International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/56 Volume 11, Issue 6, November – December (2024)

RESEARCH ARTICLE

Mitigating Blockchain Endpoint Vulnerabilities: Conceptual Frameworks

Mohd Azeem Faizi Noor
Department of Computer Science, Jamia Millia Islamia, New Delhi, India.
azeemfaizif@gmail.com

Khurram Mustafa
Department of Computer Science, Jamia Millia Islamia, New Delhi, India.
kmustafa@jmi.ac.in

Received: 11 October 2024 / Revised: 12 December 2024 / Accepted: 17 December 2024 / Published: 30 December 2024

Abstract – Since the inception of Blockchain technology, attackers have consistently exploited vulnerabilities and enjoyed the money from attacks and heists. They have outpaced the users' defence mechanisms and targeted every possible way and trick to make a profit. There were numerous threats, namely double spending, Sybil attacks, phishing, block-related attacks, smart contract attacks, mining-related attacks etc. One such prominent threat is endpoint security which is identified as broken authentication, cryptographic failures, security misconfiguration, web security vulnerability and human vulnerabilities. The attackers find a relatively easy job to target the identified endpoint of the users to take complete control over the system and steal the sensitive information, resource abuse and credit the cryptocoin. Despite its significance, identified endpoint security has received limited attention, and users still lack robust frameworks or solutions. In this paper, a novel approach has been developed to manage the identified endpoint violation in blockchain applications. Overall, three different conceptual frameworks and abstract ideas were presented that aimed at mitigating the identified endpoint vulnerabilities and hence enhancing endpoint security. These conceptual frameworks were validated through Proof-of-Concept and Defence-in-Depth mechanisms. To illustrate the conceptual framework, a use case was provided. The first framework integrates two recent technologies: Blockchain and Remote Browser Isolation (RBI) that offer a secure and isolated environment for user requests. This framework solves web security vulnerabilities completely and broken authentication, cryptographic failures, security misconfiguration, and human vulnerabilities partially. The subsequent framework incorporates a Trusted Execution Environment (TEE) into the in previous framework that provides secure environments for cryptographic operations. Therefore, it solves broken authentication, cryptographic failures, security misconfiguration and web security vulnerabilities completely while solving human vulnerabilities partially. Finally, the use of steganography was proposed within the above framework to enhance security. This framework, though discussed only briefly and its nature is very complex; hides sensitive data and hence makes it harder to attack and solves broken authentication, cryptographic failures, security misconfiguration and web security vulnerabilities completely while solving human vulnerabilities partially. Conclusively, this paper introduces solutions to mitigate various endpoint vulnerabilities in blockchain applications and enables users to leverage blockchain technology more frequently, more easily and more hassle-free.

Index Terms – Endpoint Vulnerability, Blockchain, Defense in Depth Principle, Remote Browser Isolation, Trusted Execution Environment, Steganography.

1. INTRODUCTION

Blockchain endpoints are the bridge between users and the vast world of blockchain networks that play a critical role in enabling interaction [1]. It allows applications and users to connect to a blockchain network and perform actions. It includes computers, laptops, servers, smartphones, and various other interconnected devices within the network [2]. The vulnerabilities related to blockchain endpoint are termed as Endpoint vulnerabilities in a blockchain application that refer to weaknesses and potential points of exploitation at the user interface or interaction points of the system.

Despite the decentralized and secure nature of blockchain technology, endpoints such as user interfaces, APIs, and communication channels remain vulnerable to numerous security threats. These vulnerabilities can manifest in various forms that including wallet vulnerabilities, broken authentication, cryptographic failures, insecure storage of private keys, susceptibility to phishing attacks, cryptojacking, and inadequate encryption measures, all of which jeopardize users' digital assets [3]. Strategies like 2-factor Authentication (2FA), Multi-Signature (MultiSig), the use of hot and cold wallets, regular updates and patches, and encryption have been employed to mitigate the vulnerabilities [4], [5], [6], [7], [8], but these measures have often proven ineffective in fully preventing breaches. Moreover, to the best of current knowledge, no standard method, literature, or framework has been identified that specifically addresses endpoint vulnerabilities in blockchain applications, except for the work by [9].

To overcome these issues of endpoint vulnerabilities, collaboration of blockchain with Remote Browser Isolation (RBI) is recommended. RBI protects against malicious links or scripts, phishing, malicious content, scripts and payloads that are automatically identified and remedied and provides secure sessions for using blockchain applications [10], [11]. Even if the user system is compromised then also attacker cannot capture the credentials and cannot install the malicious code. Therefore, it protects the credential theft, insecure credential storage, wallet attacks, malware, cryptojacking etc. Overall, it provides a very safe way to ensure the endpoint protection.

The later framework includes the Trusted Execution Environment (TEE) with the previous framework that provides a secure environment for the user to enter the data into the blockchain network [12], [13] . The TEE adds a secure environment for cryptographic operations that gives protection to cryptographic failures and broken authentication more efficiently and protects against security misconfiguration, web security vulnerabilities and human-related vulnerabilities also. Overall, it adds slight complexity but provides another layer of protection.

To make the system more secure, the usage of steganography [14] was recommended, as it adds another layer of protection. The steganographic tool for Ethereum is Zephyrus [15]. However, this framework is full of complexity and not for hassle-free usage. By taking advantage of these frameworks, users will be able to save their crypto money, wallet and control it more efficiently. In other words, users can experience blockchain services without any discomposure. Figure 1 shows the brief introduction of the technologies discussed in this study.

A Proof-of-Concept (PoC) is used to test how effectively blockchain, RBI, TEEs, and steganography can work together to protect against endpoint vulnerabilities using a layered Defense-in-Depth (DiD) security strategy.

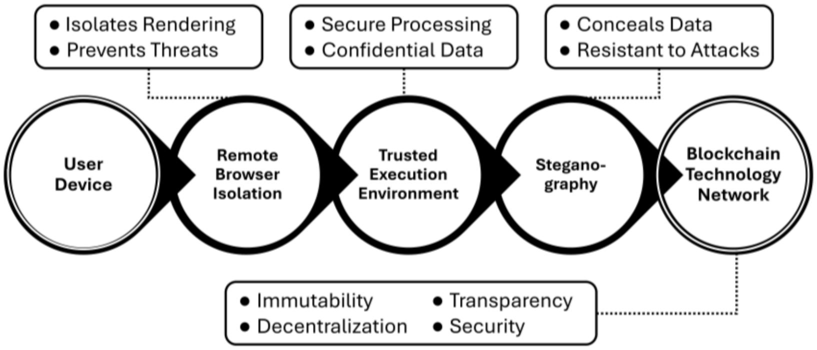


Figure 1 Brief Introduction of Key Security Technologies: Isolation, Trusted Execution, Steganography and Blockchain

1.1. Blockchain Endpoint Vulnerabilities

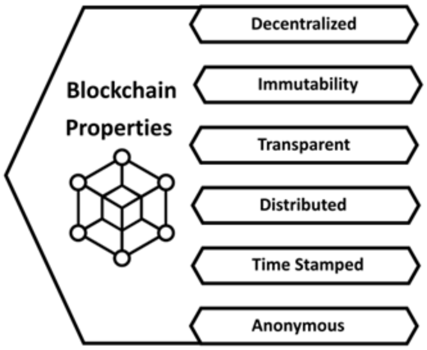


Figure 2 Blockchain Properties

Blockchain technology is designed to provide a secure and tamper-resistant way of recording transactions and is considered secure due to its decentralized and cryptographic nature [16] . It is the basis of cryptocurrencies such as Bitcoin [17], Ethereum [18] and various other applications beyond digital currencies such as supply chain, real estate, voting, healthcare, biometric applications identity registration, financial, energy system applications etc [1],[19], [20], [21], [22], [23], [24]. The prominent properties of blockchain technology are described in Figure 2.

However, despite these features and security, blockchain technology is not impervious to issues and vulnerabilities like 51% attacks, smart contract vulnerabilities, private key security, scalability challenges, regulatory compliance, interoperability, privacy concerns, mining-related issues, energy consumption, block-related issues, transaction malleability, double-spending etc [25], [26], [27] . One such problem that emerges at the point of interface between users and the blockchain network is endpoint vulnerability that presents varied challenges that go beyond the fundamentals of the technology [28], [29], [30]. From the risk of malicious software compromising private keys to the susceptibility of wallets to phishing attacks, endpoint vulnerabilities intertwine with issues of cryptojacking, insider job and malware [3], [31], [32], [33]. These various threats and attacks are possible due to the flaws at the different parts of the endpoint. In terms of wallet or any application, the threat at the data entered by users (For example: login) is termed as wallet-related attacks which can be grouped under broken authentication or cryptographic failures vulnerabilities. Similarly, installing the malicious script is a cryptojacking or malware threat which is grouped with web security and human vulnerability. So, following such analysis, the identified endpoint vulnerabilities are grouped into five different headings namely broken authentication, cryptographic failure, security misconfiguration, web security vulnerability and human-related vulnerabilities that encompass various possible threats and attacks which are comprehensively discussed in Table 1.

Table 1 A Comparative Overview of Endpoint Vulnerabilities

Vulnerabilities name	Reasons & Technique	Possible Attack/Threat	Adverse Effects	Example	Detection	Prevention
Broken Authentication	• Poor Password Management • Misconfiguration • Insecure credential storage • Inadequate session management • 2FA bypass • Blockchain node compromise	• Wallet Attack • Brute Force • Sybil Attacks • Eclipse Attacks	• System breach • Security breach • Unauthorized access • Unauthorized transactions • Loss of accounts, keys and cryptocoins • Session hijacking	• Inputs.io • Coincheck	• Multiple failed login attempts • Unusual login times or locations • Security Scanning Tools • Anomaly detection techniques	• Regular security audits • Multi-factor authentication • Trusted and secure cryptocurrency wallets • Regular patch code
Cryptographic failures	• Poor Password Management • Failure to update software • Collision and Preimage • Weak ECDSA randomness • Flawed Key Generation • Nonce reuse	• Double spending • Wallet Attack • Smart Contract Exploitation • Transaction malleability attacks • Signature forgery attacks	• Loss of key • Loss of cryptocoin • Loss of account • Data tampering • Loss of trust	• Picostocks	• Unexpected Behavior in Smart Contracts • login attempts or transactions consistently fail without clear explanations • Data appearing corrupted or functionality breaking unexpectedly • Excessive CPU or battery drain	• Regular security testing • Use secure crypto-graphic libraries • Trusted and secure cryptocurrency wallets • Multi-factor authentication

Vulnerabilities name	Reasons & Technique	Possible Attack/Threat	Adverse Effects	Example	Detection	Prevention
Security Misconfiguration	• Unpatched vulnerabilities • Default configuration • Unprotected files/directories • Use of vulnerable XML files • Vulnerable and outdated configuration • Weak access controls • Unnecessary services enabled	• Injection attack • DoS attack • MitM attack	• Unauthorized access • Data exposure • Unsecured Wallets • Blockchain forking	• BIPS	• Frequent error messages related to authentication, authorization • application crashes or instability	• Adjusting settings, user access and default file permission • Input validation • Grant least privilege • Configuration Review and Audits
Web Security Vulnerability	• Outdated Software • Weak password • Malicious link/email/website/phishing • Web advertising • Cross-site scripting • Embed crypto-mining JavaScript code • Insecure browsing habits • Disable security software • Keylogger • Public network like Wi-Fi	• Cryptojacking (web and host) • Malware	• Compromised Private Keys • Data Manipulation • Privacy breaches • Reputation Damage • Unauthorized Access	• US defense department website • UK government website • YouTube ads • Monero • Bitcash.cz	• Poor performance • Overheating • High electricity cost • CPU usage • Battery consumption	• Strong cybersecurity protocols • Use anti-cryptojacking browser extension • Use adblocker and disable JavaScript • Use secure channels to interact blockchain • double-check URLs • Verify the authenticity of the communication
Human vulnerabilities	• Human behavior & Negligence • Neglecting security protocols • Ignoring updated security practices (E.g., MFA) • Storing sensitive information in plain text • Lack of education and awareness • Insider job	• Social Engineering • Malware • Cryptojacking	• System Breach • Loss of wallet • Loss of cryptocoins • Abuse of computational resources • Access to confidential data including private keys	• Bitfloor • Bithumb • NiceHash • Bitfinex	• Falling Victim to Phishing Attempts • Increased Support Requests • Social Engineering Reports	• Educate the users about the approaches of social engineering fraud • Applying multi-level authentication • Avoid mishandling private keys •

Vulnerabilities name	Reasons & Technique	Possible Attack/Threat	Adverse Effects	Example	Detection	Prevention
	• Carelessness in Smart contract development • Exposure to phishing attack					

Table 1 shows that there are different types of endpoint vulnerabilities in blockchain applications. It includes broken authentication, cryptographic failures, security misconfigurations, web security vulnerabilities, and human factors. These vulnerabilities make blockchain services vulnerable to various attacks such as wallet attacks, double spending, smart contract exploits, injection attacks, cryptojacking, and social engineering. Effective mitigation methods are regular security audits, multi-factor authentication, use of secure cryptographic libraries, proper configuration management, strong cybersecurity protocols, and comprehensive user education.

