Received: 2 November 2024 | Revised: 6 February 2025 | Accepted: 23 May 2025 | Published online: 19 June 2025

RESEARCH ARTICLE

Journal of Comprehensive Business Administration Research
2025, Vol. 00(00) 1–14
DOI: 10.47852/bonviewJCBAR52024714

BON VIEW PUBLISHING

# A Blockchain Based Secure and Privacy Preserving Smart E-Government Application Execution System with Reduced Service Completion Delay

**Md. Nahid Imtiaz[1] and Mahfuzulhoq Chowdhury[1,*]**

[1]*Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, Bangladesh*

**Abstract:** In today's world, e-government services are critical for assisting citizens with their daily activities such as visa applications, tax submission, emergency security assistance, and electronic tendering. By combining blockchain and Internet of Things (IoT) technologies, e-government services can be made far more secure and efficient. Existing e-government applications suffered from a number of limitations, including a lack of privacy and security, increased job processing time, a lack of coordination among various parties, and a lack of services. More specifically, they did not conduct simultaneous investigations into citizen service, employee service, and business service while comparing performance. To conquer these issues, this article proposes a decentralized blockchain-based secure and privacy-preserving smart e-government system that considers the interactions between informers, government, smart contracts, MetaMask-based public and private wallets, Ethereum, and the Interplanetary File System. We investigated the time and cost delays associated with employee, business, and citizen services in the proposed blockchain-based e-government system. This paper provides appropriate security measures for mitigating malware attacks, DDoS attacks, and Sybil attacks. Our simulation results show that the proposed blockchain-based e-government system can reduce the completion time of existing works by at least 33%.

**Keywords:** e-government, Blockchain, data security, privacy, Ethereum, IPFS, service completion time

## 1. Introduction

With the advancement of the information technology sector, electronic government, or e-government, has become popular in many countries due to its numerous benefits, including cost reduction, flexibility, automation, easy information access, time savings, less corruption, and harassment, among others [1]. The rising population growth rate in many South Asian countries, including Bangladesh, puts significant strain on several aspects of the country's development, including healthcare, education, infrastructure, and employment. Bangladesh's population is expected to be around 174 million by early 2024, up from 171 million in 2022. To assist citizens in their daily lives, the Bangladesh government has also made several services available electronically (via e-government services) to its citizens, including passport applications, electronic tender processes, national ID card registration, and tax and utility fee payments [1].

Currently, due to the lack of a secure and privacy-preserving e-government system, citizens of this country face a number of issues, including data breaches, identity theft, a lack of security, vulnerability to various types of malicious attacks, and unauthorized access to information [2]. People in Bangladesh suffer from problems such as misconduct, power abuse, corruption, inconsistencies, time and economic losses, defense threats, and lack of fairness and integrity as a result of the lack of a security and privacy-preserving e-government system [3–6]. Blockchain technology [7–10] has the potential to transform Bangladesh's e-government system by allowing for the implementation of a decentralized cabinet system.

Blockchain technology can improve administrative and public sector transparency and accountability by securely documenting and validating transactions. By eliminating the need for middlemen, this decentralized ledger system reduces the likelihood of corruption in processes such as document verification, purchasing, and budget distribution. Bangladesh may improve the reliability and effectiveness of public service delivery by embracing blockchain technology. The blockchain-based decentralized ledger system allows for the recording of transactions associated with e-government applications without the need for a central authority. Blockchain technology provides several benefits to the e-government system, including increased transparency, reliability, secure data sharing, increased data integrity, decentralized structure, distributed management, user and data authenticity, the use of cryptographic algorithms, data validation techniques using miners, smart contracts usage, public and private networks, and so on [8].

Currently, the existing blockchain-based e-government works [15–20] have several limitations. They did not create a blockchain-based e-government system that provided various business,

***Corresponding author:** Mahfuzulhoq Chowdhury, Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, Bangladesh. Email: mahfuz_cse@cuet.ac.bd

employee, and citizen services at the same time. They did not look into the time and cost delays associated with various services (e.g., employee, business, and citizen services) in a blockchain-based e-government system. They failed to provide adequate security measures for preventing malware attacks, distributed denial of service (DDoS) attacks, and Sybil attacks in a blockchain-based e-government system.

Due to a lack of a proper coordination system, the existing e-government system experiences significant service completion delays as well as high time and space complexities. They also made no comparison with existing works in terms of delay and attack mitigation. To address these issues, this paper proposes a blockchain-based secure and privacy-preserving smart e-government system for Bangladeshi citizens, taking into account various types of users, services, and parties. More specifically, the novel contribution of this paper is the inclusion of blockchain-based business, employee, and citizen services with low delay and cost.

The primary contributions of the paper presented are elaborated below: (i) This article describes a decentralized blockchain-based smart e-government system that reduces service completion time with high security and privacy by coordinating with various services, informers, government authorities, smart contracts, MetaMask-based public and private wallets, the Ethereum platform, and the Interplanetary File System (IPFS). (ii) To improve security, transparency, and trust, this paper introduces a public blockchain for informants and a private blockchain for government officials. This paper provides appropriate security measures for malware attacks, DDoS attacks, and Sybil attack mitigation. (iii) This paper investigates the service completion time and monetary cost delay for not only employee services but also business and citizen services in our proposed e-government system. This paper also compares the performance of the proposed system to that of existing systems.

The second section provides a detailed overview of existing blockchain-based e-government systems. Section three describes the working steps for the proposed blockchain-based e-government system. Section four discusses the outcomes of our proposed system. Section five concludes the paper by providing a brief summary.

## 2. Literature Review

Blockchain technology has ushered in a completely new domain in computer science research. In section two, we will look at existing research on blockchain-based e-government systems. In Yaga et al. [21], a comprehensive overview of blockchain technology was provided, emphasizing its importance as the foundation of Bitcoin and its growing popularity. It investigates the characteristics of blockchains as an immutable ledger that allows for decentralized transactions, as well as their applications in a variety of fields. The paper addresses existing challenges regarding blockchain, such as scalability and security, a comparison of consensus algorithms, and recent technological advances. It also discusses upcoming trends and potential developments in the blockchain space. In Monrat et al. [8], a comparative analysis of blockchain technology was conducted, focusing on its applications in digital cryptocurrencies and various industries. It investigates how blockchain features such as decentralization, immutability, transparency, and audibility improve transaction security and tamper-proofing. The paper discusses blockchain taxonomy, architecture, and consensus mechanisms while addressing issues such as scalability, privacy, interoperability, energy consumption, and regulatory compliance. It also discusses the future potential of blockchain technology.

In Khayyat et al. [9], the challenges and benefits of integrating blockchain technology into Saudi Arabia's e-government platforms were investigated. The study examines previous research on blockchain technology, drawing on both secondary data from the literature and primary data from expert interviews. The qualitative data analysis uses thematic analysis. This study sheds light on the potential impact of blockchain on KSA's e-government. The study looks at the challenges and benefits of incorporating blockchain into Saudi Arabia's e-government platforms. However, it may fail to investigate potential solutions or practical implementations for addressing the identified challenges effectively. They also did not conduct simultaneous investigations into business, employee, and citizen services. Their work also lacks a time and cost analysis for the blockchain-based electronic government system. In the article by Górski [22], a smart contract for coherent transaction types especially for the energy sector was developed. However, they did not include multiple different types of transactions like citizen, government, and business services.

