Blockchain-Based Autonomous Authentication and Integrity for Internet of Battlefield Things in C3I System

AQSA RASHID\textsuperscript{1} AND ATTA UR REHMAN KHAN\textsuperscript{2}, (Senior Member, IEEE)

\textsuperscript{1}Department of Information Security, National University of Sciences and Technology, Islamabad 44000, Pakistan
\textsuperscript{2}College of Engineering and Information Technology, Ajman University, Ajman, United Arab Emirates

Corresponding author: Atta Ur Rehman Khan (dr@attaurrehman.com)

This work was supported by the Deanship of Graduate Studies and Research (DGSR) Program, Ajman University, United Arab Emirates.

\textbf{ABSTRACT} In the Internet of Battlefield Things (IoBT), users and sensor-equipped entities send multiple messages to the Command Control Center (CCC) over the network. The authentication and integrity of these messages are crucial because if an adversary or malicious node transmits, alters, or replays these messages, the consequences will be disasters. Current centralized authentication systems are not suitable for the distributed environment because such schemes are prone to a single point of failure, privacy, and scalability issues. Moreover, the high communication overhead caused by centralization increases energy consumption. In this work, we propose a technique called Blockchain-based Autonomous Authentication and Integrity for the Internet of Battlefield Things (BIoBT) for the C3I system. The proposed technique does not require an explicit authentication channel for the authentication of entities because it is performed on the blockchain side when receiving the data. In addition, it provides data integrity and non-repudiation. BIoBT prototype is created, deployed, and tested on the Ethereum test network. The results prove that BIoBT is efficient, cost-effective, and satisfies the security requirements of a distributed environment for IoBT. BIoBT also outperforms contemporary mechanisms in terms of the number of messages required to establish a secure channel, reducing communication overhead and resource consumption.

\textbf{INDEX TERMS} Authentication, autonomous, C3I, Ethereum, Internet of Battlefield Things (IoBT), smart contract.

\section{I. INTRODUCTION}

The Internet of Things (IoT) is present globally in nearly every aspect of life. According to Statista, 29.4 billion IoT-connected devices will be connected by 2030 [1]. IoT applications automate daily life processes, including smart homes, smart parking, smart waste management, smart healthcare, intelligent transportation, traffic management, environmental monitoring, intelligent military wearables, smart battlefield etc. [2], [3]. IoT enables interconnecting intelligent and self-configurable sensor-equipped entities to create a platform for secure collaboration and communication [4].

Authentication is essential in IoT ecosystems for identifying legitimate IoT for secure network communication. The CCC must receive information from reliable sources as the adversary conducts multiple cyberattacks on the battlefield to gain superiority. Typically, the adversary attempts to gain control over IoT entities through communication. If the enemy seizes communications control, they can send CCC false information. It is necessary to establish trust in which the interacting parties ensure that the data comes from a legitimate source. If CCC cannot verify the source, it will execute enemy commands. This situation can turn a battlefield in favor of the enemy and cause damage to one’s forces.

Due to the resource-constrained and heterogeneous nature of IoTs [3], conventional schemes are unsuitable for usage [5]. There is a need for an efficient authentication scheme that...
utilizes less computational power, requires low storage space, and has a low communication overhead. Present state-of-the-art authentication schemes proposed for IoT are centralized [6], [7], [8], [9], [10], [11], [12], [13], [14]. In centralized schemes, Centralized Authority (CA) or Trusted Third Party (TTP) is responsible for the authentication of things. Due to centralization, such methods are susceptible to a single point of failure, security threats, privacy concerns, and scalability challenges. In addition, centralization techniques are less energy efficient because of the high communication overhead.

Over the past few years, blockchain technology [15], [16], [17], [18] has emerged as a viable alternative for providing IoT identification and access control services. Researchers have developed decentralized blockchain-enabled authentication techniques to circumvent the problems associated with centralized schemes [19], [20], [21]. Although these schemes show promising results, they suffer from severe limitations regarding the initialization phase, limited communication scope, and dependence on trusted fog nodes. In addition, communication overhead is a major concern when the association phase for establishing secure communication requires numerous messages to complete the authentication process.