From Table 1, it is evident that various vulnerabilities can lead to different threats and attacks. Given the primary concern for data safety during transmission to the blockchain network and the protection of sensitive data at the endpoint, it is recommended to secure the input channels and devices while entering data. Theoretically, RBI and TEE fulfil these criteria since these technologies provide a secure and isolated environment for entering data and preventing malicious scripts from running on the system. As a result, these technologies combined provide security to broken authentication, cryptographic failures, misconfiguration, web security vulnerability and human vulnerabilities effectively including protection against wallet attacks, insecure credential key storage, cryptojacking, malware and social engineering. Therefore, provides security to the accounts, keys, unauthorized access, cryptocoins, data tampering, trust, privacy and prevents the abuse of computational resources.

Conclusively, integrating RBI, TEEs and steganography can further enhance security of the blockchain services. These technologies add an extra layer of security by isolating browsing sessions and providing secure enclave for executing sensitive operations, respectively. Therefore, by combining these technologies, the resilience of blockchain applications against endpoint vulnerabilities can be substantially improved.

In the following section, the concepts of RBI and TEE are discussed, which are used in this paper. Very little literature on steganography has been provided in this study.

1.2. Remote Browser Isolation

It is a cybersecurity technology that isolates web browsing activity from a user's device and network. This task is accomplished by rendering web pages in a remote, controlled environment (e.g. cloud server) and then streaming the output to the user's device [34]. This isolation helps to protect users from malware, phishing attacks, and other threats. One notable feature of RBI is its ability to wipe out all browsing history, cookies, and session data after the session concludes and guarantees that no sensitive data, including private keys or login credentials used during blockchain interactions, is stored locally on the user's device. Still, unfortunately, if any harmful scripts or potential viruses are injected during the session, they will effectively be eliminated from the endpoint [35]. Figure 3 explains the working of RBI. Merging RBI with blockchain applications is indeed innovative, unique and holds various potential benefits which are illustrated in Figure 4.

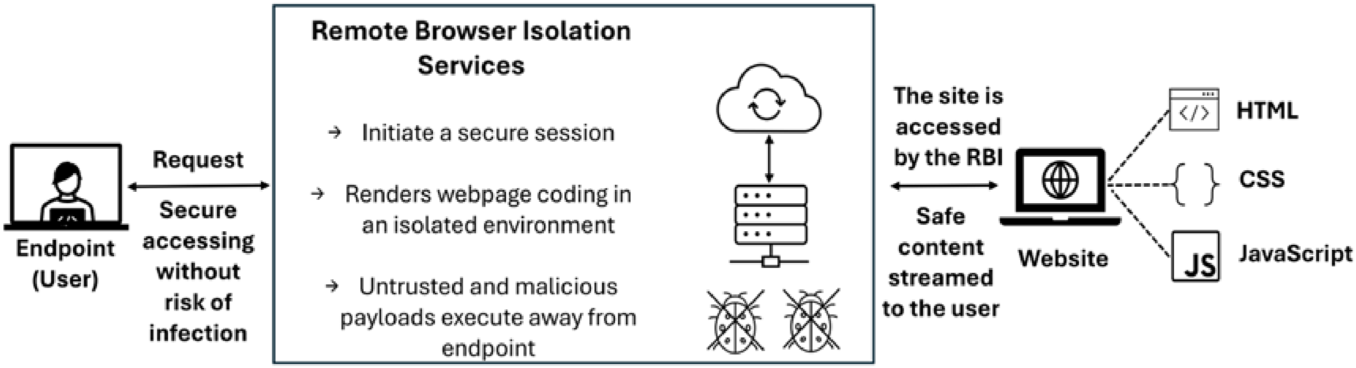
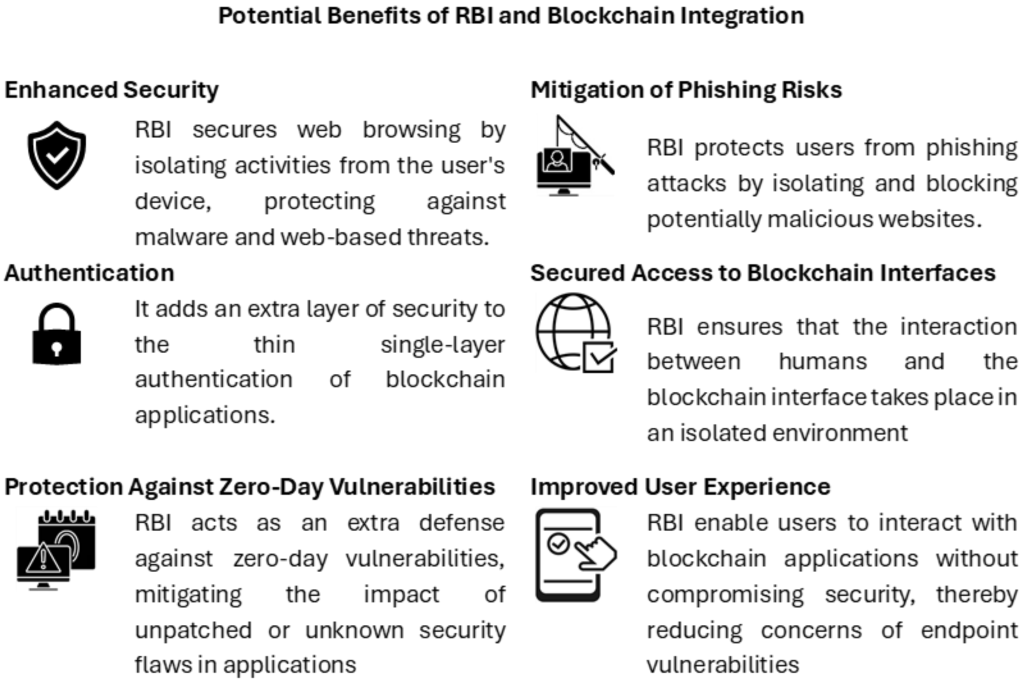

Endpoint (User)
Request
Secure accessing without risk of infection
Remote Browser Isolation Services
→ Initiate a secure session
→ Renders webpage coding in an isolated environment
→ Untrusted and malicious payloads execute away from endpoint
The site is accessed by the RBI
Safe content streamed to the user
Website
HTML
CSS
JavaScript
JS

Figure 3 RBI Working



Potential Benefits of RBI and Blockchain Integration

Enhanced Security

RBI secures web browsing by isolating activities from the user's device, protecting against malware and web-based threats.

Mitigation of Phishing Risks

RBI protects users from phishing attacks by isolating and blocking potentially malicious websites.

Authentication

It adds an extra layer of security to the thin single-layer authentication of blockchain applications.

Secured Access to Blockchain Interfaces

RBI ensures that the interaction between humans and the blockchain interface takes place in an isolated environment

Protection Against Zero-Day Vulnerabilities

RBI acts as an extra defense against zero-day vulnerabilities, mitigating the impact of unpatched or unknown security flaws in applications

Improved User Experience

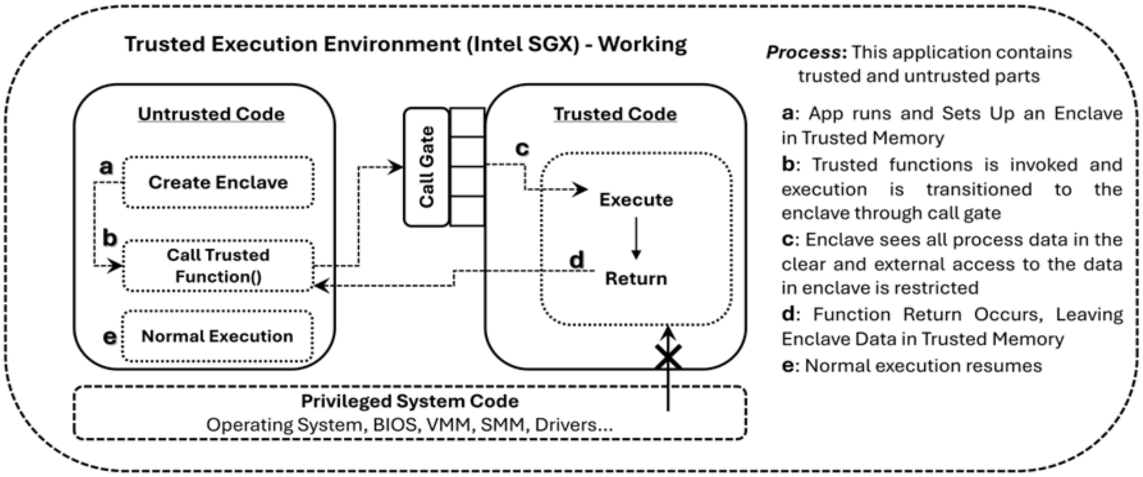
RBI enable users to interact with blockchain applications without compromising security, thereby reducing concerns of endpoint vulnerabilities

Figure 4 Potential Advantages of Merging RBI with Blockchain

1.3. Trusted Execution Environment (TEE)

It is a secure and isolated area within a computer system's hardware. It offers a reliable and tamper-resistant environment for performing sensitive tasks. It is installed as a separate component within the processor and makes sure that critical processes like authentication mechanisms, secure key storage and cryptographic operations, remain secure from external threats and unauthorized access. The TEE functions independently of the main operating system and executes in a secure enclave, thereby providing security assurances [9], [36].

Intel SGX (Software Guard Extensions), AMD SEV (Secure Encrypted Virtualization), ARM TrustZone, AWS Nitro Enclaves etc are various examples that implemented the TEE concepts. Other than AWS nitro enclaves, all implementations are hardware-based and provide better security than software-based TEEs [37]. Digital payments, password management, login authentication, identity management and blockchain applications are some of the usages of TEEs. It safeguards data even if BIOS and other system components are compromised. The working of a TEE (example: Intel SGX)[38] is as described in Figure 5.



Process: This application contains trusted and untrusted parts

a: App runs and Sets Up an Enclave in Trusted Memory

b: Trusted functions is invoked and execution is transitioned to the enclave through call gate

c: Enclave sees all process data in the clear and external access to the data in enclave is restricted

d: Function Return Occurs, Leaving Enclave Data in Trusted Memory

e: Normal execution resumes

Figure 5 TEE Working

Section 1 provided a prologue on blockchain endpoint vulnerabilities, RBI and TEE. Next, section 2 provides an overview of the solution presented by researchers and scholars. In Section 3, a detailed description of the proposed conceptual framework, including the PoC, DiD, and a use case, is presented. A related analysis and discussion are provided in Section 4. Section 5 presents limitations and Section 6 concludes the paper. It is worth noting that this paper addresses endpoint vulnerabilities in blockchain applications, which apply to any general use case without specifying a specific application.

