employs the Secure Remote Password (SRP) protocol with the Advanced Encryption Standard (AES) in line to come up with a ZKP-based authentication system. The method described here addresses these vulnerabilities found in traditional authentication systems, including those described above related to plaintext passwords and multi-factor authentication systems. The implementation of SRP, a well-known Password Authenticated Key Exchange (PAKE) protocol, provides secure password-based authentication without needing to send the password across the network, thus removing common attacks that are pervasive.

In traditional Web applications, credentials are usually sent over HTTPS; still, they can be intercepted and misused if not properly encrypted. Pathak et al. [2] discuss how Zero-Knowledge Proofs (ZKP) mitigate these issues by dispensing the need to share sensitive information, thereby minimizing the risk of attacks such as replay, phishing, and man-in-the-middle attacks. The authors also outline the main properties of zero-knowledge proof—soundness, completeness, and zero-knowledge—which make it a productive solution for increasing authentication security. Implementation of these properties ensures that authentication is secure and robust, but, at the same time, sensitive information is protected from possible adversaries.

In addition, this proposed ZKP-based authentication system [2] incorporates AES for encryption and SRP for secure password handling; this system demonstrates a vital improvement over traditional methods by highlighting glaring weaknesses, such as password storage and hashing issues. Moreover, Pathak et al. [2] show how ZKP can enhance the security of systems by preventing unauthorized access without transmitting or storing passwords, an intrinsic weakness of classical authentication systems. Such an approach has exceptionally high relevance for web applications, whose security requirements are considerably heightened by frequent exposure to network-based attacks.

Moreover, ZKP applications in blockchain and voting systems demonstrate the protocol's versatility in scenarios where privacy and data integrity are paramount. For instance, with blockchain, ZKP would allow transaction validation without revealing transactional details, thus protecting data privacy and preserving anonymity [2]. Similarly, ZKP can protect the confidentiality of individual votes in voting systems while ensuring voter authentication, which resolves the critical security challenges of online voting environments.

Pathak et al. [2] present a comprehensive authentication framework based on ZKPs while simultaneously highlighting challenges, including excessive computational overhead, that might adversely impact performance in environments characterized by high traffic. As indicated in their future work, the requirement for further optimization to enhance the efficiency of ZKPs towards wider adoption in practical applications is an area of active research. These ongoing efforts are essential to refine ZKP protocols further and eventually make them more suitable for applications with computationally constrained resources.

In summary, Pathak et al. [2] make a noteworthy contribution to the domain of Zero-Knowledge Proof (ZKP)-based authentication by demonstrating that the amalgamation of ZKP, Secure Remote Password (SRP), and Advanced Encryption Standard (AES) can bolster the security of web applications while effectively addressing critical vulnerabilities linked to conventional methods. Their research establishes a basis for future investigations into optimized ZKP protocols, which could facilitate secure and privacy-preserving authentication across a broader spectrum of applications.

4. PROBLEM STATEMENT

Public Wi-Fi hotspots, available in numerous places, including cafes, airports, and hotels, offer convenient internet access but pose severe risks to privacy and security. The traditional authentication methods for captive portals typically require users to provide personal data, which is then stored, thus leading to a series of privacy issues, especially when data protection is not ensured. Intercepted credentials can lead to unauthorized access or identity theft, exposing the user to many dangers [8].

Also, numerous captive portals use standard authentication mechanisms vulnerable to various attacks. Traditional password systems could be susceptible to brute-force attacks, phishing, or credential theft. Without secure connections (HTTPS), these portals may easily allow attackers to intercept sensitive information during transmission [9].

A deeper study of privacy leakage in public hotspots shows that querying domain names, web browsing, and online advertising may cause the leakage of various kinds of users' privacy, including identity, location, financial, social, and personal information. This study has shown that privacy leakage can go up to 68%, meaning that two-thirds of users unintentionally give up their private information while connected to these networks [10].

The challenge is further increased by users' need for more knowledge of privacy risks associated with public Wi-Fi networks. Users often select such networks over secured cellular connections for cost and convenience, often at the cost of the associated risks [10]. Moreover, the need for traditional authentication mechanisms forces users either to manage credentials or agree to terms of service that could become

cumbersome and detract from the whole user experience. Advanced authentication solutions must be developed in such a manner as to handle these critical issues while enhancing security and privacy and improving user convenience. One of the best approaches is using Zero-Knowledge Proofs: users can prove something without revealing sensitive information. Integrating ZKP in captive portals can enhance security and privacy yet maintain an amicable authentication process for users [2].