In the article by Hou [10], the authors focused on the use of blockchain technology in e-government regarding a Chinese city. The article discusses how blockchain-based techniques can improve service quality, transparency, information delivery, and the dynamic credit system. However, issues such as data security, cost, and reliability must be addressed. This study lays the groundwork for the practical application and theoretical exploration of blockchain in government services. It may lack broader perspectives on the proposed solutions' scalability and adaptability to diverse government systems. In Hingorani et al. [11], the authors discussed how the rise in criminal activity and the traditional practice of handwritten First information reports (FIRs) present challenges to law enforcement in India. The current centralized system-based crime and criminal tracking systems lack a decentralized approach and are prone to failure and unauthorized access. To address these issues, they proposed a blockchain-based solution. By encrypting and storing FIRs in a decentralized IPFS and adding their hashes to the blockchain network, the system ensures secure and tamper-proof complaint management while also providing strong evidence in the event of denial or pressure. In Mukherjee and Halder [12], the authors described a blockchain-based dynamic policing system that significantly improves accountability and trust in the management among various stakeholders, employing Hyperledger Fabric and ABAC policy for a strong proof of concept. The system enables seamless participation from citizens as well as multiple law enforcement and judicial entities, resulting in improved performance based on experimental evaluation. While the system uses blockchain technology for law enforcement, it does not thoroughly investigate advanced encryption algorithms that could improve security, nor does it address broader smart government requirements beyond law enforcement. The paper by Mali et al. [13] describes how to build a distributed electronic tendering system with smart contracts using the Ethereum blockchain. The system is divided into four major sections: creating the tender, bidding, evaluating bids, and selecting the winning bid. They did not provide the proposed system's feasibility results, as well as time and cost analyses. In Al-Ameri and Ayvaz [14], the authors created a secure authentication scheme for Turkish e-government services based on blockchains. They did not use both the public and private blockchain frameworks. They also did not offer any solutions for various types of attacks. Their work is restricted to a single type of e-government work rather than multiple types of services (such as business, customer, and

government services). They were also unable to provide any information about service delays or monetary costs in comparison to existing work. According to Elisa et al. [15], the elliptic curve cryptography algorithm and the delegated proof of stake (DPoS) consensus process are used to ensure effective and secure data management in a blockchain-based e-government system. They also did not offer any solutions for different types of attacks or for reducing service delivery delays. In Chentouf and Bouchkaren [16], the authors created a smart e-voting system based on blockchain technology. However, they did not provide any information about the service completion delay or the monetary cost associated with the e-voting transaction. According to the preceding discussion, existing blockchain-based e-government works failed to account for three distinct types of services: business, employee, and citizen services. They also did not create a blockchain-based system for Bangladeshi e-government services that took into account multiple types of attacks and required multi-party coordination involving public and private blockchains, MetaMasks, and IPFS systems. The existing works also lack evaluations of service delivery delays and monetary costs. To outperform previous works, this paper develops a low-service delivery delay decentralized blockchain-based e-government system that supports various business, employee, and citizen services while maintaining security and privacy.

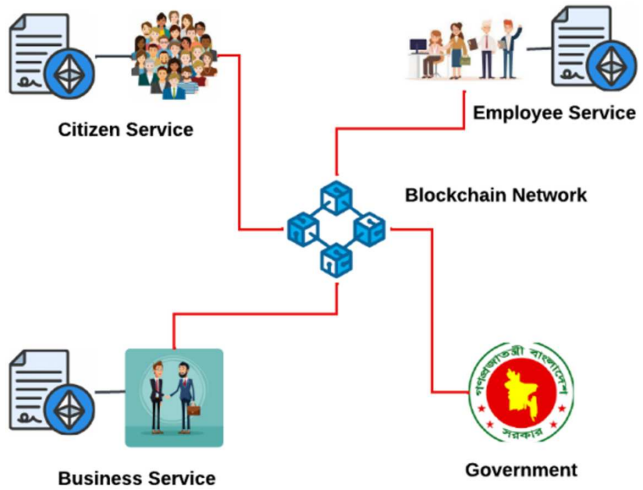
## 3. Proposed Framework

This section will go into great detail about our proposed blockchain-based e-government system.

### 3.1. System design

Figure 1 reveals the design overview for the proposed blockchain-based e-government system. The government side and the informant side are the two fundamental components of the system's operation. To implement the e-government system, we used three different types of smart contracts: citizen service, business service, and employee service. Citizen services include visa applications, utility payments, and income tax returns, among others. Employee services include emergency information, regular interactions with the government, and salary updates, among other things. Business services include financial assistance and e-tenders, among others. Informers publish their transactions on the IPFS

**Figure 1**
**Design overview of proposed system**

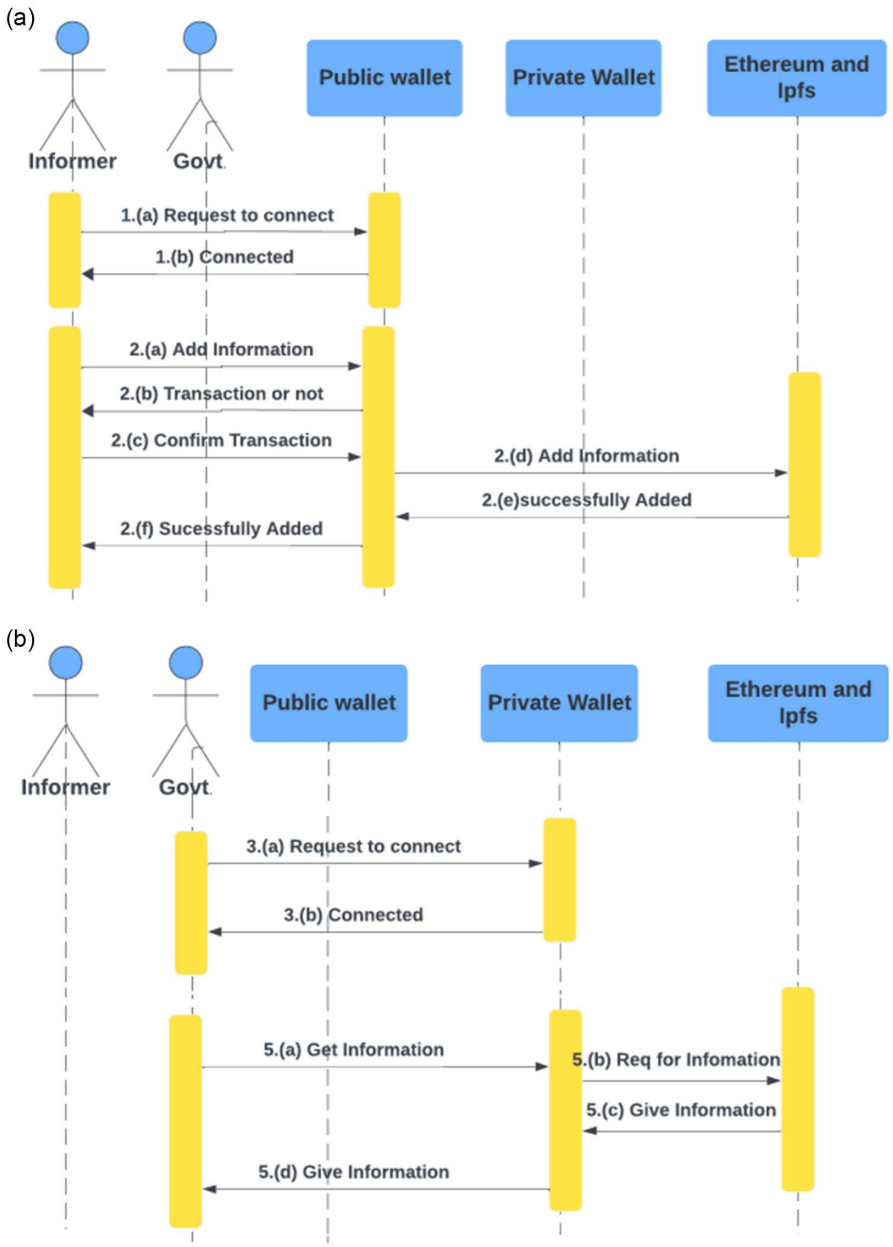



and Ethereum. The government can take action after reviewing the database from the IPFS and Ethereum. Figure 1 depicts how businesses, citizens, and government authorities are linked to the blockchain network. Figure 2 depicts the overall e-government and blockchain interaction framework. The proposed framework uses blockchain technology to transform governance in Bangladesh by establishing a decentralized government structure. Our solution consists of several key components, including Ethereum, IPFS, and public and private wallets. Together, these components enable our system architecture to provide secure data storage, efficient information retrieval, and transparent transaction processing. Our solution provides a secure environment in which private wallets and government actors can easily communicate. These wallets act as intermediaries, responding quickly and effectively to requests for specific information from the authorities. Private wallets can safely access and retrieve data using IPFS and the Ethereum blockchain. Ethereum guarantees smart contract functionality and transactional transparency, while IPFS provides decentralized storage and data integrity protection throughout the process. When these elements are combined, they form a solid framework that promotes trustworthy and responsible information sharing between public and private sector actors. Our method facilitates information transmission by mediating interactions between public wallets and informant actors. Informants send queries to these public wallets, which serve as gateways to decentralized networks such as IPFS and Ethereum, seeking specific information. To securely store data, public wallets connect to IPFS's decentralized storage network and Ethereum's blockchain. This architecture provides a dependable and secure environment for data storage and access by ensuring data integrity, transparency through Ethereum smart contracts, and robust storage capabilities via IPFS. The informant communicates with the Ethereum blockchain using the public wallet. The informant first establishes a connection with the public wallet. Following the creation of this link, the informant enters data into the public wallet.