2. RELATED LITERATURE

Various methodologies have been developed and proposed to address the various issues and threats of blockchain applications. Some of them have received great attention from the research community while some of them received little attention. Scalability issues, mining issues, incentive issues, and block fabrication issues have received various solutions and measurements. Endpoint vulnerabilities have received minimal attention. Thus, the most recognized work is done by [9]. They mentioned SGX-based TEE as a solution to endpoint vulnerabilities through the implementation of the security of eHealth auditing.

Although, many researchers have highlighted the existence of endpoint vulnerabilities in their literature. [1], [3], [29], [39], [40], [41], [42] highlighted that endpoint security continues to be a critical concern in blockchain technology.[32], [43] have provided a wide range of endpoint threats that include 51% attacks, Sybil attacks, vulnerabilities in personal key security, and malicious activities such as mining malware and cryptojacking. [28] and [33] have added more factors contributing to endpoint vulnerabilities that include flawed key generation, signature tools exposing users' private keys, and lack of awareness and knowledge. [28] along with [33] and [30], argue that endpoint vulnerabilities are exacerbated by various attack methods such as social engineering, phishing, and physical access to user wallets. These methods exploit human factors and physical security weaknesses, making them difficult to mitigate through technical means alone.

Thus, overall, a few works emphasize the solution of endpoint vulnerability but they are not enough to address it. The literature provided on endpoint vulnerabilities reveals that it has various components like wallet, malware, keys etc [16]. These components have been addressed with specific countermeasures and suggestions, like [44] suggested BlueWallet, [45] suggested a group key management (GKM) mechanism, [46] suggested two methods against brute force attacks on private keys, [33] suggested not to share wallet keys, [30] suggested multilevel authentication, [28] suggested HSM (hardware security models), [47] suggested a request for comments (RFC) 6979, [1] suggested biometric, [48] suggested steganography, [49] suggested knowledge awareness and [3] and [1] suggested using TEE. However, none of these resolved the endpoint vulnerability issue and the question remains as it was. Figure 6 presents a review of the current literature on endpoint vulnerabilities. Table 2 presents a glimpse of studies related to literature. Table 3 summarizes the types of endpoints vulnerabilities, and the countermeasures obtained respectively.

Previously, TEE has been employed for various purposes, such as facilitating off-chain transactions using TEEChain [50], implementing the proof-of-useful-work (PoUW) scheme using SGX [51], generating random numbers for the proof-of-luck (PoLK) consensus algorithm [52], enabling private smart contracts in ShadowEth [53], and resolving trust issues in the Airtnt scheme by using TEEs to calculate rent [54]. Similarly, RBI has been recognized as an enterprise security control [10], a network security protection system based on remote browser isolation technology [34], and an enhancement for endpoint security [55]. However, these technologies have not been previously utilized to mitigate endpoint security vulnerabilities within a comprehensive framework. This study aims at integrating TEEs and RBI with blockchain technology to address and mitigate endpoint security issues effectively.

Table 2 A Glimpse of Some Studies Related to Literature

Ref.	Description	Methodology	Advantages	Disadvantages
[16]	It identifies root causes, major challenges, and mitigation techniques for endpoint security risks. The study highlights the thin security layers, human errors, cryptojacking, and weak randomness in private key generation as critical causes of vulnerabilities.	Systematic Literature Review	comprehensive study addressing blockchain endpoints. Raises user and developer awareness about vulnerabilities.	Absence of experimental validation. Overlooking broader blockchain challenges like scalability and interoperability.

[44]	It provides an overview of the research area, assesses existing evidence, and quantifies research outcomes related to blockchain	Systematic mapping study	Provides a structured overview of the blockchain research landscape. Highlights areas that require further investigation, such as latency, scalability and usability.	The end-user experience, critical for wallets like Blue Wallet, is insufficiently explored. Minimal focus on wallet-specific vulnerabilities like private key management or user authentication.
[45]	It focuses on secure key handling for Bitcoin wallets and Introduces a Group Key Management (GKM) scheme for blockchain networks to manage keys	Review and Analysis. Proposes new framework GKM, utilizing a multi-layered architecture to enhance security	It offers protection against key compromise via a one-way cryptographic function. The proposed framework accommodates IoT environments, which often involve endpoints with varying privileges and security requirements	Computational overhead. If ‘root group’ is compromised, it could jeopardize the entire system.
[46]	The paper discusses detecting brute-force attacks on cryptocurrency wallets. Also, proposes modifications to the bitcoin protocol and smart contracts to mitigate vulnerabilities.	Protocol proposals ‘evidence transactions’ and developed smart contract-based rewards for reporting vulnerabilities	Novel detection mechanism. Use of smart contracts to reward users for reporting vulnerabilities	When collisions occur due to brute-force attacks, it is challenging to identify the legitimate owner of the public key. This creates ambiguity in distinguishing between attackers and victims.
[33]	Proposes a framework to systematically evaluate risks, explore associated threats, vulnerabilities, and propose countermeasures for sybil attacks and double spending.	Security Risk Management (SRM) domain model	Provides a structured SRM-based model applicable to various blockchain systems. Educates blockchain developers, practitioners, and stakeholders on specific risks and mitigation strategies.	Some countermeasures are conceptual and lack real-world implementation or validation. The paper highlights that key vulnerabilities exist
[30]	Introduce a security ontology framework, HealthOnt, which systematically identifies, assesses, and mitigates security threats for both traditional healthcare applications (THAs) and blockchain-based healthcare applications (BBHAs).	Systematic Literature Review. Ontology Development. Validation Case Study	Covers security risks in both traditional and blockchain-based healthcare systems. HealthOnt can be updated iteratively as new security threats or countermeasures emerge.	wallet keys or user authentication may be mishandled due to lack of awareness or weak security controls.

[47]	Investigates the impact of weak randomness in the Elliptic Curve Digital Signature Algorithm (ECDSA) used in Bitcoin. It affects private keys that allows attackers to recover them and steal bitcoin	Theoretical Analysis of ECDSA	The proof-of-concept attack illustrates the ease of compromising private keys when randomness is flawed. Best practices for generating secure random numbers are proposed	Does not analyse other digital signature schemes. ECDSA security relies heavily on the randomness.
[1]	blockchain limitations and vulnerabilities could compromise the e-voting process and emphasizes the need to carefully assess these risks before integrating blockchain into real-world democratic elections.	Literature review and comparative analysis approach	blockchain-based e-voting systems offers transparency, trust, security. Auditability and efficiency.	Lack of protection for private keys. Blockchain's reliance on user-managed credentials adds a human error factor, which could compromise security
[48]	It introduces an algorithm that embeds blockchain private keys into digital images using Discrete Wavelet Transform (DWT) and Spread Transform Dither Modulation (STDM) methods to improve security and protecting from unauthorized access	Watermark and steganography	It offers enhanced security, robustness transparency and efficiency. Humans cannot perceive changes in the carrier image after embedding.	The robustness is only maintained in controlled environments. Altering image resolution, compression, or format could interfere with key recovery.
[49]	It examines the vulnerability of Bitcoin users to key leakage, both explicit and implicit, which can lead to cryptocurrency theft.	Investigation and Analysis	Practical implications. Step-by-step breakdown of the attack vectors. Discussions on ethical considerations and recommendations for countermeasures.	The study is limited to Bitcoin. The results rely on publicly available data. Nonce reuse. Pastebin dependency
[3]	It explores the application of blockchain technology in healthcare that emphasize its potential to enhance data security, privacy, and interoperability. It reviews the evolution of blockchain (from versions 1.0 to 5.0)	Literature Review and Case Study.	Homomorphic encryption and zero-knowledge proofs protect sensitive health information.	TEE implementation challenges and high costs. Vulnerabilities like endpoint attacks, key mismanagement, and consensus mechanism exploits remain concerns.

Table 3 Endpoint Vulnerabilities and Suggested Mitigations

Endpoint Vulnerabilities	Mitigations/ Suggestions
Broken Authentication	BlueWallet, Biometric, Multi-level authentication, modification in consensus, create reward transaction
Cryptographic failures	Group Key Management, Image hiding
Security Misconfiguration	RFC6979, Hardware Security Model, Multi-factor Authentication, Disable JavaScript

Endpoint Vulnerabilities	Mitigations/ Suggestions
Web Security Vulnerability	Hardware Security Model, TEE, Various Browser Extension
Human vulnerabilities	Awareness, not to share wallet keys

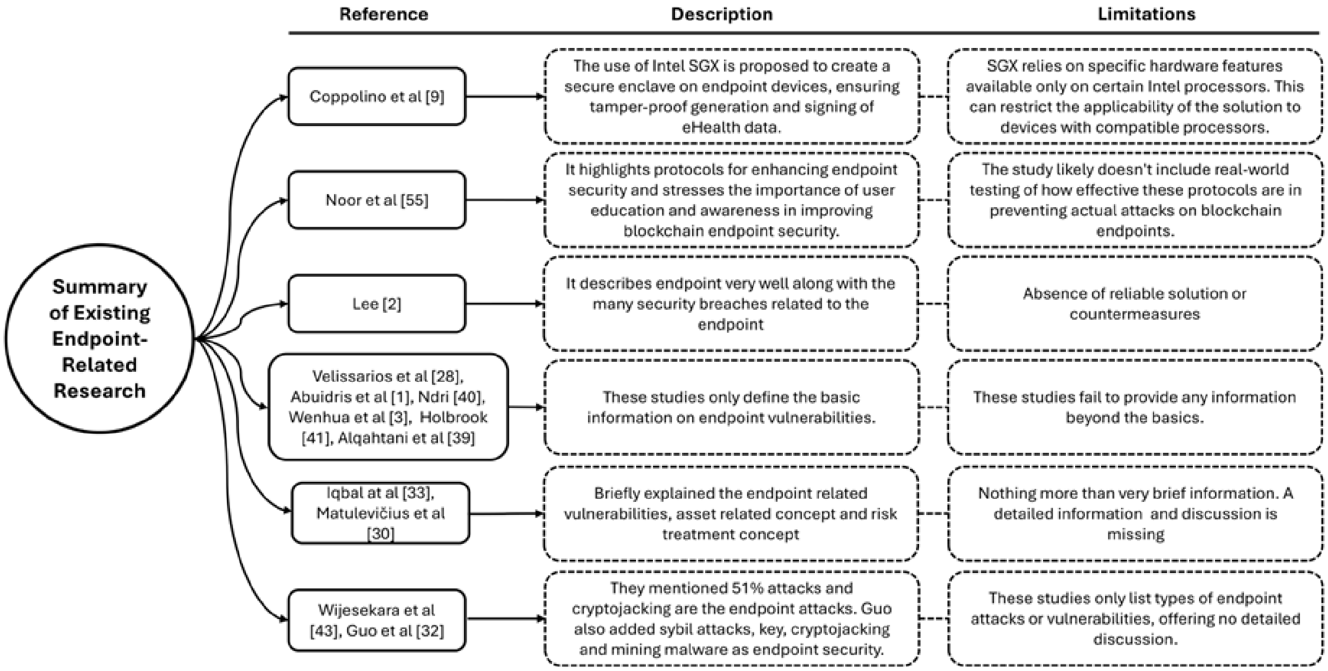

Reference
Description
Limitations
Summary of Existing Endpoint-Related Research
Coppolino et al [9]
The use of Intel SGX is proposed to create a secure enclave on endpoint devices, ensuring tamper-proof generation and signing of eHealth data.
SGX relies on specific hardware features available only on certain Intel processors. This can restrict the applicability of the solution to devices with compatible processors.
Noor et al [55]
It highlights protocols for enhancing endpoint security and stresses the importance of user education and awareness in improving blockchain endpoint security.
The study likely doesn't include real-world testing of how effective these protocols are in preventing actual attacks on blockchain endpoints.
Lee [2]
It describes endpoint very well along with the many security breaches related to the endpoint
Absence of reliable solution or countermeasures
Velissarios et al [28], Abuidris et al [1], Ndri [40], Wenhua et al [3], Holbrook [41], Alqahtani et al [39]
These studies only define the basic information on endpoint vulnerabilities.
These studies fail to provide any information beyond the basics.
Iqbal at al [33], Matulevičius et al [30]
Briefly explained the endpoint related vulnerabilities, asset related concept and risk treatment concept
Nothing more than very brief information. A detailed information and discussion is missing
Wijesekara et al [43], Guo et al [32]
They mentioned 51% attacks and cryptojacking are the endpoint attacks. Guo also added sybil attacks, key, cryptojacking and mining malware as endpoint security.
These studies only list types of endpoint attacks or vulnerabilities, offering no detailed discussion.