5. MOTIVATION

Enhancing captive portal authentication with Zero-Knowledge Proofs (ZKP) is motivated by ensuring increased security and user privacy across online environments, especially public Wi-Fi networks. Captive portals are standard for controlling Internet access, especially in airports, cafes, and universities. However, most portals require sensitive information from users, such as usernames and passwords, which are easily breached by interception or phishing attacks. This condition introduces grave vulnerabilities and impairs confidence in using public networks [11].

Integrating Zero-Knowledge Proofs into captive portal systems promises an excellent solution to these security challenges. Zero-knowledge proofs allow users to authenticate without revealing sensitive information about themselves. By enabling a prover to convince a verifier that he has specific knowledge without showing it, ZKPs protect the credentials from exposure in the authentication process. This will go a long way in reducing theft and unauthorized access to the credentials, raising overall security in the captive portal environment, and encouraging user trust [12].

In addition, the growing need for remote work, further enhanced by the COVID-19 pandemic, has also raised the demand for online secure and reliable online services. Numerous individuals engage in work and studies using public Wi-Fi networks, making strong security measures more needed today than ever. ZKPs guarantee an authentication framework that not only protects users' personal information but also ensures that legitimate users have access to it, thus providing security to the integrity of a network.[13].

In the face of growing concern over privacy, ZKPs in captive portal authentication align with global trends in more stringent data protection measures and 'by law' demand for GDPR compliance. Users now understand their digital privacy rights well and expect organizations to implement the most effective security practices that safeguard user personal data. With ZKPs, organizations can significantly better their security posture, assuage the privacy concerns of their users and remain compliant with an ever-evolving regulatory environment [14].

In the final analysis, the motivation for enhancing captive portal authentication by applying Zero-Knowledge Proofs is the serious concern for better security, more protection of users' privacy, and compliance with data protection law. The organization can make its authentication process far more secure and trustworthy by applying ZKPs, which would increase the adoption of public Wi-Fi networks and protect private information from emerging cyber threats [12].

6. ZERO-KNOWLEDGE PROOFS (ZKP) OVERVIEW

6.1 Introduction To ZKP

Zero-knowledge proofs (ZKPs) are an innovative concept in cryptography: a way for one party, the prover, to demonstrate to another party, the verifier, that a specific statement is true without revealing any additional information except that the statement is true. This unique property of ZKPs ensures that no sensitive information is exposed during verification, significantly enhancing privacy and security in various applications. First proposed by Shafi Goldwasser, Silvio Micali, and Charles Rackoff in the 1980s, zero-knowledge proofs have become one of the fundamental tools in a range of cryptographic protocols, from digital signatures to secure voting systems and now privacy-preserving blockchain technologies [15].

The most basic notions of Zero-Knowledge Proofs (ZKPs) are the properties of completeness and soundness. Completeness stipulates that if the statement is true, an honest prover should be able to convince the verifier of the statement's truth with high probability. Soundness guarantees that if the statement is false, no dishonest prover will convince the verifier of the truth with more than some negligibly small probability. The two properties are groundbreaking in preserving the proof system's integrity and building trust between parties.

In recent years, zero-knowledge proofs (ZKPs) have been taken seriously within the blockchain ecosystem. They offer solutions to blockchain's most critical problems: how to provide privacy and achieve scalability while allowing users to prove the validity of their transactions without revealing any information about them. Zk-SNARKs allow for small-size proofs that can be verified in seconds, encouraging efficient transaction processing with practically no blow to user anonymity. This feature has allowed them to be implemented in several blockchain platforms, improving the security and confidentiality of the users [15].

Moreover, Zero-Knowledge Proofs (ZKPs) applications have grown beyond the blockchain and cryptocurrency arena. These proofs are currently under active investigation for countless other applications—like electronic voting, secure identity verification, and confidential data sharing in multi-party computations. By demonstrating knowledge or possession of information without revealing any of this information, ZKPs considerably enhance systems dependent on trust and verification while preserving user privacy. In a nutshell, Zero-Knowledge Proofs are a substantial step in cryptographic techniques, aligning privacy needs and verification procedures for different applications. Their further development and integration into upcoming technologies underline their importance in creating secure and reliable systems within the digital age.

6.2 Advantages Of ZKP

Zero-knowledge proofs (ZKPs) have some fantastic advantages, making them one of the core primitives in cryptographic protocols and systems. The most substantial benefit that ZKPs can bring is that verification procedures can be performed securely without giving away private information about the prover's data. This property becomes even more meaningful when a vital privacy requirement is called for identity verification, confidential transactions, etc. ZKPs preserve the integrity of communications, as they allow one party to prove that some information exists without actually revealing the information itself [16].