After entering the transaction details, the informant verifies it in the public wallet. Following confirmation, the public wallet sends the data to Ethereum and IPFS. The public wallet ensures that Ethereum and IPFS are connected by unique addresses, or hashes. These special hashes enable the systems to integrate and verify data smoothly. As a result, the entire procedure ensures that data is freely accessible and securely stored on decentralized storage platforms and blockchains. The private wallet facilitates interactions between government authorities and the Ethereum blockchain. Initially, the government side is connected to the private wallet. Following this connection, the government authorities acquire data from the private wallet. Following that, the government authorities confirm the information obtained from the private wallet. In the meantime, the public wallet connects IPFS and Ethereum via unique addresses, or hashes. These unique addresses are required for storing and retrieving data. The private wallet uses these addresses to receive data from Ethereum and IPFS. Finally, the authorities receive the data from the private wallet, ensuring a precise and authentic transfer. Our system is based on Ethereum and IPFS. The IPFS decentralizes data over a peer-to-peer network, revolutionizing file storage. Using content-addressed hyperlinks ensures that the material is always available and unchangeable. IPFS enables reliable and effective data distribution by storing and retrieving files based on their unique cryptographic hash.

Figure 3 gives the system architecture of the proposed e-government system based on the blockchain framework. Informer connects wallets to the public MetaMask. Informer uploads files to IPFS using a public MetaMask wallet and adds data to the Ethereum blockchain. Ethereum and IPFS communicate with each other via

**Figure 2**
**Government blockchain sequence diagram**




addresses (hashes). Files or information are transferred to a private MetaMask wallet via IPFS and the Ethereum blockchain. The government has obtained information from a private MetaMask wallet. A virtual machine that uses the Ethereum protocol is known as an EVM. The EVM is the primary component that processes transactions, executes smart contracts, and updates Ethereum balances. IPFS is a decentralized file storage system designed to connect devices that use the same file system.

## 3.2. Network architecture

Figure 4 delivers the detailed network architecture of the proposed e-government system using blockchain. Our proposed model integrates business, citizen, and employee services. So network architecture integrates services for businesses, citizens, and employees. The term "government-to-citizen," or G2C, refers to the interactions and relationships between the state and its constituent people. The term G2E refers to contacts and relationships between the government and its workers. The term G2B refers to how corporations and the government interact. Blockchain enables G2B, G2C, G2E, and G2G interactions between parties. The government uses blockchain technology to communicate with businesses, employees, and citizens. Blockchain technology is being used in e-government to integrate multiple services.

## 3.3. Block generation

Figure 5 depicts the creation of a block in the proposed system. The proposed system involves several steps. The informer adds information to the smart contract, which starts the block generation process. The smart contract generates a transaction and submits it to MetaMask for further processing. MetaMask can verify the

**Figure 3**
**System architecture of proposed system**

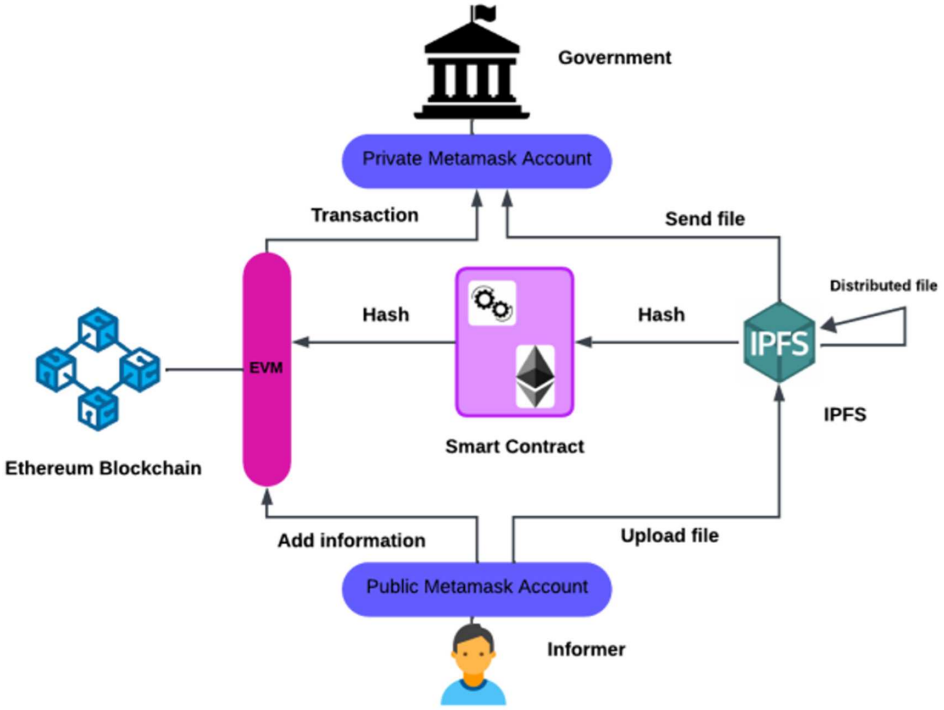
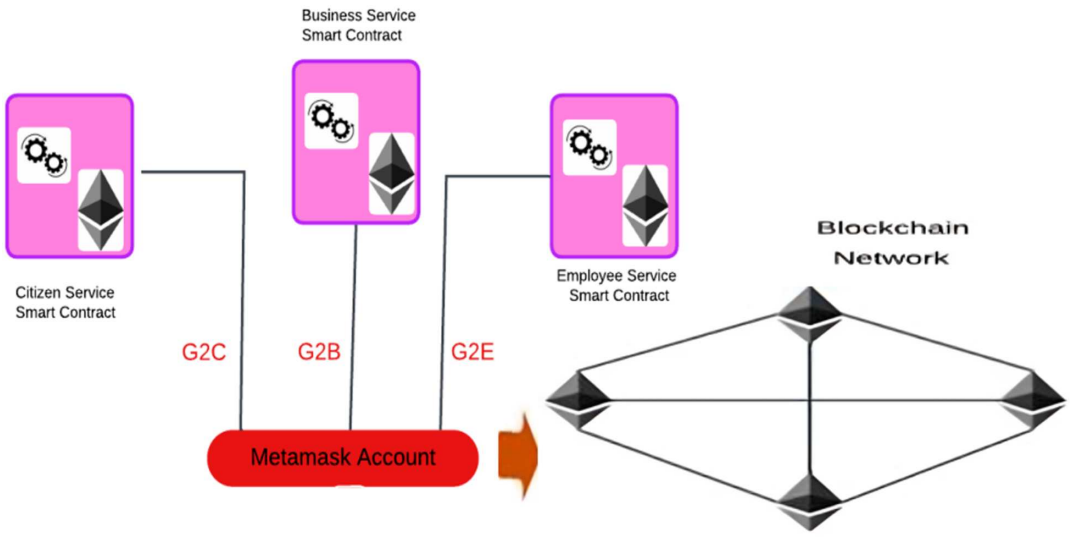



**Figure 4**
**Network architecture of proposed system**




smart contract. Then it can send the data to the blockchain network. The blockchain executes the transaction on all nodes before sending it to the validator. The validator creates a new block using the PoS (proof of stake) consensus mechanism. The new block is added to the blockchain network once the validator has verified it. The transaction is completed once the new block has been successfully integrated into the blockchain. Figure 6 depicts the real-time block in Ethereum. This block represents a smart contract transaction that involves uploading information. This step confirms that data has been stored in a block on the Ethereum network. Blockchain technology improves the trustworthiness and reliability of service information.