Figure 6 A Summary of the Existing Literature on Endpoint Vulnerabilities

3. THE PROPOSED CONCEPTUAL FRAMEWORKS

A conceptual framework is a network of interconnected concepts that together offer a thorough understanding of a phenomenon or phenomena [56]. Conceptual frameworks are the outcomes of qualitative processes of theorization where each concept supports one another, articulates their phenomena and establishes an understanding [56]. It facilitates efficiency, consistency, rapid development, security, and reduces both time and costs. This paper provides a new conceptual framework that combines the concepts of blockchain, RBI, TEE and steganography to mitigate the endpoint vulnerabilities in blockchain applications.

The proposed conceptual framework can be validated through the Proof-of-Concept (PoC) which is a theoretical determination of an idea that can be transformed into reality. So, it is a realization of specific ideas, principles or methods to demonstrate their feasibility or viability to verify that these ideas, principles or methods have practical implementation. Several PoC methods can be used to assess the conceptual framework such as Law of Averages, Principles of Security, Mathematical Proof, Contradiction, Geometrical Proof, Existential Proof and Defense-in-Depth (DiD). Among these, DiD is a particularly suitable strategy to be used to validate the theoretical framework because it perfectly matches the proposed scenario. DiD is one of the 12 principles of security that uses multilayered and multiple security measurements and practices to safeguard the network, web properties and resources. The proposed frameworks combine Blockchain RBI, TEE and Steganography and each offers unique strengths that collectively create robust security measurements and help in mitigating the endpoint vulnerabilities.

3.1. Defense in Depth Principle: A Multi-Layered Security

Defence in depth is a security concept where multiple layers of security controls are implemented to protect valuable data and information. By combining the above technologies, a robust and layered defence can be achieved, which is shown in Figure 7.

- Layer 1: Remote Browser Isolation (RBI)

User interacts with a dApps content within a secure, isolated environment that runs remotely, thereby providing security against malicious content from reaching the users' device. Also, it protects the endpoint and network from web-based threats, such as phishing, cryptojacking, and malicious scripts.

- Layer 2: Trusted Execution Environment (TEE)

It executes critical cryptographic operations and manages sensitive information in a secured environment that protects cryptographic keys, and authentication processes from tampering and exposure to external threats.

- Layer 3: Steganography

This technique is employed to embed sensitive information to obscure the presence of data which acts as an additional security measure which makes it more difficult for the attackers to identify and extract sensitive information. It prevents unauthorized access and detection.

- Layer 4: Blockchain Technology

This distributed technology stores transactions permanently and is tamper-resistant ensuring integrity, traceability and immutability.

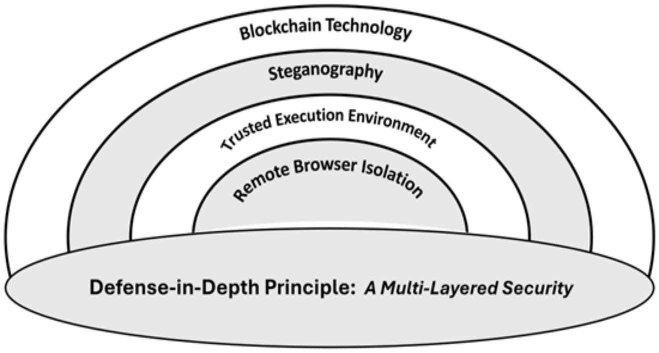

Blockchain Technology
Steganography
Trusted Execution Environment
Remote Browser Isolation
Defense-in-Depth Principle: A Multi-Layered Security

Figure 7 Defense-in-Depth Principle: A Multi-Layered Approach

By combining blockchain, remote browser isolation, TEE and steganography, a robust defence-in-depth layered strategy can be implemented to mitigate the endpoint vulnerabilities which makes it more challenging for attackers to compromise the system and endpoints.

The next section introduces three conceptual frameworks based on DiD. Framework 1 covers the figure, process, data flow, and minimum system requirements for implementation, along with a discussion on how it will mitigate endpoint vulnerabilities. A use case has been given as an example. Framework 2 provides the figure, process, data flow, and minimum system requirements for implementation. Framework 3 has limited discussion due to its extreme complex nature. Section 4 explains an analysis of how these frameworks will impact or mitigate endpoint vulnerabilities.

3.2. Need of the Proposed Model

The proposed model integrating blockchain technology with RBI and TEE that theoretically addresses the critical endpoint vulnerabilities in a dApps. The threat of endpoint exploitation increases with the adoption and usage. The lack of technical knowledge, unawareness and unusual behaviour leads to the endpoint exploitation. In these cases, traditional security measures fail to provide adequate protection, and attackers get benefitted through installing malicious code, hack security keys, phishing, abuse the computational resources etc. By integrating RBI with the blockchain technology, model creates a secure and isolated environment that ensures that blockchain transactions are executed within a tightly controlled, secure environment, preventing malware infiltration, reducing attack surfaces, providing real-time threat monitoring and separates user interactions from potential threat vectors. Thus, it will secure the user endpoint interaction. This innovative approach not only ensures data confidentiality and integrity but also strengthens user trust in blockchain systems. Figure 8 illustrates comparison of traditional dApps endpoint with RBI-enhanced dApps endpoint.

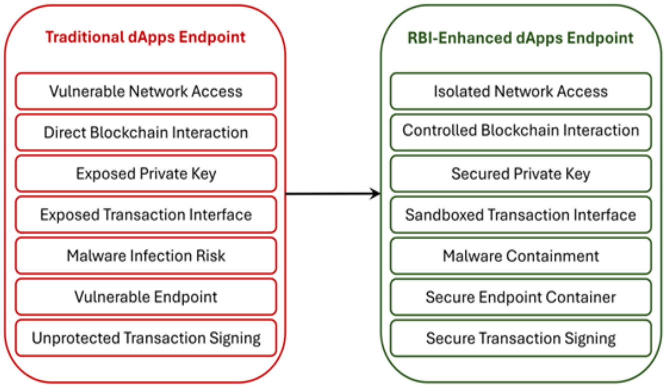

Traditional dApps Endpoint
Vulnerable Network Access
Direct Blockchain Interaction
Exposed Private Key
Exposed Transaction Interface
Malware Infection Risk
Vulnerable Endpoint
Unprotected Transaction Signing
RBI-Enhanced dApps Endpoint
Isolated Network Access
Controlled Blockchain Interaction
Secured Private Key
Sandboxed Transaction Interface
Malware Containment
Secure Endpoint Container
Secure Transaction Signing

Figure 8 Solutions Offered by RBI-Enhanced dApps Endpoint

3.3. Conceptual Framework 1 (Merging RBI with Blockchain Technology)

Figure 9 illustrates Conceptual Framework 1, where RBI is integrated with blockchain technology. RBI provides three basic facilities: cloud, on-premises and client side. These services separate web content from the user's device to reduce its attack surface [57]. When a user navigates to a webpage, the server renders all the HTML, JavaScript, and other web components necessary to build the Document Object Model (DOM) within a secure, isolated sandbox environment. There are three types of rendering: Pixel, DOM, and Streaming media. Pixel rendering is ideal because it provides high security and no rendering of web pages. DOM is a medium risk by rendering less risky elements while streaming media renders risky web pages. So, the latter is good for low risk

[58]. After rendering, the server converts the output into a safe interactive media stream. This stream can include HTML elements, images, texts, and user interface components, which are transmitted to the user's local browser [59].

3.3.1. Blockchain Environment

To create it, first install Node.js and npm (Node Package Manager), truffle framework (development framework for Ethereum), and Ganache (deploy applications and run tests). After installing, create a project using truffle, and connect truffle to ganache. Ganache will create a local blockchain and provide a list of accounts with private keys. Now create smart contracts in the contracts directory using solidity language (truffle) [60]. Then, compile and deploy contracts. Now install Web3.js, a library, which allows users to interact with the Ethereum blockchain as front end. Finally, install MetaMask as a browser extension from the MetaMask website and then connect MetaMask to the Ganache local blockchain and now interact with the blockchain services [61, 62].

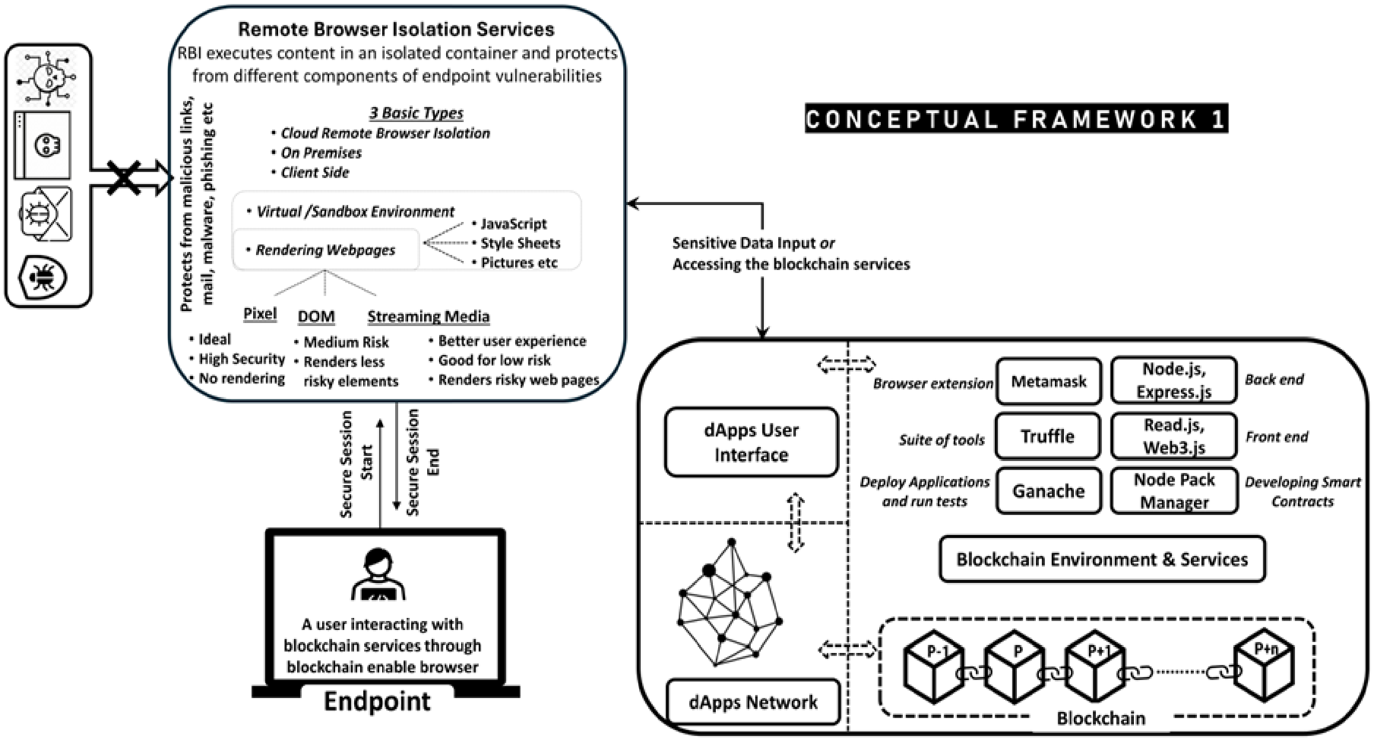

Remote Browser Isolation Services
RBI executes content in an isolated container and protects from different components of endpoint vulnerabilities
Protects from malicious links, mail, malware, phishing etc
3 Basic Types
• Cloud Remote Browser Isolation
• On Premises
• Client Side
• Virtual /Sandbox Environment
• Rendering Webpages
• JavaScript
• Style Sheets
• Pictures etc
Pixel
DOM
Streaming Media
• Ideal
• High Security
• No rendering
• Medium Risk
• Renders less risky elements
• Better user experience
• Good for low risk
• Renders risky web pages
CONCEPTUAL FRAMEWORK 1
Sensitive Data Input or Accessing the blockchain services
Secure Session Start
Secure Session End
A user interacting with blockchain services through blockchain enable browser
Endpoint
dApps User Interface
Browser extension
Metamask
Node.js, Express.js
Back end
Suite of tools
Truffle
Read.js, Web3.js
Front end
Deploy Applications and run tests
Ganache
Node Pack Manager
Developing Smart Contracts
Blockchain Environment & Services
dApps Network
P-1
P
P+1
P+n
Blockchain

Figure 9 Conceptual Framework 1: Merging RBI with Blockchain Technology

3.3.2. Process

This section introduces the overall step of the flow of actions. In subsequent paragraphs, RBI and creating a blockchain environment will be introduced in more detail. Later, it will be discussed how RBI provides security to the endpoint of blockchain applications.