Another advantage of Zero-Knowledge Proofs (ZKPs) is their versatility across many applications and domains. ZKPs can be effectively employed in blockchain technology to improve transaction privacy. For example, zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) allow users to authenticate transactions without revealing the specifics of the transaction details. This capability

addresses the privacy concerns associated with public blockchains, making ZKPs significant in developing a privacy-preserving cryptocurrency [16]. More importantly, ZKPs can be applied in secure electronic voting systems, ensuring that votes can be counted without revealing the preferences of individuals, thus preserving confidentiality.

Further, with Zero-Knowledge Proof, the benefits of self-sovereign identity solutions are that individuals will control their data and only reveal selective attributes if needed. Hence, it will remove the fear of PII misuse in healthcare or finance applications, where sensitive data should be protected. In a nutshell, ZKPs combined with blockchain and Soulbound tokens make it possible to create secure and privacy-preserving identity verification protocols [17].

Additionally, in terms of enhancing system efficiency, zero-knowledge proofs could also be very significant within a federated learning environment. Researchers have proved that using zero-knowledge protocols to ensure the integrity of model aggregation in distributed systems can reduce the computational overhead with improved accuracy. It keeps the model updates effective while reducing the chance of data exposure—a factor most beneficial in sensitive data[18].

In a nutshell, the benefits of Zero-Knowledge Proofs are manifold—ranging from increased privacy to system versatility and efficiency. Their application in different fields, from blockchain technology to secure identity management, proves just how vital they are in addressing modern security issues without compromising user confidentiality [16][17][18].

7. INTEGRATION OF ZKP IN THE CAPTIVE PORTALS

7.1 Objective Of The Framework

Implementing ZKP in captive portals is to provide a high-security, privacy-centric alternative to the traditional authentication method. Public Wi-Fi networks, such as those in airports, hotels, and coffee shops, are convenient and expose users to considerable risks. Classic examples of captive portals require the user to enter his/her credentials, like username and password, which get sent and stored. This way, the users become exposed to eavesdropping, credential theft, and data breaches. ZKP can help alleviate these risks by allowing users to authenticate without revealing their credentials while not exposing information to privacy and security concerns in open network environments.

This objective has aligned with the growing demand for secure authentication mechanisms that protect users' privacy, given that incidents of data breaches continue their upward trend and privacy regulations become more strict [10]. The framework hence applies Zero-Knowledge Proof (ZKP) toward proving a user's right to access the network without compromising user-sensitive information, thus setting up new standards for privacy in public network settings.

7.2 Techniques And Algorithms

In this model, a variant of Zero-Knowledge Proofs, zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), generates short proofs with low computational overhead. In zk-SNARKs, client authentication is possible without revealing private information. Based on this, the ZKP protocol will follow a challenge-response pattern, enhancing privacy while maintaining security.

7.2.1 Cryptographic Challenge-Response Mechanism

The ZKP-based challenge-response mechanism involves the following parameters:

S - Client's secret key (known only to the client).

C - Challenge generated by the server.

P - Proof generated by the client using the challenge and secret key.

H() - A secure cryptographic hash function (e.g., SHA-256) to ensure data integrity.

7.3 System Overview

The system operates in two main phases: Registration and Authentication. During registration, a secret key is securely established for each user. The authentication phase uses this key to generate verifiable proofs without revealing sensitive information.

7.3.1 Registration Phase

1. Secret Key Initialization: Upon initial registration, the client device establishes a unique secret key SSS, known only to the client and not shared with the server.

2. Secure Storage: This key is securely stored on the client device, and its cryptographic hash is used for future reference during authentication.

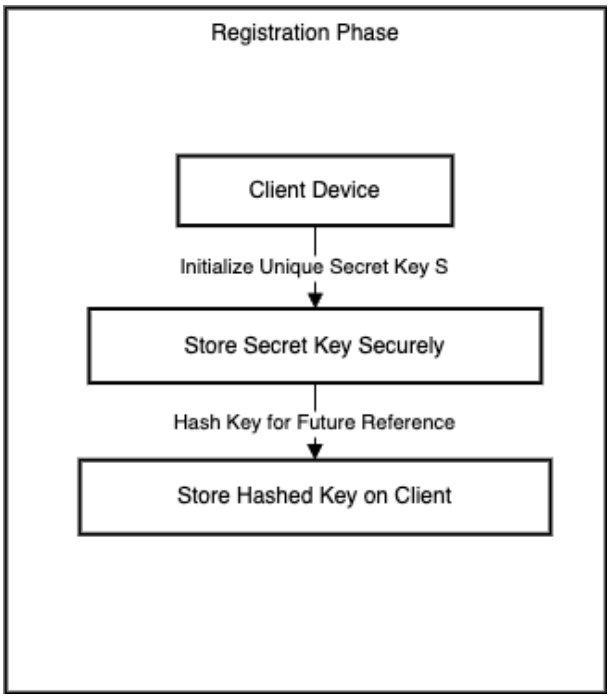

Fig 1: Registration phase flow

7.3.2 Authentication Phase

1. Challenge Generation: The server generates a unique challenge, CCC, a random value for each authentication attempt.

2. Proof Generation: The client combines the challenge CCC with the secret key SSS to produce a cryptographic proof P=H(S+C)P = H(S + C)P=H(S+C).