### 3.4. Detail explanation about implementation

In this subsection, we will look at how the government and the informant parts of the blockchain are being implemented. The informer side of the blockchain refers to the process of initiating transactions, signing them with a private key, and broadcasting them to the network for inclusion in a block. From the government's perspective, the procedure entails using the public key infrastructure to ensure that the data has not been altered, cryptographic techniques to confirm the data's validity and integrity, and querying the blockchain to obtain specific information. Figure 7 depicts the informer side of blockchain architecture and how to add data to

**Figure 5**
**Creation of block in proposed blockchain-based system**

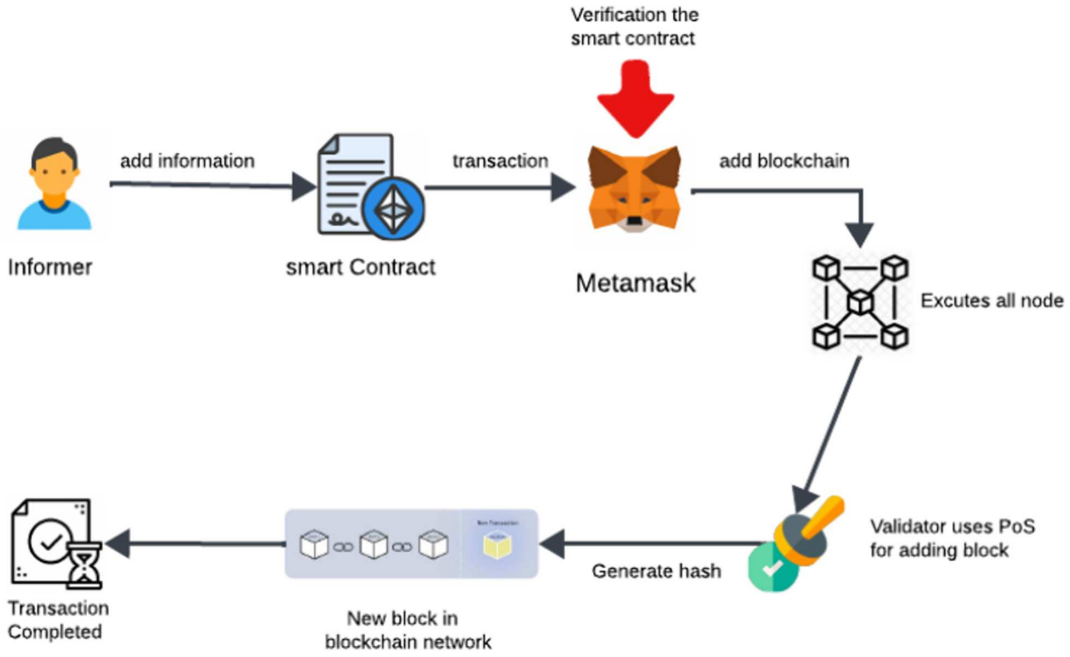
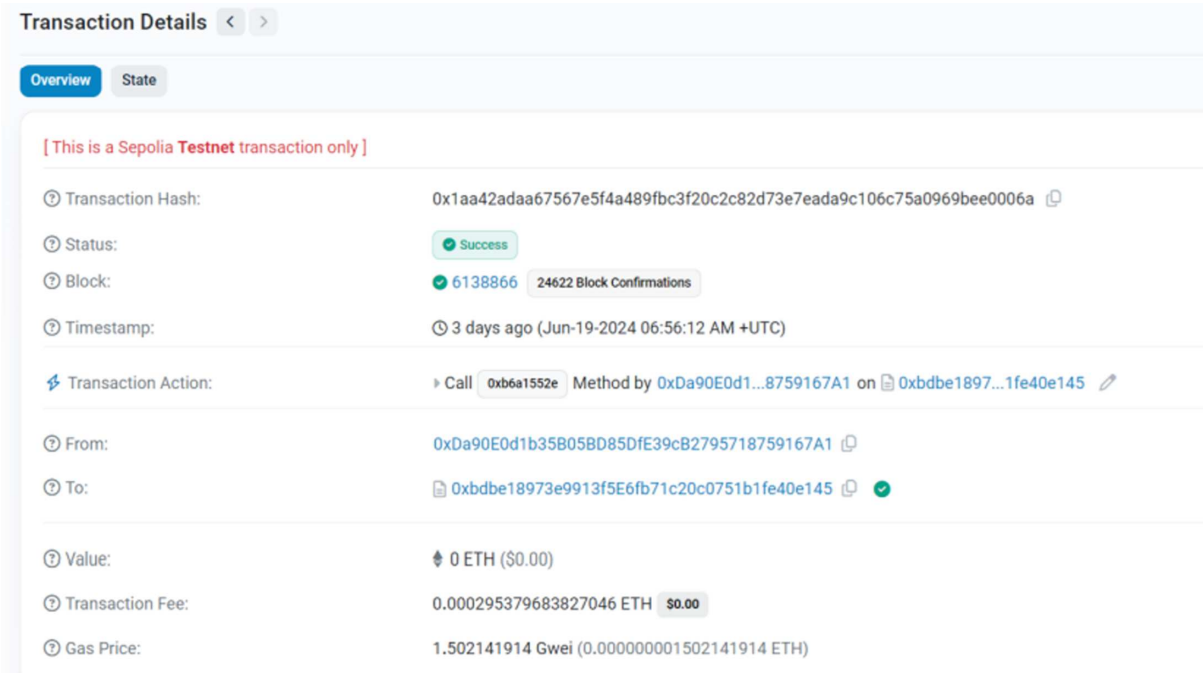



**Figure 6**
**A real-time block in Ethereum**




MetaMask, IPFS, and Ethereum. It explains how to create transactions, use MetaMask to sign them with a private key, save the data to IPFS, and broadcast the transaction to the Ethereum network for inclusion in a block. On the informant side of the blockchain architecture, there are several components to an information transaction. Figure 7 shows that the first informers chose the public blockchain account for operation. Informers enter data into the public MetaMask account. A public MetaMask account requires ETH to conduct transactions and sends a confirmation message. A transaction cannot take place if the informer's account is low on ETH. After the informer confirms the transaction, the public account connects to both the Ethereum network and IPFS. The public account uploads files to IPFS and contributes data to the Ethereum network. The Ethereum network and IPFS communicate with one another via addresses (hashes). The public account gets its address from the Ethereum network. Figure 8 depicts the government side of blockchain architecture. Figure 8 demonstrates how to obtain information from MetaMask, IPFS, and Ethereum. It describes how

**Figure 7**
**Informer side of blockchain architecture**

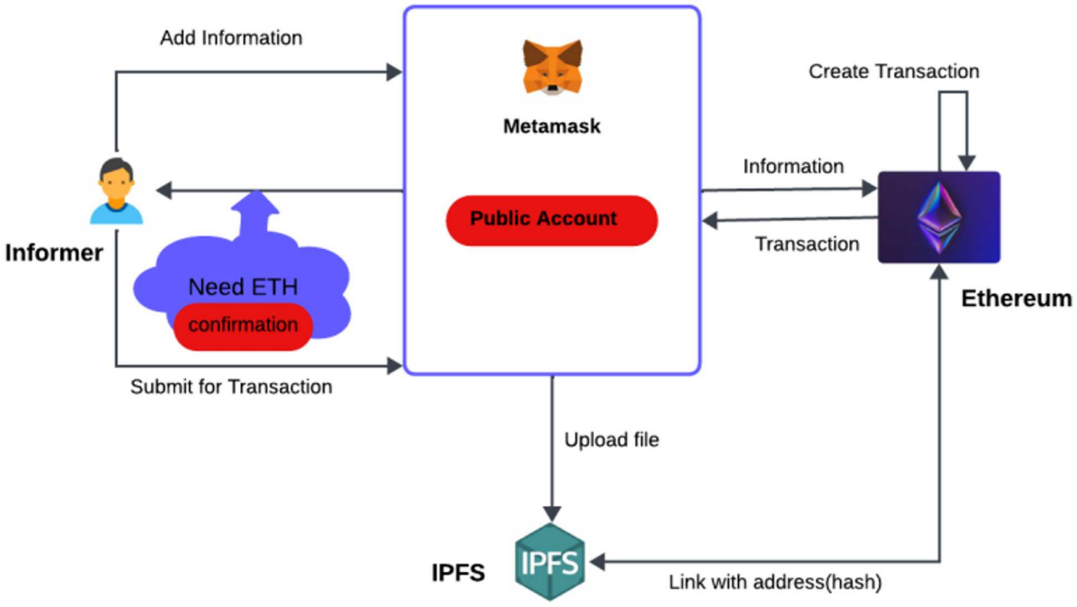
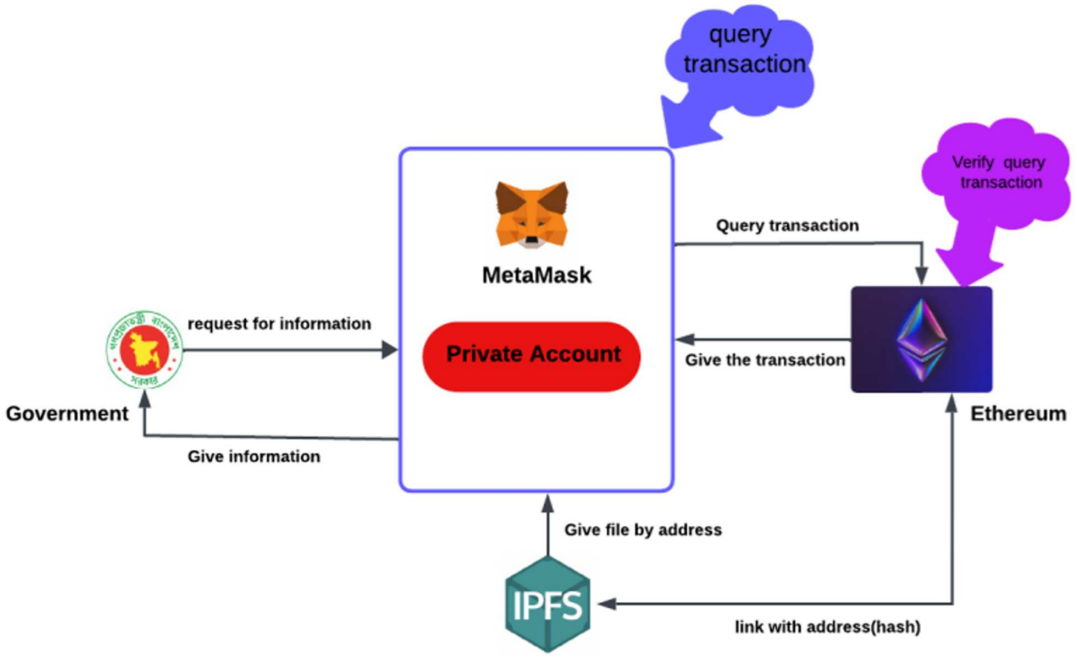