Initially, a user initiates a transaction request from their system through blockchain enable browser or specific applications. Then, the request is executed under the secure and isolated environment of RBI with a new session. Next, the request is connected to the blockchain network. The blockchain environment consists of various mini frameworks like Truffle, Metamask, Ganache, Node.js, Read.js, Node Pack Manager etc. These dependencies work together to provide a blockchain environment and services. The user accesses to the services of blockchain under the RBI environment. After completing, RBI closes the session and the link is terminated.

3.3.3. Dataflow Overview

Figure 9 shows the location of RBI services, dApps interface and blockchain services. When a new request is initiated, e.g., a user enters their login details or user enters the data on the blockchain network, then the request is acknowledged by RBI by initiating a secure session and executing the request in a secure location. RBI types provide different facilities depending on the user requirements and security. Now, users are able to access the blockchain services, executing smart contracts, performing transactions etc. in a remote and isolated environment provided by the RBI services that ensure the integrity and confidentiality of the data being transmitted. The activities are recorded on a distributed ledger which is tamper-proof and verifiable by all participating nodes.

Finally, the user sends a request for session termination by logging out of the blockchain application. Then, the RBI server sends a logout request to the blockchain application on behalf of the user and closes the connection to the blockchain network, leaving no operations hanging. Later, the RBI server clears all files, data and sessions ensuring no residual is left behind. The corresponding minimum system requirement is shown in Table 4.

Table 4 Minimum System Requirements for Conceptual Framework 1 (RBI+ Blockchain Technology)

System Requirements		
Component	Minimum Requirement	Remarks
OS	Ubuntu 20.04 LTS	Ubuntu preferred over Windows due to better support
RAM	8 GB	For basic development and tastings.
CPU	Quad-core Intel i5 or AMD Ryzen 5	Multi-core processor for handling complex computations
Storage	100 GB SSD	For fast read and write speeds.
Graphics Card	Integrated Graphics	For basic implementations integrated graphics are sufficient.
Blockchain Platform	Ethereum, Hyperledger Fabric	For smart contracts and dApps
RBI Tools	Selenium, OWASP ZAP, JsSandbox	To develop browser automation and isolation
Development Frameworks	Truffle Suite, Hardhat, npm, Ganache	To develop blockchain environment

3.4. How RBI Provides Security to the Endpoint

- RBI executes all web content including HTML, JavaScript, and other scripts, on a remote server that prevents any malicious script from running on the user's device. Hence, reducing the risk of malware infections or exploitation of vulnerabilities in the browser.
- Users can enter sensitive information in a secure and isolated environment and attackers cannot reach them. RBI ensures that sensitive data entered by the user, such as private keys or login credentials for blockchain applications, never directly interacts with potentially compromised web pages. The interaction happens within the isolated environment, keeping the data secure. By providing a secure and controlled interface for transaction signing, RBI reduces the risk of user errors leading to financial loss.
- RBI operates within a secure isolated sandbox environment, and any malicious script contained within this sandbox cannot affect the server itself or reach the user's device.
- Because of the session, RBI can prevent phishing attacks that attempt to steal credentials or sensitive information. It can also detect and block phishing attempts before they reach the user, because the remote server manages all interactions with the web.
- By executing all browser code remotely, RBI eliminates the threat of malware that attempts to intercept and manipulate web transactions on the user's device. Hence, it solves the keylogger and cryptojacking problem as well.
- Suspicious sites and content are blocked before the user can interact with them, protecting users from accidentally disclosing their private keys, passwords, or other sensitive information.
- Human negligence often leads to falling for phishing scams, where users unwittingly provide sensitive information to fraudulent sites. RBI helps prevent this by isolating the web content and analysing it for phishing indicators in real time. RBI solutions often include features that educate users about safe web practices. For instance, if a user attempts to access a malicious site, RBI can display a warning and explain the potential risks. These notifications help raise awareness and encourage users to adopt safer browsing habits.
- Users may accidentally download malicious files that could compromise their systems or blockchain wallets. RBI intercepts downloading and scans them for malicious content before allowing the user to access them. Hence, keeps the system safe.
- This process prevents users from unintentionally executing harmful files that could lead to security breaches. By consistently reinforcing secure browsing practices, users become more aware of security risks and are less likely to engage in negligent behaviours.

RBI effectively addresses endpoint vulnerabilities in blockchain applications by isolating web interactions on remote servers. By executing web content in secure sandboxes, RBI prevents malware, phishing, and browser exploits from compromising local environments. This approach ensures secure handling of credentials, blocks malicious downloads, and educates users about safe web practices. RBI's proactive measures significantly reduce the risk of human errors in transaction signing and other critical activities, thereby providing a robust defence against a wide range of web-based threats and enhancing overall endpoint security for blockchain applications.

3.5. Use case: Online Student Registration for an Exam in a University Information System

In connection with RBI merging with the blockchain technology framework, a use case titled "Online Student Registration for an Exam in a University Information System" was conducted to illustrate the connection among technologies, flow of the data, error handling and working of the entities. There are mainly 4 components, namely dApps, RBI, blockchain technology and student as user. The flow of data is shown in Figure 10 through the numeric, error handling through the dashed line and the dotted line shows the flow chart of the different states of the exam registration process which is an integrated part of the dApps.

A student initiates the registration process through the dApps interface which enables RBI rendering automatically through a request. The student interacts with the dApps and complete the process which is shown in a dotted rectangle in Figure 10. Its process starts with the available selection of subject and date then enrolment. After enrolment, the student has the option to cancel their enrolment or to proceed further, attend the exam and complete the process. All this information gets hashed and is saved to the blockchain permanently providing data integrity and security.

This use case design is free from phishing attacks, malware, and unauthorized access issues, which significantly reduces the impact of the risk of users falling victim to various endpoint vulnerabilities in blockchain applications.

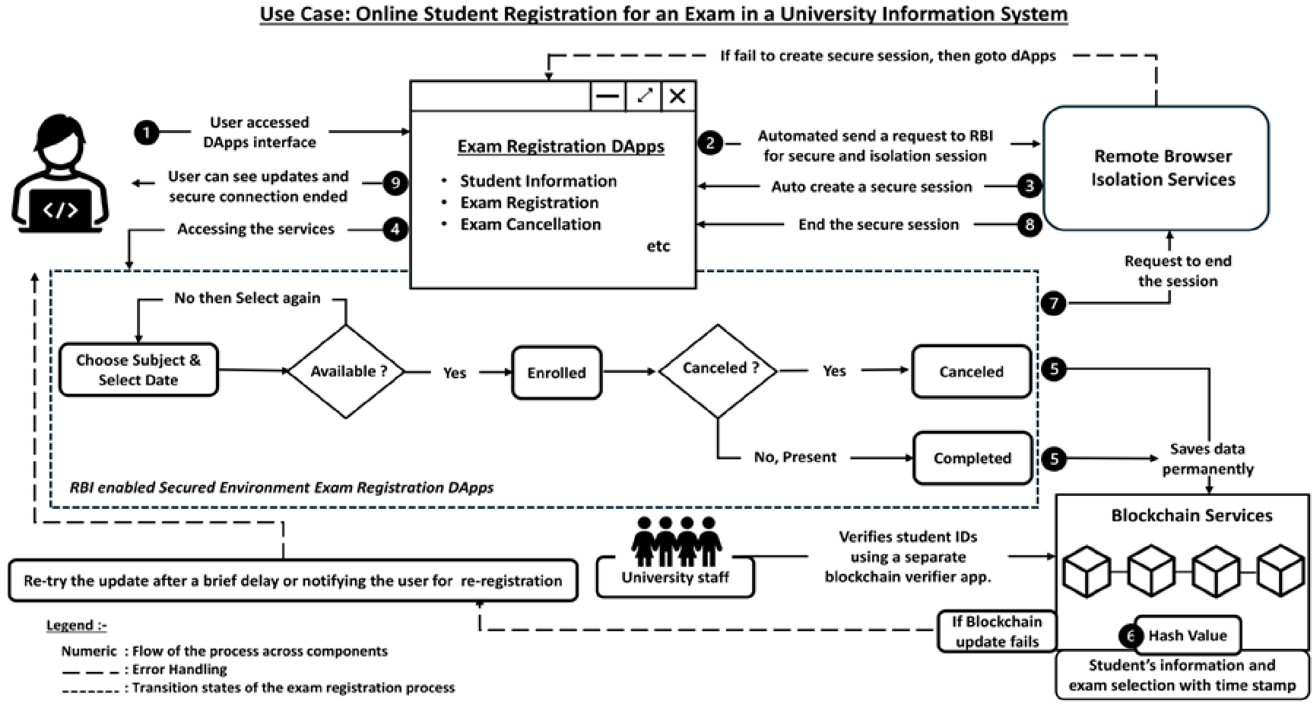

Use Case: Online Student Registration for an Exam in a University Information System
If fail to create secure session, then goto dApps
1 User accessed DApps interface
9 User can see updates and secure connection ended
4 Accessing the services
Exam Registration DApps
• Student Information
• Exam Registration
• Exam Cancellation
etc
2 Automated send a request to RBI for secure and isolation session
3 Auto create a secure session
8 End the secure session
Remote Browser Isolation Services
Request to end the session
7
No then Select again
Choose Subject & Select Date
Available ?
Yes
Enrolled
Canceled ?
Yes
Canceled
5
No, Present
Completed
5
Saves data permanently
RBI enabled Secured Environment Exam Registration DApps
Blockchain Services
Re-try the update after a brief delay or notifying the user for re-registration
University staff
Verifies student IDs using a separate blockchain verifier app.
If Blockchain update fails
6 Hash Value
Student's information and exam selection with time stamp
Legend :-
Numeric : Flow of the process across components
— — — : Error Handling
------- : Transition states of the exam registration process

Figure 10 Use Case: Online Student Registration for an Exam in a University Information System

3.6. Conceptual Framework 2 (Merging RBI and TEE with Blockchain Technology)

To provide more security and robustness, TEE can be integrated with the previous framework design, as shown in Figure 11. TEEs, such as Intel SGX or ARM TrustZone, provide secure enclaves for executing sensitive computations and storing private keys. By integrating TEE with RBI (which isolate and secure browser sessions from potential threats) and Blockchain technology (which ensures decentralized trust and transparency in transactions) applications can achieve a new level of security. This integration enables secure handling of cryptographic operations within the enclave, while RBI protects user interactions with blockchain-based applications from malicious attacks. Together, these technologies foster a safer environment for sensitive data, transactions, and decentralized applications, ensuring confidentiality, integrity, and reliability in digital interactions. It is important to note that implementing these technologies together is a complex task and requires careful planning, technical expertise, and rigorous testing.