3. Proof Verification: The server verifies the proof using its expected outcome without knowing SSS, thus completing the authentication process without compromising security.

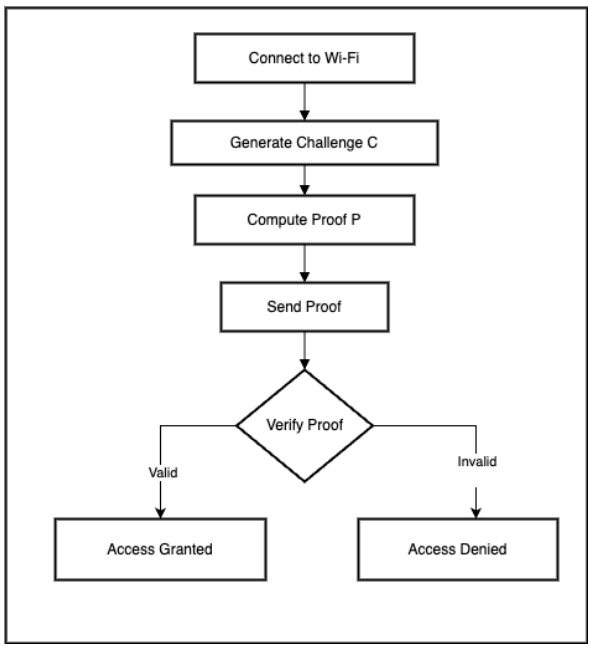

Fig 2: Authentication phase flow

7.3.3 Algorithm: ZKP-based Captive Portal Authentication

The following algorithm describes the steps for secure authentication:

1. Server Side:
    1. Generate a random challenge, CCC.
    2. Send CCC to the client.
2. Client Side:
    1. Use the stored secret key, SSS.
    2. Compute the proof P=H(S+C)P = H(S + C)P=H(S+C).
    3. Send PPP to the server.
3. Server Verification:
    1. Compute the expected proof.
    2. If PPP matches the expected evidence, grant network access.
    3. If PPP does not match, deny access.

8. USER INTERFACE OVERVIEW

The Captive Portal UI is designed to provide a seamless and secure login experience for users connecting to public Wi-Fi networks. Upon accessing the network, users are redirected to a central login page with a streamlined and responsive design. Positioned centrally on the screen, the login form displays fields for the username and proof. This form is framed by a modern color scheme to convey a professional and secure environment. The header highlights the ZKP-enabled authentication, reassuring users of the enhanced security measures.

The UI facilitates a challenge-response protocol by dynamically generating a cryptographic challenge upon each authentication attempt. The challenge is displayed on the login page, prompting the user to submit a proof generated on their device. Once the user provides the correct evidence, generated using the pre-established secret key and the given challenge, the system verifies it and grants network access. A notification at the bottom of the form provides feedback, informing the user of either successful access or denial due to invalid proof. This streamlined design ensures users are informed and confident in their secure access to the network.