**Figure 8**
**Government side of blockchain architecture**




to query the blockchain with MetaMask to retrieve data stored on IPFS and then verify the data's authenticity and integrity on the Ethereum network using cryptographic techniques. The information transaction on the government side of the blockchain architecture consists of several components. The government authority first selects the private blockchain account for operation. The government authority sends data requests to the private MetaMask account. A private MetaMask account generates a query transaction and submits it to the Ethereum network. The Ethereum network verifies the query transaction issued from the private MetaMask account. The Ethereum network and IPFS communicate with one another via addresses (hashes). The private account retrieves information from the Ethereum network. IPFS sends the file to the private MetaMask account using its address.

## 3.5. Deploy smart contract on MetaMask

Figure 9 depicts smart contracts for three different services. We set up three different service smart contracts. Figure 9(a), (b), and (c) depicts the main components of the smart contracts for citizens, business, and employee services, respectively. Informants can add information to the smart contract and initiate the

**Figure 9**
**Smart contract of proposed system: (a) citizen service, (b) business service, and (c) employee service**

(a)

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract CitizenService {
    struct CInformation {
        string ownernid;
        string ownername;
        string owneraddress;
        string bank_acc;
        string mobile_no;
        string service_name;
        string payment;
    }
```

(b)

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract BusinessService {

    struct BInformation {
        string ownernid;
        string ownername;
        string owneremail;
        string bank_acc;
        string mobile_no;
        string service_name;
        string description;
    }
```

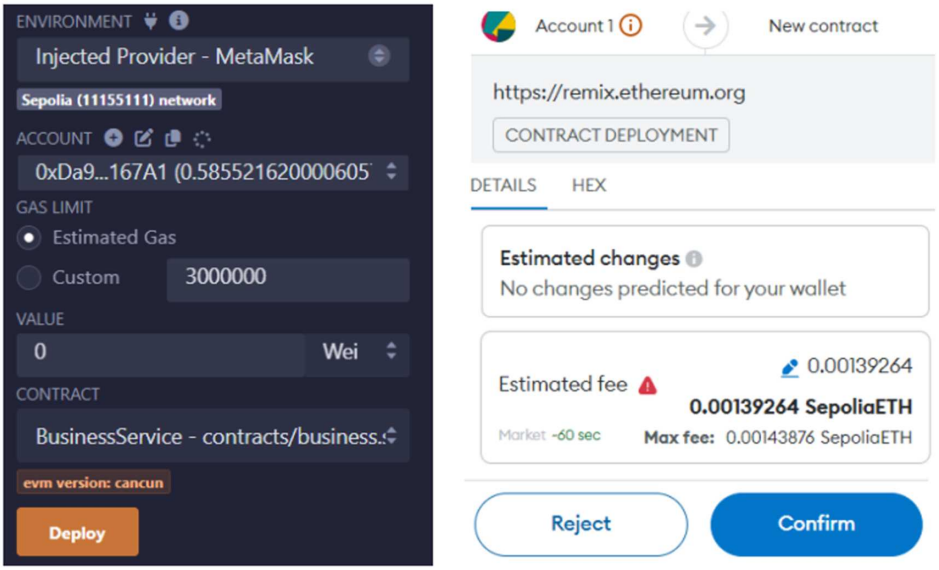
(c)