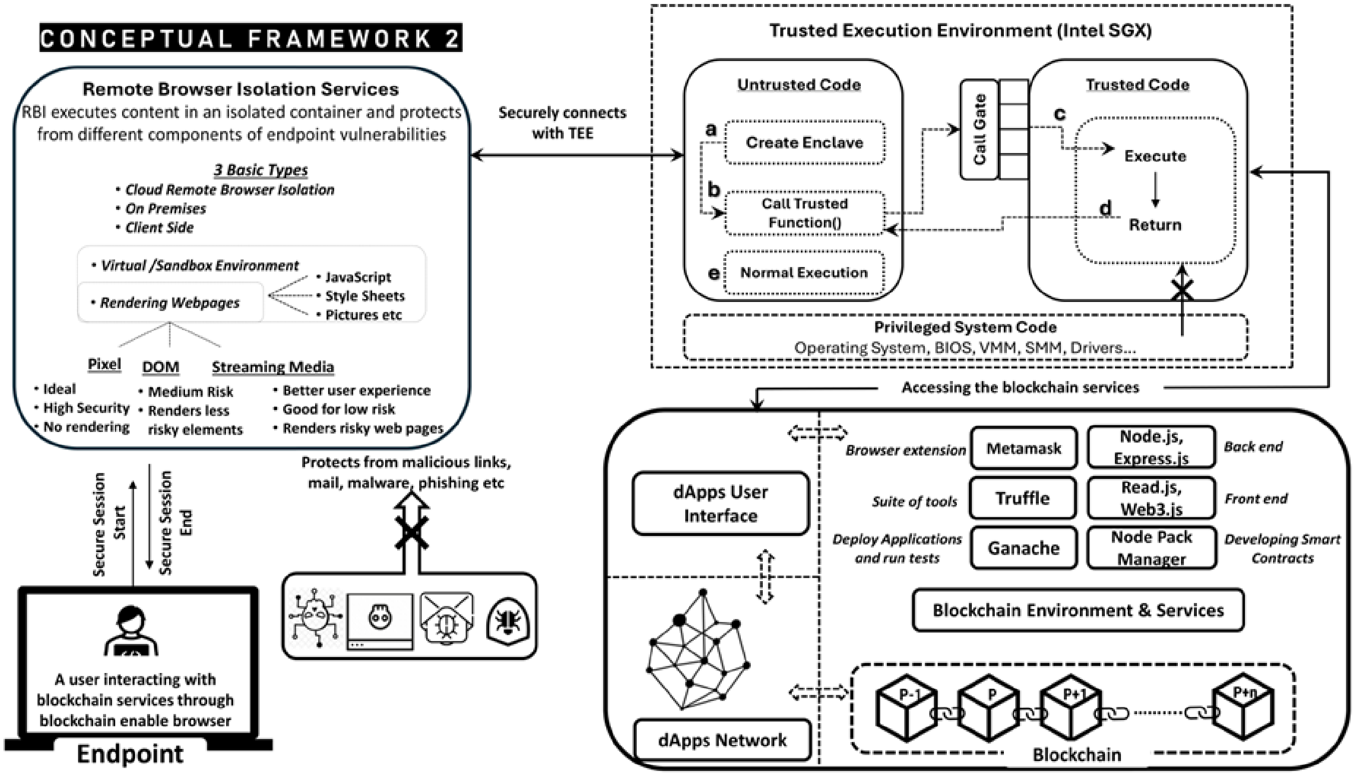

CONCEPTUAL FRAMEWORK 2
Remote Browser Isolation Services
RBI executes content in an isolated container and protects from different components of endpoint vulnerabilities
3 Basic Types
• Cloud Remote Browser Isolation
• On Premises
• Client Side
• Virtual /Sandbox Environment
• Rendering Webpages
• JavaScript
• Style Sheets
• Pictures etc
Pixel
• Ideal
• High Security
• No rendering
DOM
• Medium Risk
• Renders less risky elements
Streaming Media
• Better user experience
• Good for low risk
• Renders risky web pages
Securely connects with TEE
Secure Session Start
Secure Session End
Protects from malicious links, mail, malware, phishing etc
A user interacting with blockchain services through blockchain enable browser
Endpoint
Trusted Execution Environment (Intel SGX)
Untrusted Code
a
Create Enclave
b
Call Trusted Function()
e
Normal Execution
Call Gate
Trusted Code
c
Execute
d
Return
Privileged System Code
Operating System, BIOS, VMM, SMM, Drivers...
Accessing the blockchain services
dApps User Interface
Browser extension
Metamask
Node.js, Express.js
Back end
Suite of tools
Truffle
Read.js, Web3.js
Front end
Deploy Applications and run tests
Ganache
Node Pack Manager
Developing Smart Contracts
Blockchain Environment & Services
P-1
P
P+1
P+n
Blockchain
dApps Network

Figure 11 Conceptual Framework 2: Merging RBI and TEE with Blockchain Technology

3.6.1. Process

In this integrated setup, when a user initiates an action through a web browser isolated by RBI, their request is securely transmitted to the application's backend. Within this secure environment, TEEs such as Intel SGX or ARM TrustZone ensure that sensitive computations occur within protected enclaves, safeguarding against unauthorized access.

Once processed securely within the TEE enclave, the request interacts with Blockchain services, leveraging its decentralized ledger for executing smart contracts, validating transactions, or accessing blockchain data. The response flows back through TEE and RBI, ensuring that users receive trusted feedback through the secure browser session. This comprehensive approach not only protects user data and transactions from potential threats but utilizes blockchain's decentralized trust to ensure transparency and reliability in digital interactions also.

3.6.2. Dataflow Overview

Figure 11 shows the location of RBI services, TEE, dApps interface and blockchain services. The user initiates a new request from their device to access blockchain services like entering the login details or entering the data on blockchain network. RBI server fetches the request and renders in an isolated environment and securely communicates with the TEE to process sensitive data within a secure main processor area and ensures that private keys entering, transaction signing, and other critical operations taking place in a very rich secure environment. The processed data and transactions are securely sent to the blockchain network where it gets time-stamped, validated, and are then sent back through the TEE and RBI to the user’s device. Finally, the user initiates a request to terminate the session by logging out of the blockchain application, RBI server securely closes the TEE and blockchain network, ensuring no operations are left behind. RBI clears the environment securely and Confirmation of logout is sent back to the user’s device. The corresponding minimum system requirement is shown in Table 5.

Table 5 System Requirement for Conceptual Framework 2 (TEE+ RBI+ Blockchain Technology)

System Requirements	
Component	Minimum Requirement
OS	Ubuntu 20.04 LTS
RAM	16 GB
CPU	Quad-core Intel i5 or AMD Ryzen 5
Storage	100 GB SSD

Graphics Card	Integrated Graphics
Blockchain Platform	Ethereum, Hyperledger Fabric
RBI Tools	Selenium, OWASP ZAP
TEE Technologies	Intel SGX, AMD SEV, or ARM TrustZone
Development Frameworks	Truffle Suite, Hardhat

3.7. Conceptual Framework 3 (Merging RBI, TEE and Steganography with Blockchain Technology)

The integration of Steganography with the above framework design yields very high security at the cost of maximum complexity. In this integrated system, a user's request, initiated via a browser session managed by RBI, ensures that interactions are isolated and protected from potential web-based threats. The steganographically hidden data within the user's request is securely transmitted to the backend, where a TEE such as Intel SGX or ARM TrustZone processes the sensitive information within a secure enclave. This guarantees that the hidden data remains protected during processing and is only accessible within the secure boundaries of the TEE. After the secure processing in the TEE, the request interacts with Blockchain services. Finally, the processed information, still hidden within non-sensitive data, is returned to the user through the RBI-managed browser session. This end-to-end integration of steganography with TEE, RBI, and Blockchain not only protects sensitive data from unauthorized access and threats but also ensures that its presence remains undetectable, enhancing the overall security and privacy of digital interactions. No figure is provided in this paper for Framework 3.

Apart from numerous security benefits, this integration also presents several disadvantages and complications. Some of the notable complexities are need of technical expertise, high computational load, deep understanding of each technology, substantial development effort, high coding and testing, development of new protocols if needed, decreased latency, need of high computational resources, limitations on the amount of data that can be hidden without detection, the contrast of transparency between steganography and blockchain and compatibility issues.

4. IMPACT OF THE FRAMEWORKS ON ENDPOINT VULNERABILITIES

The integration of various advanced technologies through the frameworks has the potential to reduce or mitigate endpoint attacks in blockchain applications. Table 6 shows the impact of different frameworks on the types of endpoint vulnerabilities. A filled circle means, this particular framework can mitigate the particular types of endpoints whereas a half-filled circle means it can mitigate partially and a hollow circle means it cannot mitigate the issues. For example, broken authentication, an endpoint vulnerability, can be partially resolved using Framework 1 (symbolized by a half-filled circle) and fully resolved using Frameworks 2 and 3 (symbolized by a filled circle). Table 7 provides the impact of the conceptual frameworks on possible endpoint threats and attacks. Figure 12 shows the mapping of endpoint vulnerabilities to potential threats and conceptual frameworks.

Table 6 Combination of Technologies and Framework-wise Effect on the Mitigation of Endpoint Vulnerabilities

Endpoint Vulnerabilities	Conceptual Framework 1 (RBI + Blockchain Technology)		Conceptual Framework 2 (RBI + TEE+ Blockchain Technology)		Conceptual Framework 3 (RBI + TEE+ Steganography + Blockchain Technology)	
	Summary	Impact	Summary	Impact	Summary	Impact
Broken Authentication	Limits exposure of authentication sessions to potential attackers by isolating browser activities	◒	Ensures integrity and confidentiality of authentication processes	●	Ensures integrity and confidentiality of authentication processes; hides sensitive data	●
Cryptographic failures	Can prevent certain types of attacks that exploit cryptographic weaknesses	◒	Provides a secure environment for cryptographic operations	●	Provides a secure environment for cryptographic operations; hides data making it harder to attack	●

Endpoint Vulnerabilities	Conceptual Framework 1 (RBI + Blockchain Technology)		Conceptual Framework 2 (RBI + TEE+ Blockchain Technology)		Conceptual Framework 3 (RBI + TEE+ Steganography + Blockchain Technology)	
	Summary	Impact	Summary	Impact	Summary	Impact
Security Misconfiguration	Reduces risk by centralizing browser configurations	◒	Ensures that security configurations are enforced and tamper-proof	●	Ensures that security configurations are enforced and tamper-proof	●
Web Security Vulnerability	Isolates web content, reducing the impact of web-based vulnerabilities	●	Protects sensitive operations from web-based attacks	●	Protects sensitive operations from web-based attacks; hides data securely	●
Human vulnerabilities	Limits impact of user errors by controlling and isolating browser interactions	◒	Reduces risks associated with human errors by securing critical operations	◒	Reduces risks associated with human errors by securing critical operations; provides an additional layer of security by hiding data	◒
●: Solves fully ◒ : Solves partially ○ : Does not solves						

Table 7 Impact of the Conceptual Frameworks on Possible Endpoint Threats and Attacks

Possible Endpoint Threats	Conceptual Framework 1 (RBI+ Blockchain Technology)		Conceptual Framework 2 (RBI + TEE+ Blockchain Technology)		Conceptual Framework 3 (RBI+TEE+ Steganography + Blockchain Technology)	
	Summary	Impact	Summary	Impact	Summary	Impact
Wallet attack	RBI provides an isolated environment for logs and authentication activities	●	TEE protects sensitive operations and ensures secure execution.	●	It adds layer of hidden security, making it harder for attackers to identify targets	●
Brute force	RBI may be ineffective	○	TEE ensures secure login mechanisms, making brute-force attacks less effective	◒	Steganography hides login attempt details, further obfuscating attack vectors	◒
Signature forgery	RBI does not solve it	○	TEE secures the signature creation and verification process.	●	Steganography protects signature data, making forgery more difficult.	●
Transaction malleability	RBI does not solve it as it falls under transaction vulnerability	○	TEE is unable to protect it	○	Steganography is unable to protect it	○