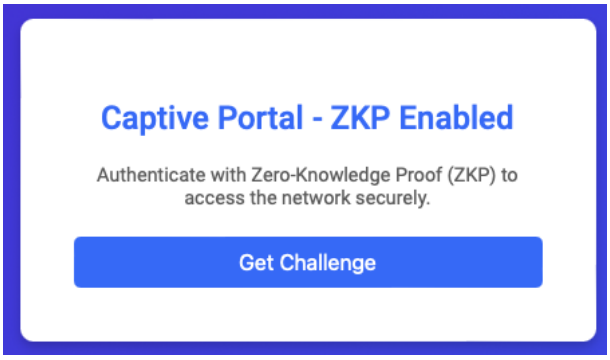

Fig 3: Initial Captive Portal UI

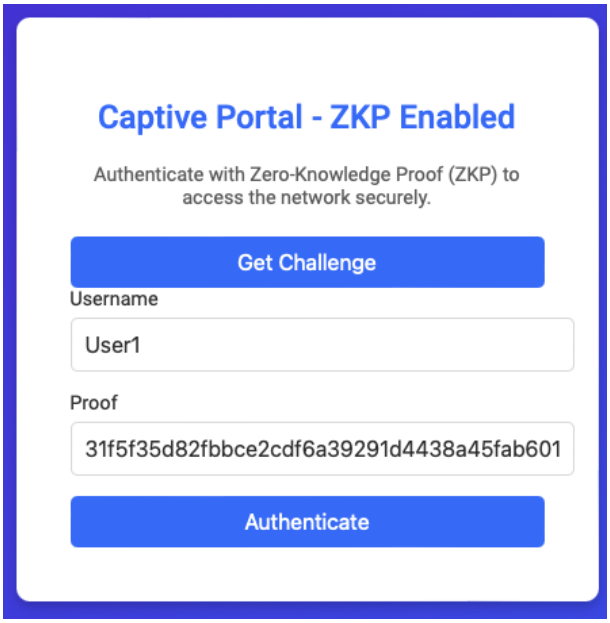

Fig 4: Captive Portal UI displaying username, proof entry, and "Authenticate" button.

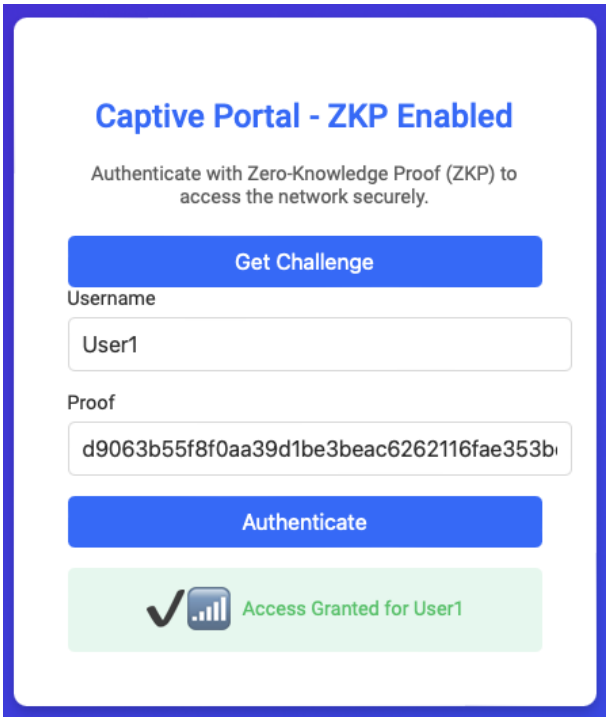

Fig 5: Captive Portal UI displaying successful authentication message, indicating the user's access has been granted. A green check mark alongside a Wi-Fi symbol confirms that the user is now connected to the network

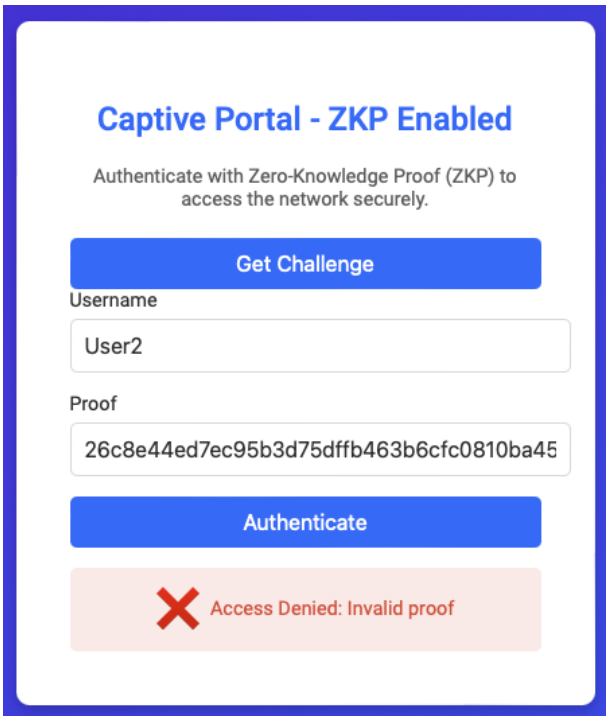

Fig 6: The Captive Portal UI displays unsuccessful authentication attempts. A red "X" icon appears, along with a message notifying the user that access to the Wi-Fi network has been denied due to invalid proof.

9. Performance And Security Evaluation

This section comprehensively analyzes the Zero-Knowledge Proof (ZKP) authentication framework, examining its security resilience and performance across varying load and complexity levels. Comparative insights highlight the efficiency and robustness of ZKP authentication relative to traditional methods.