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract EmployeeService {

    struct EInformation {
        string ownernid;
        string ownername;
        string job;
        string email;
        string salary_update;
        string problem;
    }
```

**Figure 10**
**Deploy smart contract on MetaMask**




transaction creation process. The government can see the user information from smart contracts. Citizen service smart contracts contain information such as the owner's national identification number (NID), name, address, bank account, mobile number, service name, and payment. Smart contract creation for business services includes features such as the owner's NID, name, email, bank account, mobile number, service name, and description. Employee service smart contract creation includes details such as the owner's NID, name, email, job, salary update, and problem type. Citizen service at this job entails applying for a visa, paying utility bills, and paying taxes. The business service includes financial assistance and e-tendering. Salary updates, emergency information, and government interactions are all examples of employee services. Figure 10(a) depicts the deployment of a smart contract on MetaMask, while Figure 10(b) depicts the confirmation of that deployment. First, we injected the smart contract into MetaMask. The MetaMask account is then shown on Remix IDE. At this point, we press the deploy button in Remix IDE. The MetaMask account displays the estimated gas price. Then we confirm the MetaMask account. Following that, it takes time for confirmation before deploying the smart contract on the Meta Mask account. We deploy three types of smart contracts on the MetaMask account: citizen service, business service, and employee service. Figure 11 depicts the various services of the proposed system: citizen service, business service, and employee service. Each service is created using a specific type of smart contract. Smart contracts connect to a MetaMask account. Figure 12 depicts adding information to the MetaMask account. Data for citizen service includes NID, address, name, service name, and payment method. We press the "Send" button to save this information to our MetaMask account. This process ensures that citizen service data is seamlessly integrated into the MetaMask platform. Services are divided into three categories: business, employee, and citizen services. To ensure that people's needs and concerns are met, citizen service focuses on providing direct assistance and resources to the public. Business services meet the needs of businesses and organizations, allowing them to expand and function smoothly. The goal of employee service is to improve

**Figure 11**
**Services of the proposed system**


**Figure 12**
**Add information to MetaMask account**


employees' overall job satisfaction and productivity by assisting them with a variety of workplace issues.

Figure 13 depicts the confirmation of a MetaMask account. MetaMask enhances user interaction with blockchain networks by securely storing users' private keys and managing their Ethereum accounts. Users can create custom tokens by entering token contract information, and the system records transaction history in addition to signing and sending transactions. MetaMask integrates with decentralized applications (dApps) to enable even safer and more convenient data exchanges and interactions. Typically, we established a connection with MetaMask to handle our Ethereum transactions efficiently and securely. Each transaction carries an estimated charge to ensure efficient processing. Fortunately, there is enough ETH in the MetaMask account to complete this transaction without any issues. We double-check all the information, including the recipient's address and the amount being sent, before completing the transaction. Furthermore, we confirm that the estimated cost is reasonable and fits within our budget. After verifying that everything is correct and satisfactory, we press the "Confirm" button to approve the transaction. This final stage secures the transaction on the Ethereum blockchain while also approving it. Once this procedure is completed, the necessary data is seamlessly integrated with our MetaMask account, ensuring a dependable and simple transaction experience. Figure 14 depicts the government-side view of our proposed system. We converted the MetaMask account into a private MetaMask account. Using this figure, we can access government-side information about the blockchain network.

**Figure 13**
**Submit information to MetaMask account**

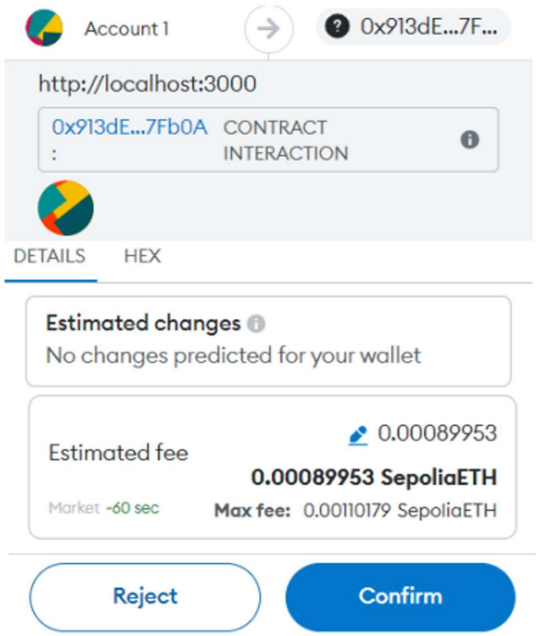



Figure 15(a) depicts how the citizen service manages various data, including the owner's NID, name, and address, to provide a complete profile of each citizen. Additional data fields include the owner's bank account information and mobile phone number, ensuring secure and efficient communication and transactions. Each service used by the citizen is documented with a service name and payment information. This structured data enables streamlined service delivery, accurate recordkeeping, and effective management of citizen services. Figure 15(b) shows that the employee service data field includes the owner's NID, name, and job title, which provides detailed information about each employee. It also includes the employee's email address for communication, as well as salary updates to track compensation changes over time. In addition, the system records any reported problems or issues involving the employee. This organized data management enables efficient HR operations, accurate recordkeeping, and timely resolution of employee concerns. Figure 15(c) depicts the business service data fields, which include the owner's NID, name, and address, resulting in detailed profiles of business owners. It also saves the owner's bank account information, mobile phone number, and email address to ensure secure transactions and effective communication. Each business service is documented with a service name and description. This organized data management enables more efficient service delivery, accurate recordkeeping, and improved business operations.

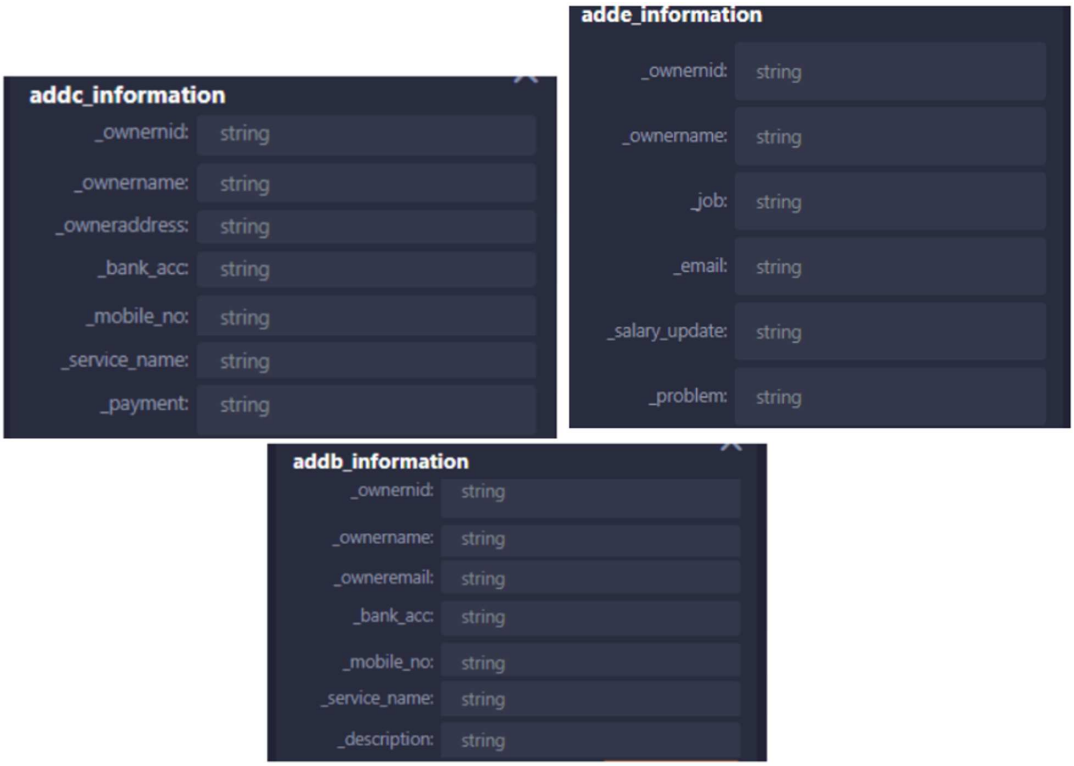
## 3.6. Security attack analysis

This subsection delves into a variety of security analysis topics, including virus attacks, man-in-the-middle (MITM) interceptions, double-spending incidents, and sneaky Sybil attacks. Figure 16 depicts the scenario for two different types of attacks. Figure 17 shows our proposed system's security measures against malware, MITM attacks, DDoS attacks, and the Sybil attack. A malware attack is a malicious act in which software is used to infiltrate a

**Figure 14**
**Government side view of proposed system**

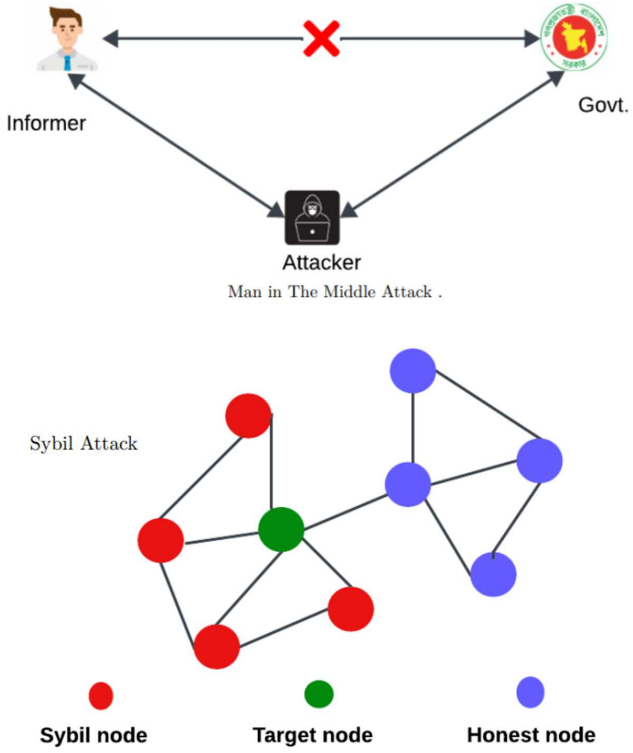

| Nation ID | Name | Address | Bank Account | Mobile Number | Service Name | Payment Option |
|---|---|---|---|---|---|---|
| 5678989765 | Md. karib | Satkhira,Khulna | 01018934871888 | 01732456576 | Passport fee | Sonali Bank |

**Figure 15**
**Data fields for citizen service, employee service, and business service**




computer system or network with the intent of damaging, exploiting, or otherwise compromising it. Malware can steal financial information and passwords once installed. Malware may occasionally encrypt or lock files and demand a ransom to unlock them. Our proposed work uses a decentralized blockchain to store data rather than in a single central location but rather across multiple nodes. Malware cannot take control of the entire system by infecting a single node, making it more difficult to disrupt the entire network. Blockchain verifies transactions through consensus methods such as proof of stake (PoS). Because most nodes need to be agreed on the transaction validation, malware has a difficult time introducing dangerous or fake data. A MITM attack can show many avatars, including eavesdropping on unprotected Wi-Fi networks and tampering with HTTPS communications. Attackers can gain unauthorized access to confidential data by employing tactics like packet injection or session hijacking. After that, the attacker has the ability to eavesdrop, steal data, modify messages, confuse recipients, or alter data. Blockchain utilizes SSL (Secure Socket Layer) along with TLS (Transport Layer Security). TLS can encrypt transmitted data between blockchain apps and users. This encryption