This paper presents a new Blockchain-based Autonomous Authentication and Integrity technique for the IoBT (BIoBT) in the C3I system. This technique uses a blockchain-based association based on the trust in the IoBT. The IoBTs entities obtain a digital identity by using association to present themselves to the CCC. The entities establish the data source authenticity by verifying the association relation at the blockchain in a decentralized manner. Due to the trust established through the association, the proposed scheme does not require the establishment of an explicit authentication channel. The collected data and authentication data are delivered to the CCC for decision-making. The recipient autonomously verifies the sender’s association trustworthiness to authenticate the sender IoBT. Unlike negotiation-based authentication schemes, this authentication method is fast and does not occupy a communication channel. The time factor is essential in the battlefield because it impacts the speed of decision-making and the action against the enemy. BIoBT aims to achieve autonomous authentication, integrity assurance, privacy preservation, and decentralized trust. The major contribution of this work are summarized as follows:

- Comprehensive review and analysis of the blockchain-based state-of-the-art techniques for the IoBT.
- A new blockchain-based architecture for IoBT and C3I systems called BIoBT.
- Proof of Concept (PoC) implementation of the BIoBT.
- Experimental evaluation and comparison of BIoBT with the existing techniques.

Table 1 presents the list of acronyms and their definitions used in this paper.

The rest of the paper is organized as follows. Section II presents motivation and related work, Section III presents the proposed technique, i.e., BIoBT, Section IV presents implementation, evaluation, and discussions, and Section V presents a qualitative comparison of the proposed scheme with the existing schemes. Finally, Section VI presents conclusions and future work.

### II. RELATED WORK

The battlefield contains entities (things) that are more or less intelligent and perform a wide range of tasks, such as data collection, communication, and performing specific activities (individual and mutual). The entities are laptops, mobile, sensors, ammunition, weapons, vehicles, robots, and human-wearable devices. Some entities are autonomous and monitored on the battlefield, while the others are on vehicles, weapons, or soldiers. They collect, process, or transmit data to aggregators, who forward it for further processing. Also, some entities receive processed data through orders to execute actions against the enemy. In other words, entities represent IoT in a military environment called IoBT.

The IoBT environment has many challenges, such as communication of entities with the CCC, adaptation and flexibility to rapidly changing military environments, managing entities, the workload of soldiers with IoBT, and the presence of enemy entities. In this environment, IoBT authentication is essential for managing secure entities and protecting the data sources. In today’s military operations, many sensors are deployed on the battlefield that delivers large amounts of data. Therefore, verifying the authenticity of the data and things in IoBT is challenging. Many researchers have discussed the incorporation of Blockchain and IoBT in military systems. However, to the best of our knowledge, none of the contributions specifically present the autonomous authentication and integrity in the C3I system using blockchain.

In [22], the researchers present the characteristics of C3I and IoBT. They examined the ramifications of the IoBT concept for C3I and demonstrated how IoBT could herald...
in C3I. In addition, they present C3I decision processes. The merger of IoBT and C3I systems present an interesting network-centric, multi-domain area for strategic and tactical operations.

In [23], the researchers propose a blockchain-empowered three-layered architecture for the IoBT. The architecture layers consist of battlefield sensing, consensus, and service and network layers. The battlefield sensing layer includes all the military objects, such as ammunition, weapons, vehicles, robots, human-wearable devices, and soldiers. These objects gather and disseminate data/information about the battlefield and jointly work to achieve a shared goal. The network layer is responsible for capturing and transmitting transactions at the battlefield-sensing layer. The consensus and service layer is responsible for accepting valid transactions from the battlefield layer on a consensus mechanism. For this architecture, the researchers do not provide the Proof of Concept (PoC) to evaluate the practical requirements of an IoBT environment.