Cryptojacking	An attacker cannot install a malicious script	●	TEE provides more protection	●	Protect due to RBI and TEE and steganography plays no part in it	●
Malware	An attacker cannot install malicious script	●	TEE provides more protection	●	Protect due to RBI and TEE and steganography plays no part in it	●
Credential theft	The isolated environment keeps attackers away	●	TEE provides more protection	●	Steganography hides credential and storage, making theft more difficult.	●
Social engineering	RBI can help identify and mitigate risks from social engineering by focusing on risky areas and vulnerabilities	●	A secure environment protects against attacks facilitated by social engineering	●	It adds another layer of protection	●

●: Decrease the attack effect ◒ : Partially decrease the attack effect ○ : No effect

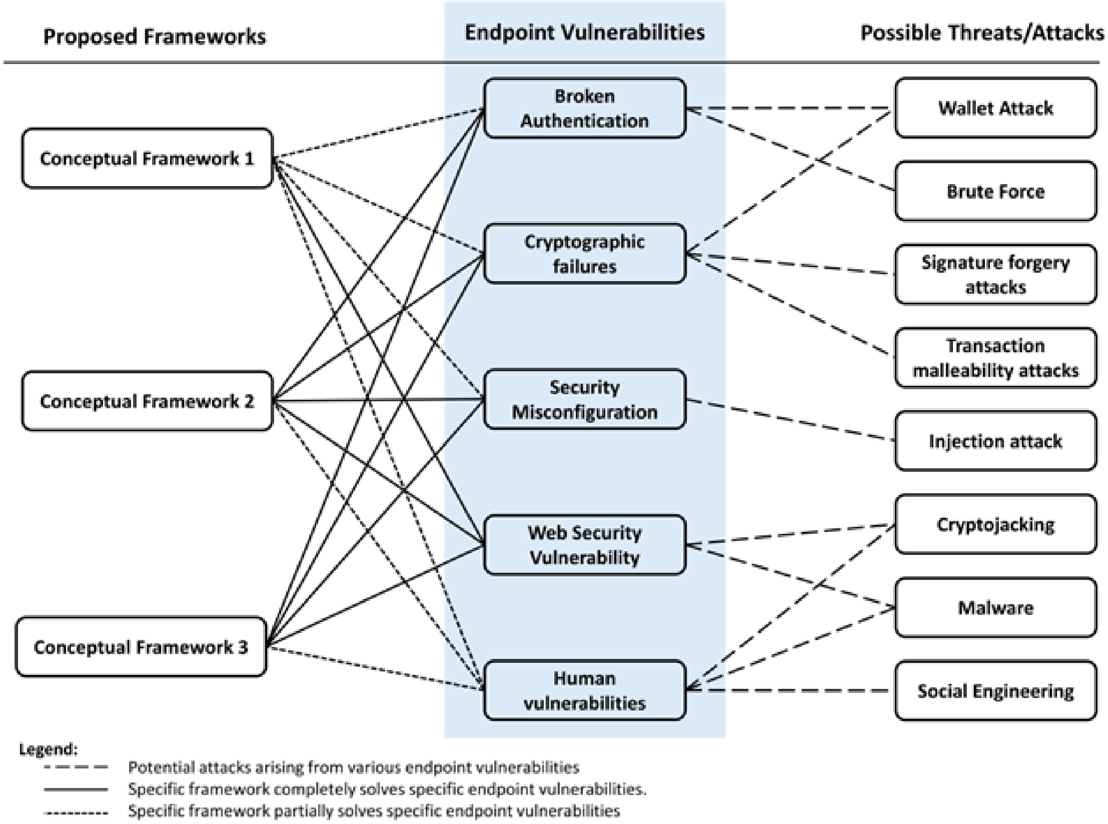

Proposed Frameworks
Endpoint Vulnerabilities
Possible Threats/Attacks
Conceptual Framework 1
Conceptual Framework 2
Conceptual Framework 3
Broken Authentication
Cryptographic failures
Security Misconfiguration
Web Security Vulnerability
Human vulnerabilities
Wallet Attack
Brute Force
Signature forgery attacks
Transaction malleability attacks
Injection attack
Cryptojacking
Malware
Social Engineering
Legend:
Potential attacks arising from various endpoint vulnerabilities
Specific framework completely solves specific endpoint vulnerabilities.
Specific framework partially solves specific endpoint vulnerabilities

Figure 12 Mapping Endpoint Vulnerabilities to Potential Threats and Conceptual Frameworks

5. LIMITATIONS

The framework designed to solve the endpoint issues in blockchain applications is new and yet not developed and presents several limitations. To the best of to the best of current knowledge, no one has implemented it till now. It provides good security while merging RBI with the Blockchain environment but complexity and computational overhead increase while merging TEE and steganography technologies, respectively.

These factors could slow down blockchain transaction processing. Additionally, scalability may be a concern, as the resource demands of these technologies could hinder large-scale blockchain applications. While implementing the conceptual frameworks, many other and new complexities may arise. These limitations highlight the need for further research to address potential complexities before achieving widespread adoption. It is to be believed that the successful implementation of these framework designs will open new advancements and opportunities for the stakeholders, researchers and users.

6. CONCLUSION

Blockchain applications have encountered numerous issues and challenges since their inception. While researchers have addressed many of these issues, some remain largely unexplored by the academic community. One significant concern raised by experts is endpoint security, which is yet to be fully addressed. Endpoint vulnerabilities were divided into various subtypes and each vulnerability was assessed deeply in terms of reasons and technique, possible threats, adverse effects, detection and prevention. This paper proposes the implementation of RBI with blockchain technology to provide a secure and safe environment for users, thereby minimizing endpoint threats. The integration of RBI with blockchain theoretically addresses web security malware, cryptographic failures, and vulnerabilities arising from human negligence. To further enhance security, the paper suggests incorporating a layer of TEE with RBI and blockchain. Although this addition introduces some complexity, it significantly improves security. Moreover, the paper introduces steganography as an additional layer of protection, offering premium security at the cost of increased computational demands and complexity. These frameworks were backed by PoC and DiD multi-layered approach. These approaches aim to place security at the forefront of blockchain applications and ensure robust protection against a wide range of threats. By addressing endpoint vulnerabilities and integrating these advanced security measures, this paper contributes substantially to enhancing the overall security framework of blockchain technology, making it more resilient to both known and emerging threats. This multidimensional strategy not only strengthens security but also raises greater trust and confidence in the use of blockchain applications.

REFERENCES

[1] Y. Abuidris, A. Hassan, A. Hadabi, and I. Elfadul, “Risks and opportunities of blockchain based on e-voting systems,” in 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, 2019, pp. 365–368. doi: 10.1109/ICCWAMTIP47768.2019.9067529.

[2] J. H. Lee, “Systematic approach to analyzing security and vulnerabilities of blockchain systems,” Massachusetts Institute of Technology, 2019. doi: https://web.mit.edu/smadnick/www/wp/2019-05.pdf.

[3] Z. Wenhua, F. Qamar, T.-A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, “Blockchain technology: security issues, healthcare applications, challenges and future trends,” Electronics (Basel), vol. 12, no. 3, p. 546, 2023, doi: 10.3390/electronics12030546.

[4] Y. Erinle, Y. Kethepalli, Y. Feng, and J. Xu, “SoK: Design, Vulnerabilities and Defense of Cryptocurrency Wallets,” arXiv preprint arXiv:2307.12874, 2023, doi: 10.48550/arXiv.2307.12874.

[5] B. Eliasi and A. Javdan, “Comparison of blockchain e-wallet implementations,” 2019, School of Electrical Engineering and Computer Science. Accessed: Oct. 25, 2023. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1350402/FULLTEXT01.pdf

[6] S. Gomzin and K. Westin, Crypto Basics: A Nontechnical Introduction to Creating Your Own Money for Investors and Inventors, 1st ed. Apress Berkeley, CA, 2022. doi: 10.1007/978-1-4842-8321-9.

[7] P. McCorry, M. Möser, and S. T. Ali, “Why preventing a cryptocurrency exchange heist isn’t good enough,” in Cambridge International Workshop on Security Protocols, Springer International Publishing, 2018, pp. 225–233. doi: 10.1007/978-3-030-03251-7_27.

[8] S. Eskandari, D. Barrera, E. Stobert, and J. Clark, “A First Look at the Usability of Bitcoin Key Management,” in Proceedings 2015 Workshop on Usable Security, Internet Society, Feb. 2015. doi: 10.14722/usec.2015.23015.

[9] L. Coppolino, S. D’Antonio, G. Mazzeo, L. Romano, and P. Campegiani, “Facing the blockchain endpoint vulnerability, an SGX-based solution for secure eHealth auditing,” 5th Italian Conference on Cybersecurity - CEUR Workshop Proceedings, vol. 2940, pp. 298–308, 2021, Accessed: Dec. 09, 2024. [Online]. Available: https://ceur-ws.org/Vol-2940/paper25.pdf.

[10] H. Harrison, “Browser isolation as an enterprise security control,” Cyber Security: A Peer-Reviewed Journal, vol. 6, no. 2, pp. 141–147, 2022, doi: 10.69554/RNYH1344.

[11] Cloudflare, “What is browser isolation?” Cloudflare. Accessed: Jul. 16, 2024. [Online]. Available: https://www.cloudflare.com/learning/access-management/what-is-browser-isolation/

[12] M. Sabt, M. Achemlal, and A. Bouabdallah, “Trusted execution environment: What it is, and what it is not,” in 2015 IEEE Trustcom/BigDataSE/Ispa, Helsinki, Finland: IEEE, 2015, pp. 57–64. doi: 10.1109/Trustcom.2015.357.

[13] Joel Timothy, “What is a Trusted Execution Environment (TEE)?,” Duality. Accessed: Jul. 16, 2024. [Online]. Available: https://dualitytech.com/blog/what-is-a-trusted-execution-environment-tee/

[14] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, “A review on text steganography techniques,” Mathematics, vol. 9, no. 21, p. 2829, 2021, doi: 10.3390/math9212829.

[15] M. Gimenez-Aguilar, J. M. De Fuentes, L. González-Manzano, and C. Camara, “Zephyrus: an information hiding mechanism leveraging Ethereum data fields,” IEEE Access, vol. 9, pp. 118553–118570, 2021, doi: 10.1109/ACCESS.2021.3106713.

[16] M. Noor and K. Mustafa, “A systematic literature review on endpoint vulnerabilities of blockchain applications,” International Journal of Advanced Technology and Engineering Exploration, vol. 10, no. 109, pp. 1665–1695, Dec. 2023, doi: 0.19101/IJATEE.2023.10101498.

[17] S. Nakamoto, “A peer-to-peer electronic cash system,” Bitcoin. –URL: https://bitcoin. org/bitcoin. pdf, vol. 4, 2008.

[18] V. Buterin, “Ethereum white paper,” GitHub repository, vol. 1, pp. 22–23, 2013, Accessed: Dec. 09, 2024. [Online]. Available: https://static.peng37.com/ethereum_whitepaper_laptop_3.pdf

[19] M. A. F. Noor, S. Khanum, T. Anwar, and M. Ansari, “A Holistic View on Blockchain and Its Issues,” in Blockchain Applications in IoT Security, IGI Global, 2021, pp. 21–44, doi: 10.4018/978-1-7998-2414-5.ch002.

[20] G. Yang, C. Li, and K. E. Marstein, “A blockchain-based architecture for securing electronic health record systems,” Concurr Comput, vol. 33, no. 14, p. e5479, 2021, doi: 10.1002/cpe.5479.

[21] S. Mollajafari and K. Bechkoum, “Blockchain technology and related security risks: towards a seven-layer perspective and taxonomy,” Sustainability MDPI, vol. 15, no. 18, p. 13401, 2023, doi: 10.3390/su151813401.

[22] S. Sharma and R. Dwivedi, “A survey on blockchain deployment for biometric systems,” IET blockchain, vol. 4, no. 2, pp. 124–151, 2024, doi: 10.1049/blc2.12063.