**Figure 16**
**Man-in-the-middle attack and Sybil attack**




ensures that unauthorized parties cannot read the intercepted data. To prevent malicious actors from impersonating nodes, SSL/TLS also uses digital certificates to authenticate node identities. When establishing an SSL/TLS connection, the secure handshake procedure generates an encrypted link and verifies the node's legitimacy. Although TLS provides additional security to user interactions on blockchain platforms, blockchain transactions are still secure on their own. A distributed denial of service (DDoS) attack generally occurs due to its relationship with a single server-based system. The blockchain's decentralized network topology eliminates a single point of failure and allows for the prevention of DDoS attacks. Data dissemination across multiple nodes ensures that the system will continue to function even if some nodes are compromised. Consensus procedures, such as PoS, are implemented by requiring validation from multiple nodes, thereby improving network security. Traffic spikes can be effectively managed by rate limiting and load balancing among nodes, preventing any single node from becoming overloaded. Furthermore, the immutability and inherent transparency of blockchain technology facilitate the early detection and mitigation of malicious activity. A Sybil attacker can create multiple false identities. The attacker's goal is to gain excessive authority or influence within the network. National IDs may bolster Sybil's attacks. When attackers must provide a verified ID to register an account, it becomes more expensive and difficult to create multiple false identities. The network may maintain integrity and trust by requiring national IDs for participation, significantly reducing the possibility of Sybil attacks. We have used PoS to deal with the Sybil attack. PoS can help to prevent Sybil attacks by making them more costly. Users put their money into PoS to participate in validation. A significant amount of cryptocurrency must be purchased and staked, discouraging attackers from attempting to take over the network by establishing a large number of phony nodes.

**Figure 17**
**Attacks and their security measures**

Attacks and their security measure methods

| Attack | Security measure Method |
|---|---|
| Malware | Decentralized data server |
| Man-in-the-middle | Web secure socket, SSL, TLS |
| DDoS | Decentralized data server, PoS |
| Sybil | Access control using NID, PoS |

## 3.7. Performance evaluation

The Remix IDE's unit testing feature allows for efficient testing of smart contracts within a development environment. We can create and run extensive test suites in the browser using Remix's testing plugins, such as Solidity Unit Testing and Remix Tests. This method allows contract logic to be quickly iterated and debugged, ensuring dependability before deployment to the Ethereum network. When Remix IDE is integrated into the testing workflow, it improves efficiency by seamlessly integrating with contract creation and testing processes.

**Table 1**
**Unit testing and service cost estimation**

| Test cases | Pass | Citizen service | Business service | Employee service |
|---|---|---|---|---|
| 3 | 3 | 0.41 s | 0.71 s | 0.46 s |
| 5 | 5 | 1.03 s | 1.10 s | 1.02 s |
| 10 | 10 | 2.5 s | 3.07 s | 2.91 s |

**Table 2**
**Service delay and monetary cost in citizen service**

| Consumer | Transaction | Gas price | Time delay |
|---|---|---|---|
| Informer | Create smart contract | 0.167 ETH | 43 s |
| Informer | Add information | 0.0055 ETH | 25 s |
| Government | Get information | 0 ETH | 0 s |
| Total | | 0.0222 ETH | 68 s |

Unit testing is a type of software testing in which individual program units or components are tested independently of the overall application. Unit testing is used to ensure that all software units work as intended. These tests improve code quality, make future maintenance and restructuring easier, and help identify and correct errors early in the development process. Table 1 depicts unit testing results in citizen service. The first run completed three tests in 0.41 s, the second five in 1.03 s, and the third ten in 2.5 s. Every test passed on every iteration, indicating a stable and trustworthy codebase. Table 1 also depicts unit testing results in business services. The first run completed three tests in 0.71 s, the second five in

**Table 3**
**Service delay and monetary cost in business service**

| Consumer | Transaction | Gas price | Time delay |
|---|---|---|---|
| Informer | Create smart contract | 0.0257 ETH | 43 s |
| Informer | Add information | 0.0079 ETH | 27 s |
| Government | Get information | 0 ETH | 0 s |
| Total | | 0.0336 ETH | 70 s |

1.10 s, and the third ten in 3.07 s. Table 1 also displays unit testing results in employee service. The first run completed three tests in 0.46 s, the second five in 1.02 s, and the third ten in 2.91 s. Every test passed on every iteration, indicating a stable and trustworthy codebase.

In MetaMask, this duration is calculated using the transaction time delay, which is the difference between transaction submission and confirmation times. When a MetaMask transaction is submitted to the blockchain network, the validation process begins. The exact moment of confirmation is recorded after the transaction has been verified. The total time required for the transaction to be successfully added to the blockchain can be calculated by subtracting the submit time from the confirmation time. The amount of computing power required to perform actions on blockchain networks such as Ethereum is measured in units called gas. It represents a fee that users must pay in order to use smart contracts and complete transactions.

The gas fee ensures both efficient use of network resources and payment to miners for their labor. This technology helps with workload management and network security. Table 2 depicts the monetary cost and service time delay for various transactions in citizen service, including features such as gas price, transaction details, and actual time spent. Each entry specifies the cost of a transaction as well as the time it will take to complete. This enables a clear comparison of costs and efficiency across multiple transactions. Users can examine the figure to determine the most cost-effective and time-efficient options for their citizen service needs. The total service time per day is the sum of smart contract creation time, added information time, and information retrieval time delay. Table 2 shows that the gas price (monetary cost for service) and service completion time delay for citizen service are 0.022 ETH and 68 s, respectively. Table 3 depicts the cost and time for various business transactions, including gas prices, transaction details, and actual time taken. Each entry specifies the cost of a transaction as well as the time it will take to complete. This enables a clear comparison of costs and efficiency across multiple transactions. Users can use the table to identify the most cost-effective and time-efficient options for their business services requirements. Table 3 shows that the gas price (monetary cost of service) and service completion time delay for business services are.033 ETH and 70 s, respectively. Table 4 shows that the gas price (monetary cost of service) and the service completion time delay for employee service are 0.023 ETH and 65 s, respectively.

## 4. Comparison Results

Table 5 depicts a comparison of service completion time to existing works [23, 24]. According to the results of the service completion delay efficiency comparison, the proposed system outperforms existing work by Alaslani et al. [23] and Zhang et al. [24] by more than 33% and 64%, respectively. The reason for this is that we used PoS as a consensus algorithm, whereas the current system uses PoW (proof of work). We also compared our proposed blockchain-based system to the traditional system in Bangladesh (Figure 18). We can see that the current system is centralized and vulnerable to malware attacks, MITM attacks, and cyber fraud issues. Our e-government system is built on blockchain technology and can provide security against various types of attacks. Table 6 shows a feature-based comparison of our proposed work to previous works (Mukherjee et al., 2020), [15, 16]. Table 6 clearly shows that existing work by Hingorani et al. [11] is limited to police FIR services and public blockchain-based systems. However, the existing work by Chentouf and Bouchkaren [16] is limited to smart city applications. They did not use a consensus algorithm. Unlike our

**Table 4**
**Service delay and monetary cost in employee service**

| Consumer | Transaction | Gas price | Time delay |
|---|---|---|---|
| Informer | Create smart contract | 0.0195 ETH | 41 s |
| Informer | Add information | 0.0043 ETH | 24 s |
| Government | Get information | 0 ETH | 0 s |
| Total | | 0.02386 ETH | 65 s |

**Table 5**
**Comparison with existing works**

| Previous works | Blockchain platform | Consensus algorithm | Service completion time | Solution efficiency |
|---|---|---|---|---|
| Alaslani et al. [23] | Ethereum or Bitcoin | PoW | 100 s | 33% more delay than our proposed system |
| Zhang et al. [24] | Ethereum | PoW | 189 s | 64% more delay than our proposed system |
| Our proposed scheme | Ethereum | PoS | 67.33 s | Save at least 33% and up to 64% delay |

**Figure 18**
**Features-based comparison between proposed and existing e-government system**

Blockchain E-government vs Traditional E-government

| Features | Our Proposed System | Traditional E-government |
|---|---|---|
| Control | Decentralized | Centralized |
| Storage | all nodes | single node |
| Data Transfer | Real-Time Data | Normal Data |
| Working Time | Not Effected | Effected |