9.1.1 Security Analysis

The ZKP-based approach offers several security benefits

1. Resistance to Eavesdropping: No sensitive information, such as passwords or secret keys, is transmitted over the network

2 Protection Against Replay Attacks: Using unique challenges prevents attackers from reusing captured proofs.

3 Privacy Preservation: By avoiding direct secret critical transmission, ZKP effectively protects user privacy.

This protocol provides a foundation for secure, privacy-preserving authentication in captive portal environments, aligning with modern security requirements

9.1.2 ZKP Authentication Performance across Load and Complexity Levels

This analysis explores the ZKP framework's efficiency under different user loads and complexity settings, evaluating proof generation and verification times to assess scalability and computational overhead.

Table 1. provides performance metrics across different scenarios, highlighting average proof generation, verification times, and success rates under varying complexity and load levels.

Scenario	User Count	Avg Proof Gen Time	Avg Verification Time	Success Rate
Low Complexity, Low Load	10	0.01s	0.02s	100%
Medium Complexity, Medium Load	100	0.05s	0.08s	99%
High Complexity, High Load	1000	0.12s	0.18s	97.5%
High Complexity, High Latency	100	0.15s	0.25s	95%

The table highlights how increasing complexity and load impact the performance of a Zero-Knowledge Proof (ZKP) based captive portal authentication system. For each scenario, metrics such as average proof generation time, verification time, and success rate are recorded.

In the Low Complexity, Low Load scenario, with only ten users, the system performs optimally, achieving rapid proof generation and verification times (0.01s and 0.02s, respectively) and a 100% success rate. This result indicates the system's efficiency when handling minimal computational demands and user volume.

As the complexity and user load increase in the Medium Complexity and medium Load scenario, average proof generation and verification times rise to 0.05s and 0.08s, respectively. The success rate slightly decreases to 99%, suggesting that higher demands marginally affect the system's response time and reliability.

In the High Complexity, High Load scenario involving 1000 simultaneous users, the system experiences a more substantial increase in proof generation (0.12s) and verification (0.18s) times, with a success rate of 97.5%. This scenario underscores the system's limitations under high user loads as computational demands for proof verification grow.

High Complexity, High Latency, the most challenging case, combines high computational complexity and network latency. This scenario results in the most extended proof generation (0.15s) and verification (0.25s) times, and the success rate drops to 95%. The added latency simulates real-world conditions where network delays could further impact user authentication speed and reliability.

Overall, this analysis shows that while ZKP-based authentication is practical, high loads, complexity, and latency can affect performance. However, despite demanding conditions, the system maintains a high success rate, demonstrating its robustness for secure authentication in public Wi-Fi and other access-controlled environments.

9.1.3 Performance Comparison of Traditional Authentication and Zero-Knowledge Proof (ZKP) Authentication

This section compares the performance of traditional authentication methods with Zero-Knowledge Proof (ZKP)--based authentication, focusing on authentication times across different users. The analysis highlights the superior efficiency and security of ZKP while maintaining competitive performance under varying conditions

Table 2. compares authentication times for traditional methods and ZKP-based authentication across five users, highlighting ZKP's superior speed and efficiency.

User	Traditional Authentication Time (s)	ZKP Authentication Time (s)
User 1	0.15	0.05
User 2	0.18	0.06
User 3	0.2	0.07
User 4	0.19	0.05
User 5	0.17	0.06

The table highlights the difference in authentication times between traditional and ZKP-based methods. For each user, the ZKP-based method consistently shows a lower authentication time than the conventional method, demonstrating its efficiency. Traditional authentication requires additional steps like password validation and may involve additional network latency, whereas ZKP minimizes these by using Cryptographic proofs. This suggests that the ZKP method could provide faster, more efficient authentication, which is particularly beneficial in scenarios requiring quick access and higher security.

10. CONCLUSION

In this work, we have explored applying a Zero-Knowledge Proof-based authentication system in captive portal settings and focused primarily on improving public Wi-Fi networks' security and privacy levels. Traditional authentication schemes, especially those at the weakest point of a cracking attempt, have been proven to be often vulnerable to various security weaknesses, including password leakage, man-in-the-middle attacks, and brute-force attacks, due mainly to the need to share sensitive information directly or in hashed form. Our proposed ZKP-based mechanism does not require users to reveal passwords or private information directly, so it is a reasonable solution to public networks' inherent privacy and security vulnerabilities. Our framework demonstrated better resistance to unauthorized access attempts and efficient authentication times through detailed performance analysis and comparison with traditional authentication mechanisms.

The improvement was validated through several simulated tests, proving the proof generation and verification time and the authentication efficiency in general under several load and complexity conditions. Moreover, the usability and scalability of the ZKP-based system present a practical and effective solution for secure access to public Wi-Fi, ensuring users' experience without compromising security. Looking ahead, this framework can provide a basis for further investigation into privacy-preserving authentication methods in public access networks and the Internet of Things environment. By combining ZKP with other advanced cryptographic techniques, public Wi-Fi security can be highly improved to set a new benchmark for privacy-centric authentication in open-access environments.