[23] M. Choobineh, A. Arabnya, B. Sohrabi, A. Khodaei, and A. Paaso, “Blockchain technology in energy systems: A state-of-the-art review,” IET Blockchain, vol. 3, no. 1, pp. 35–59, 2023, doi: 10.1049/blc2.12020.

[24] H. Wu et al., “Blockchain for finance: A survey,” IET Blockchain Wiley, vol. 4, pp. 101–123, 2024, doi: 10.1049/blc2.12067.

[25] A. Dixit, A. Trivedi, and W. W. Godfrey, “A survey of cyber attacks on blockchain based IoT systems for industry 4.0,” IET Blockchain, vol. 4, no. 4, pp. 287–301, 2022, doi: 10.1049/blc2.12017.

[26] M. Conti, K. E. Sandeep, C. Lal, and S. Ruj, “A survey on security and privacy issues of bitcoin,” IEEE Communications Surveys and Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018, doi: 10.1109/COMST.2018.2842460.

[27] H. Hasanova, U. jun Baek, M. gon Shin, K. Cho, and M. S. Kim, “A survey on blockchain cybersecurity vulnerabilities and possible countermeasures,” International Journal of Network Management, vol. 29, no. 2, pp. 1–36, 2019, doi: 10.1002/nem.2060.

[28] J. Velissarios, J. Herzig, and U. Didem, “Blockchain’s potential starts with security,” in Accenture, 2019. Accessed: Dec. 09, 2024. [Online]. Available: https://www.accenture.com/us-en/insights/blockchain/potential-starts-security.

[29] M. A. Rasool and H. Muhammad Shafiq, “Blockchain Technology: a new domain for Cyber Forensics,” 2018, Diva, Halmstad University. Accessed: Dec. 09, 2024. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1259867/FULLTEXT01.pdf.

[30] R. Matulevičius, M. Iqbal, E. Ammar Elhadjamor, S. A. Ghannouchi, M. Bakhtina, and S. Ghannouchi, “Ontological Representation of Healthcare Application Security Using Blockchain Technology,” Informatica (Netherlands), vol. 33, no. 2, pp. 365–397, 2022, doi: 10.15388/22-INFOR486.

[31] M. A. F. Noor and K. Mustafa, “A taxonomy of endpoint vulnerabilities and affected blockchain architecture layers,” Concurr Comput, vol. 36, no. 19, p. e8158, 2024, doi: 10.1002/cpe.8158.

[32] H. Guo and X. Yu, “A survey on blockchain technology and its security,” Blockchain: Research and Applications, vol. 3, no. 2, p. 100067, Jun. 2022, doi: 10.1016/j.bcra.2022.100067.

[33] M. Iqbal and R. Matulevicius, “Exploring Sybil and Double-Spending Risks in Blockchain Systems,” IEEE Access, vol. 9, pp. 76153–76177, 2021, doi: 10.1109/ACCESS.2021.3081998.

[34] J. Hu, H. Wang, and Y. Liu, “Strengthening Digital Marketing Security Website Threat Isolation and Protection Using Remote Browser Isolation Technology,” Computer-Aided Design, vol. 21, no. S4, pp. 56–74, 2024, doi: https://doi.org/10.14733/cadaps.2024.S4.56-74.

[35] Karlos G. Ray, “A Quick Walkthrough on Remote Browser Isolation (RBI),” Medium. Accessed: Jul. 17, 2024. [Online]. Available: https://karliris62.medium.com/a-quick-walkthrough-on-remote-browser-isolation-rbi-a563094756f6.

[36] Z. Bao, Q. Wang, W. Shi, L. Wang, H. Lei, and B. Chen, “When blockchain meets SGX: An overview, challenges, and open issues,” IEEE Access, vol. 8, pp. 170404–170420, Sep. 2020, doi: 10.1109/ACCESS.2020.3024254.

[37] L. Farrelly, “What is a Trusted Execution Environment (TEE)?,” Evervault. Accessed: Jul. 16, 2024. [Online]. Available: https://evervault.com/blog/what-is-a-trusted-execution-environment-tee.

[38] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” Future Generation Computer Systems, vol. 107, pp. 841–853, 2020, doi: 10.1016/j.future.2017.08.020.

[39] A. M. Alqahtani and A. Algarni, “A Survey on Blockchain Technology Concepts, Applications and Security,” International Journal of Advanced Computer Science and Applications, vol. 14, no. 2, pp. 841–847, 2023, doi: 10.14569/IJACSA.2023.0140296.

[40] A. N’dri, “The Applications of Blockchain To Cybersecurity,” Culminating Projects in Information Assurance, p. 141, Aug. 2023, Accessed: Dec. 09, 2024. [Online]. Available: https://repository.stcloudstate.edu/msia_etds/141/.

[41] J. Holbrook, “Blockchain Security and Threat Landscape,” in Architecting Enterprise Blockchain Solutions, John Wiley & Sons, Ltd, 2020, ch. 11, pp. 323–347. Doi: 10.1002/9781119557722.ch11.

[42] M. K. Shrivas, T. Y. Dean, and S. S. Brunda, “The Disruptive Blockchain Security Threats and Threat Categorization,” in 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), Raipur: IEEE, Apr. 2020, pp. 327–338. Doi: 10.1109/ICPC2T48082.2020.9071475.

[43] P. A. D. S. N. Wijesekara and S. Gunawardena, “A Review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges,” Network, vol. 3, no. 3, pp. 343–421, 2023, doi: 10.3390/network3030017.

[44] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where is current research on blockchain technology?—a systematic review,” PloS One, vol. 11, no. 10, p. e0163477, 2016, doi: 10.1371/journal.pone.0163477.

[45] O. Pal, B. Alam, V. Thakur, and S. Singh, “Key management for blockchain technology,” ICT Express, vol. 7, no. 1, pp. 76–80, 2021, doi: 10.1016/j.icte.2019.08.002.

[46] E. O. Kiktenko, M. A. Kudinov, and A. K. Fedorov, “Detecting Brute-Force Attacks on Cryptocurrency Wallets,” in Lecture Notes in Business Information Processing, Springer, 2019, pp. 232–242. Doi: 10.1007/978-3-030-36691-9_20.

[47] Z. Wang, H. Yu, Z. Zhang, J. Piao, and J. Liu, “ECDSA weak randomness in Bitcoin,” Future Generation Computer Systems, vol. 102, pp. 507–513, 2020, doi: 10.1016/j.future.2019.08.034.

[48] N. Wang, Y. Chen, Y. Yang, Z. Fang, and Y. Sun, “Blockchain private key storage algorithm based on image information hiding,” in International Conference on Artificial Intelligence and Security, Springer, Jul. 2019, pp. 542–552. Doi: https://doi.org/10.1007/978-3-030-24268-8_50.

[49] M. Brengel and C. Rossow, “Identifying key leakage of bitcoin users,” in International Symposium on Research in Attacks, Intrusions, and Defenses, Springer International Publishing, 2018, pp. 623–643. Doi: 10.1007/978-3-030-00470-5.

[50] J. Lind, O. Naor, I. Eyal, F. Kelbert, E. G. Sirer, and P. Pietzuch, “Teechain: a secure payment network with asynchronous blockchain access,” in Proceedings of the 27th ACM Symposium on Operating Systems Principles, in SOSP ’19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 63–79. Doi: 10.1145/3341301.3359627.

[51] F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. Van Renesse, “{REM}:{Resource-Efficient} mining for blockchains,” in 26th USENIX Security Symposium (USENIX Security 17), Vancouver: USENIX Association, Aug. 2017, pp. 1427–1444. Accessed: Dec. 09, 2024. [Online]. Available: https://eprint.iacr.org/2017/179.pdf.

[52] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of Luck: an Efficient Blockchain Consensus Protocol," in Proceedings of the 1st Workshop on System Software for Trusted Execution, in SysTEX '16. Trento: Association for Computing Machinery, 2016, pp. 1–6. Doi: 10.1145/3007788.3007790.

[53] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, and J. Xie, "Shadoweth: Private smart contract on public blockchain," J Comput Sci Technol, vol. 33, pp. 542–556, 2018, doi: 10.1007/s11390-018-1839-y.

[54] M. Al-Bassam, A. Sonnino, M. Król, and I. Psaras, "Airtnt: Fair exchange payment for outsourced secure enclave computations," arXiv preprint arXiv:1805.06411, 2018, doi: 10.48550/arXiv.1805.06411.

[55] M. A. F. Noor and K. Mustafa, "Protocols and Guidelines to Enhance the Endpoint Security of Blockchain at User's End," in ICIDSSD 2022: Proceedings of the 3rd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2022, 24-25 March 2022, New Delhi, India, New Delhi: EAI Publishing, 2023, p. 231. Doi: 10.4108/eai.24-3-2022.2318925.

[56] Y. Jabareen, "Building a conceptual framework: philosophy, definitions, and procedure," Int J Qual Methods, vol. 8, no. 4, pp. 49–62, 2009, doi: 10.1177/160940690900800406.

[57] Kaspersky, "What is browser isolation and how does it work?," Kaspersky. Accessed: Jul. 16, 2024. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-browser-isolation.

[58] Netskope, "https://www.netskope.com/security-defined/what-is-remote-browser-isolation-rbi," Netskope. Accessed: Jul. 17, 2024. [Online]. Available: https://www.netskope.com/security-defined/what-is-remote-browser-isolation-rbi.

[59] A. Kamruzzaman, S. Ismat, J. C. Brickley, A. Liu, and K. Thakur, "A comprehensive review of endpoint security: Threats and defenses," in 2022 International Conference on Cyber Warfare and Security (ICCWS), Islamabad: IEEE, 2022, pp. 1–7. Doi: 10.1109/ICCWS56285.2022.9998470.

[60] R. Verma, N. Dhanda, and V. Nagar, "Application of truffle suite in a blockchain environment," in Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021, Springer, 2022, pp. 693–702. Doi: 10.1007/978-981-19-1142-2_54.

[61] G. McCubbin, "How To Build A Blockchain App with Ethereum, Web3.js & Solidity Smart Contracts," Dapp University. Accessed: Jul. 18, 2024. [Online]. Available: https://www.dappuniversity.com/articles/how-to-build-a-blockchain-app.

[62] W.-M. Lee, "Using the MetaMask Crypto-Wallet," in Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript, Berkeley, CA: Apress, 2023, pp. 111–144. Doi: 10.1007/978-1-4842-9271-6_5.

Authors

Mohd Azeem Faizi Noor is a Senior Research Fellow at the Department of Computer Science in Jamia Millia Islamia (a central university) in New Delhi, India. He holds dual postgraduate degrees, MCA and MTech, from Pondicherry Central University. His research interests focus on Steganography and Blockchain technologies.

Dr Khurram Mustafa is an IIT Delhi alumnus, who is currently the seniormost professor in the Department of Computer Science at Jamia Millia Islamia (a central university) in New Delhi, India. Despite having completed his PhD on a topic related to eLearning, he continues to supervise students and write/speak on information security, e-learning, and research methods. During his five-year hiatus, he worked as a professor/associate professor at universities in Saudi Arabia, Yemen, and Jordan. In addition to authoring Scientific Research Primer (Ane Books, 2021) and co-authoring two other books, *Software Quality: Concepts and Practices and Software Testing: Concepts and Practices* (both published by Narosa, India, and Alpha Science, UK), he has mentored over a dozen PhD candidates. The latter's Chinese edition has also been released. Aside from these, he has co-authored more than a dozen book chapters and over 100 research papers published in international journals/proceedings. He was also the principal investigator for a three-year government-funded information security project and delivered more than 60 invited talks, including several keynote addresses. He is also a member of several professional scientific societies, including ISTE, ICST, CSI, EAI, ACM-CSTA, eLearning Guild, and InfoPier, as well as several academic committees and editorial review boards.

How to cite this article:

Mohd Azeem Faizi Noor, Khurram Mustafa, " Mitigating Blockchain Endpoint Vulnerabilities: Conceptual Frameworks ", International Journal of Computer Networks and Applications (IJCNA), 11(6), PP: 933-953, 2024, DOI: 10.22247/ijcna/2024/56.