| Creativity | More | Less |
| Malware Attack | Low Risk | High Risk |
| Man in the middle | Low Risk | High Risk |
| Cyber Fraud | Low Risk | High Risk |

**Table 6**
**Feature-based comparison (proposed vs. existing)**

| Features | Our system | Mukherjee et al. (2020) | Chentouf et al. (2023) | Elisa et al. [15] |
|---|---|---|---|---|
| Main focus | E-government | FIR system | Smart cities | E-government |
| Blockchain types | Permissioned based | Public blockchain | N/A | Permissioned based |
| Blockchain platform | Ethereum | Ethereum | Ethereum | N/A |
| Consensus algorithm | PoS | N/A | N/A | DPoS |
| Methods of data storage and management | IPFS | IPFS | N/A | N/A |
| Energy saving | Saving | N/A | N/A | Saving |
| Performance analysis of blockchain | Time and gas analysis | N/A | N/A | N/A |

proposed work, the existing work did not address service completion delay reduction or alternative attack mitigation. We have tested up to 80,000 users at a time; our system works well. For more users, we tried to add additional cloud and storage to increase scalability.

## 5. Conclusion

This paper dispatches a decentralized blockchain-based E-government system for the Bangladeshi people that prioritizes security and privacy while accommodating multiple services and users. Our proposed system provides citizen, employee, and business services simultaneously, as well as performance comparisons. Our proposed blockchain-based e-government system integrates informers, government authorities, smart contracts, MetaMask-based public and private wallets, Ethereum, and the IPFS. It uses smart contracts to make visa applications, utility payments, tax submissions, emergency information updates, salary notifications, financial support, and e-tenders more efficient. Informants upload their transactions to Ethereum and the IPFS, ensuring transparent and secure data storage that is available for government inspection and action. The proposed system provides appropriate security measures for malware, DDoS, and Sybil attack mitigation. Our proposed blockchain-based e-government system looked into the service completion time and monetary cost delays associated with employee, business, and citizen services. Our performance comparison results showed that the proposed decentralized blockchain-based e-government system could outperform the existing system's service completion time by at least 33%. The proposed system can be used for any blockchain-based e-government system implementation. In the future, we plan to use machine learning technology to forecast cybersecurity threats to the e-government system. In the future, quantum computing can be combined with advanced encryption and decryption procedures to reduce time complexity while also improving security and privacy. We will attempt to incorporate an advanced consensus mechanism to reduce the service completion delay and throughput of the proposed scheme. We will also try to determine the time complexity of our proposed system. Another future research challenge is to create a deep learning, Artificial intelligence (AI), and IoT-based real-time cyberattack classification and prevention system for the e-government system.

## Recommendation

The results suggested that a blockchain-based e-government system with MetaMask, Ethereum, and IPFS offers better security and privacy, along with lower service completion delay for e-government applications.

## Acknowledgment

The authors are grateful to Chittagong university of engineering and technology (CUET), computer science and engineering (CSE) department for research facilities.

## Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

## Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

## Data Availability Statement

The data that support this work are available upon reasonable request to the corresponding author.

## Author Contribution Statement

**Nahid Imtiaz:** Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Visualization. **Mahfuzulhoq Chowdhury:** Conceptualization, Methodology, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration.

## References


[1] Aspire to Innovate. (2022). *E-government is the present and the future*. Retrieved from: https://a2i.gov.bd/e-government-is-the-present-and-the-future/

[2] Ahmad, T. (2021). E-government in Bangladesh: Development and present state. *International Journal of Social Science and Human Research*, *4*(1), 557–567. https://doi.org/10.47191/ijsshr/v4-i1-15

[3] Dubey, R. S. (2015). Corruption and the role of middlemen. *SSRN*.

[4] Parvez, S. (2016). Terrorism and counter-terrorism in Bangladesh. In A. Riaz & M. S. Rahman (Eds.), *Routledge handbook of contemporary Bangladesh* (pp. 425–437). Routledge.

[5] Haokip, T. L. (2015). Ethnic separatism: The Kuki-Chin insurgency of Indo-Myanmar/Burma. *South Asia Research*, *35*(1), 21–41. https://doi.org/10.1177/0262728014560473

[6] Bhardwaj, S. K. (2013). India–Bangladesh border governance: Issues and challenges. *International Studies*, *50*(1–2), 109–129. https://doi.org/10.1177/0020881716654387

[7] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *IEEE International Congress on Big Data*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

[8] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, *7*, 117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094

[9] Khayyat, M., Alhemdi, F., & Alnunu, R. (2020). The challenges and benefits of blockchain in e-government. *International Journal of Computer Science and Network Security*, *20*(4), 15–20.

[10] Hou, H. (2017). The application of blockchain technology in e-government in China. In *26th International Conference on Computer Communication and Networks*, Vancouver, BC, Canada. 1–4. https://doi.org/10.1109/ICCCN.2017.8038519

[11] Hingorani, I., Khara, R., Pomendkar, D., & Raul, N. (2020). Police complaint management system using blockchain technology. In *3rd International Conference on Intelligent Sustainable Systems*, 1214–1219. https://doi.org/10.1109/ICISS49785.2020.9315884

[12] Mukherjee, A., & Halder, R. (2020). Policechain: Blockchain-based smart policing system for smart cities. In *13th International Conference on Security of Information and Networks*, 6. https://doi.org/10.1145/3433174.3433618

[13] Mali, D., Mogaveera, D., Kitawat, P., & Jawwad, M. (2020). Blockchain-based e-tendering system. In *4th International Conference on Intelligent Computing and Control Systems*, 357–362. https://doi.org/10.1109/ICICCS48265.2020.9120890

[14] Al-Ameri, H. H., & Ayvaz, S. (2023). A blockchain-based secure mutual authentication system for e-government services. In *3rd International Scientific Conference of Engineering Sciences*, 19–24. https://doi.org/10.1109/ISCES58193.2023.10311497

[15] Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving e-government system. *Wireless Networks*, *29*(3), 1005–1015. https://doi.org/10.1007/s11276-018-1883-0

[16] Chentouf, F. Z., & Bouchkaren, S. (2023). Security and privacy in smart city: A secure e-voting system based on blockchain. *International Journal of Electrical and Computer Engineering*, *13*(2), 1848–1857. https://doi.org/10.11591/ijece.v13i2.pp1848-1857

[17] Srivastava, S. C., & Teo, T. S. H. (2010). E-government, e-business, and national economic performance. *Communications of the Association for Information Systems*, *26*, 14. https://doi.org/10.17705/1CAIS.02614

[18] Chen, Y. C. (2010). Citizen-centric e-government services: Understanding integrated citizen service information systems. *Social Science Computer Review*, *28*(4), 427–442. https://doi.org/10.1177/0894439309359050

[19] Stefanovic, D., Marjanovic, U., Delić, M., Culibrk, D., & Lalic, B. (2016). Assessing the success of e-government systems: An employee perspective. *Information & Management*, *53*(6), 717–726. https://doi.org/10.1016/j.im.2016.02.007

[20] Zhang, Y., Xu, C., Li, H., Yang, H., & Shen, X. (2019a). Chronos: Secure and accurate time-stamping scheme for digital files via blockchain. In *IEEE International Conference on Communications*, 1–6. https://doi.org/10.1109/ICC.2019.8762071

[21] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

[22] Górski, T. (2024). Smart contract design pattern for processing logically coherent transaction types. *Applied Sciences*, *14*(6), 2224. https://doi.org/10.3390/app14062224

[23] Alaslani, M., Nawab, F., & Shihada, B. (2019). Blockchain in IoT systems: End-to-end delay evaluation. *IEEE Internet of Things Journal*, *6*(5), 8332–8344. https://doi.org/10.1109/JIOT.2019.2917226

[24] Zhang, Y., Xu, C., Cheng, N., Li, H., Yang, H., & Shen, X. (2019b). Chronos$^{+}$: An accurate blockchain-based time-stamping scheme for cloud storage. *IEEE Transactions on Services Computing*, *13*(2), 216–229. https://doi.org/10.1109/TSC.2019.2947476


**How to Cite:** Imtiaz, N., & Chowdhury, M. (2025). A Blockchain Based Secure and Privacy Preserving Smart E-Government Application Execution System with Reduced Service Completion Delay. *Journal of Comprehensive Business Administration Research*. https://doi.org/10.47852/bonviewJCBAR52024714