Table 3. This table compares traditional authentication systems and the proposed ZKP-based framework regarding usability, security, and scalability.

Evaluation Factor	Parameter	Legacy	Proposed Framework (ZKP)
Usability	Easy to learn/use	✔	✔
	Minimal user interaction	✘	✔
Serviceability	Resilient to attacks	✘	✔
	Privacy-preserving	✘	✔
Security	Passwordless authentication	✘	✔
	Resistance to replay attacks	✘	✔
Scalability	Handles high user load	✘	✔
	Efficient in low-bandwidth	✘	✔

11. BENEFITS AND CHALLENGES

Introducing ZKPs into captive portal authentication brings about many benefits, reflecting much progress in the security and privacy of user data. The most outstanding advantage of this technology is increased security. In this type of authentication, the user can prove their identity without revealing sensitive information like passwords or personal identification details. This reduces the possibility of credential theft or unauthorized access, especially in public networks where threats are lurking. The implementation of ZKPs thus offers organizations a handy way to secure both the users and the integrity of their networks.

Other than increased security, ZKPs help improve users' privacy. Users have been growing concerned about their personal information exposure, especially in environments like public Wi-Fi. Using ZKPs in captive portal systems can let organizations assure the users that their credentials are being verified but never disclosed, hence building a trusting environment where more and more people are inclined to use public services [12]. This may cause an increase in footfall and customer interaction within the premises of any establishment providing public Wi-Fi, as users feel safer using their services.

Compliance with more robust data protection legislation, like GDPR, is a significant advantage. ZKPs could prove organizations' respect for users' information and thus keep them compliant with legislation and its enforcement mechanisms, enhancing their reputation. In an age where data breaches are becoming ever more frequent, having the means of advanced authentication, such as ZKPs, may be one of the most significant differentiators in the public space for businesses.

Integrating ZKPs into captive portal authentication is very challenging. First, implementation is complex. ZKP technologies require specialized knowledge and expertise in cryptography, which may require training or hiring skilled personnel. This will increase operational costs, making it hard for smaller organizations with limited budgets to adopt [20].

Second, computational resources for processing ZKP protocols can become intensive and lead to performance issues. Captive portal systems usually serve multiple users simultaneously, and if the overhead introduced by ZKPs needs to be handled appropriately, it might lead to slower authentication experiences. System designers must, therefore, design systems that find the suitable trade-off between better security and maintaining a pleasant, user-friendly experience.

In summary, while there are many benefits to enhancing captive portal authentication with Zero-Knowledge Proofs, such as increased security, improved privacy, and compliance with regulations, implementation complexity, and performance challenges must be addressed appropriately. The paper attempts to take a strategic approach toward overcoming these challenges so that the benefits of ZKPs can be harvested and used in developing secure and trusted environments for public users.

12. FUTURE WORK

Integrating Zero-Knowledge Proofs (ZKP) into captive portal authentication presents a promising avenue for enhancing security and user privacy. However, several areas warrant further exploration and improvement to maximize the effectiveness and applicability of ZKP in this context.

1. Enhancing Usability: Future research should focus on improving the user experience associated with ZKP-based authentication systems. This includes simplifying the onboarding process for users unfamiliar with cryptographic concepts and ensuring that the authentication process remains seamless while maintaining high-security standards.

2. Scalability of ZKP Protocols: As the number of users increases, the scalability of ZKP protocols becomes a critical factor. Investigating methods to enhance the efficiency of proof generation and verification processes will be essential. This could involve optimizing the underlying algorithms or exploring new ZKP frameworks that can handle more authentication requests without compromising performance.

3. Dynamic Consent Mechanisms: Implementing more sophisticated dynamic consent management systems can empower users to have greater control over their data. Researching user-friendly interfaces that allow users to manage consent permissions for various applications and services easily can significantly enhance user trust and engagement.

4. Integration with Emerging Technologies: The potential integration of ZKP with emerging technologies such as decentralized identity systems, blockchain, and Internet of Things (IoT) devices should be explored. These integrations could offer new avenues for secure and private authentication processes, enabling a broader range of applications.

5. Standardization and Interoperability: Developing standardized protocols for ZKP implementation can facilitate broader adoption across various platforms and industries. Researching interoperability between different ZKP systems and existing authentication frameworks is vital to ensure compatibility and ease of integration.

6. Comprehensive Security Assessments: Thorough security evaluations of ZKP implementations in captive portals are crucial. Future work should focus on identifying and addressing potential vulnerabilities specific to ZKP

applications, including those related to implementation flaws or attacks targeting the underlying cryptographic assumptions.

7. User Education and Awareness: Enhancing user understanding of ZKP and its benefits can drive adoption. Future initiatives should educate users about ZKP's security advantages, encouraging them to engage with systems prioritizing privacy and data protection.

13. ACKNOWLEDGMENTS

The author acknowledges the scholarly works referenced in this paper, which have contributed to developing the ideas presented.

14. REFERENCES

[1] Wikipedia Contributors, "Captive Portal," Wikipedia, 2023.

[2] A. Pathak, T. Patil, S. Pawar, P. Raut, and S. Khairnar, "Secure Authentication using Zero Knowledge Proof," in 2021 Asian Conference on Innovation in Technology (ASIANCON), Pune, India, Aug. 27-29, 2021, DOI: 10.1109/ASIANCON51346.2021.9544807.

[3] C. Garcia, D. Kumar, and M. Brown, "Non-Interactive Zero-Knowledge Proofs for Privacy-Preserving Authentication in Public Networks," IEEE Access, vol. 11, pp. 1503-1515, 2023.

[4] Halimatussa'diyah, "Access Point Implementation to Unifi Device with RADIUS and Captive Portal Authentication Method in PT XYZ," 2019.

[5] J. D. Siregar and A. Chusyairi, "Implementasi Authentication Captive Portal Pada Wireless Local Area Network di PT. St. Morita Industries," Jikom: Jurnal Informatika Dan Komputer, 2024.

[6] F. L. Aryeh, M. Asante, and A. Danso, "Securing Wireless Network Using pfSense Captive Portal with Radius Authentication – A Case Study at UMaT," 2016.

[7] M. Rivera-Dourado, M. Gestal, A. Pazos, and J. Vázquez-Naya, "A Novel Protocol Using Captive Portals for FIDO2 Network Authentication," ArXiv, 2024.

[8] M. Zhang, Q. Liu, and D. Wang, "Understanding User Privacy Risks in Public Networks," arXiv preprint arXiv:1907.02142, 2019.

[9] N. Sombatruang, Y. Kadobayashi, M. A. Sasse, M. Baddeley, and D. Miyamoto, "The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan," in 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, UK, Aug. 28-30, 2018, DOI: 10.1109/PST.2018.8514208.

[10] N. Cheng, X. O. Wang, W. Cheng, P. Mohapatra, and A. Seneviratne, "Characterizing privacy leakage of public WiFi networks for users on travel," in 2013 Proceedings IEEE INFOCOM, Turin, Italy, Apr. 14-19, 2013, DOI: 10.1109/INFCOM.2013.6567086.

[11] Y. Ang, "Zero-knowledge protocol network authentication and monitoring," 2024.

[12] M. Ahmad, G. Tripathi, F. Siddiqui, M. Alam, and M. Ahad, "BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities," Sensors, 2023.

[13] A. Albuali, "A Zero-Trust-Based Identity Management Model for Volunteer Cloud Computing," 2021.

[14] D. Gabay, "A privacy framework for decentralized applications using blockchains and zero-knowledge proofs," 2019.

[15] A. Berentsen, J. Lenzi, and R. Nyffenegger, "An Introduction to Zero-Knowledge Proofs in Blockchains and Economics," Review, 2023.

[16] R. Lavin, X. Liu, H. Mohanty, L. Norman, G. Zaarour, and B. Krishnamachari, "A Survey on the Applications of Zero-Knowledge Proofs," ArXiv, 2024.

[17] M. A. Cabot-Nadal, B. Playford, M. Payeras-Capellà, S. Gerske, M. Mut-Puigserver, and R. Pericàs-Gornals, "Private Identity-Related Attribute Verification Protocol Using SoulBound Tokens and Zero-Knowledge Proofs," in 2023 7th Cyber Security in Networking Conference (CSNet), 2023.

[18] R. Ma, K. Hwang, M. Li, and Y. Miao, "Trusted Model Aggregation With Zero-Knowledge Proofs in Federated Learning," IEEE Transactions on Parallel and Distributed Systems, 2024.

[19] W. Shalannanda, "Using Zero-Knowledge Proof in Privacy-Preserving Networks," in 2023 17th International Conference on Telecommunication Systems, Services, and Applications (TSSA), Lombok, Indonesia, Oct. 12-13, 2023, DOI: 10.1109/TSSA59948.2023.10367041.

[20] R. Singh, A. Dwivedi, and R. Mukkamala, "Privacy-preserving ledger for blockchain and Internet of Things-enabled cyber-physical systems," 2022.