In [24], the researchers propose a lightweight blockchain-based technique for IoBT, which consists of three layers; (i) the IoBT layer includes all the warfighters, drones, command centers, and tankers, (ii) the network layer is responsible for capturing and transmitting transactions at the IoBT layer, and (iii) the consensus and service layer is responsible for implementing the blockchain and assigning responsibilities to IoT. The researchers simulate the PoC of a networked battlefield scenario using an NS-3 simulator and use a sharding scheme to efficiently use the IoBT device resources.

In [25], the authors propose a framework for the IoBT network based on blockchain and Named Data Networks (NDN) that only stores information on each node’s ledger, allowing the network to use its resources efficiently. In addition, they propose Interest Groups, a novel network sharding technique. Nodes that store data that is similar to one another are assigned to the same Interest Group. As a result, the network is not flooded with unnecessary interest packets. They also introduce a consensus mechanism called the Proof of Common Interest (PoCI). The results show that segmenting the network achieves efficient packet transmission and reduces packet flooding by segmenting the network.

In [26], the authors propose a UAV-assisted and blockchain-empowered Device-to-Device communication architecture. This architecture uses a bloom filter to reduce data transmission and improve validation. However, it is not implemented to test the efficiency of blockchain adaptation for military networks. Also, the authors did not propose any solution for the data congestion problem.

In [27], the researchers propose MR-Block, a blockchain-assisted content distribution scheme for mixed reality applications. In this scheme, each entity registers to participate in the system. In addition, before data transmission, a smart contract specifies rules and restrictions for data forwarding. In addition, before granting a user access to data, the smart contract performs validation. The performance results demonstrate the viability of this technique; however, the authors failed to address the application details, its security analysis, and combining data from heterogeneous devices and converting it to device-friendly data.

In [28], the authors present IoBTChain, an IoT framework based on blockchain and smart contracts. This framework uses a permissioned blockchain to associate cloud resources with each IoBT device account. IoBTChain limits the number of resources an IoBT device can acquire from a cloud server using a credit-based resource management system based on predefined priority parameters, such as application types, rules, and behavior history. This work also presents the usage of blockchain smart contracts for device registration.

In [29], the authors propose a UAV-assisted casualty detection scheme based on blockchain technology. This approach employs public key cryptography for secure data transmission from UAVs to Edge Computing (EC) server. The EC server detects the death of a soldier and stores the information in the blockchain to prevent tampering with previously saved data. In this work, the authors did not mention particulars of block formation among EC servers.

In [30], the researchers propose a Proactive Blockchain-based Spectrum Sharing (ProBLeSS) protocol, which uses blockchain technology to protect against Spectrum Sharing Data Falsification (SSDF) attacks in Cognitive Radio (CR)-based IoBT networks. The simulation results show that ProBLeSS reduces backoff rate, channel utilization, and sensing delay during SSDF attacks.

In [31], the authors propose a blockchain-based framework for resource-constrained IoT devices. This framework focuses on three points; (i) split the global blockchain into smaller disjoint local blockchains in a spatial domain to take less space on IoT devices, (ii) limit the size of the local blockchains in the temporal domain; a temporal constraint is imposed on their lifetime, (iii) maintain at least one block of the blockchain in the memory of a sensor node. The results show that this technique is storage efficient.

In [32], the researchers propose a blockchain-based secure communication framework for the Intelligent Battlefield Things (IBT) environment. IBTs are intelligent devices that monitor the enemy’s activities and respond accordingly. This work uses edge nodes to deploy blockchain and collect data from the IBT. It also uses edge servers, assuming that trusted network entities cannot be compromised. In addition, cloud servers are treated as semi-trusted network entities. The results show that this technique is resilient against possible attacks.

In [33], researchers propose a framework that uses blockchain for software-defined Internet of Unmanned Vehicles (IoUV) in battlefield applications. In this framework, blockchain provides trustworthy command and control operations at IoUV and stores operations as transactions in tamper-resistant digital ledgers. Unmanned Vehicles (UVs) serve as miners to validate each transaction and create blockchain blocks. The main aim of this framework is to improve accountability and trust.

In [34], the researchers propose an unconventional security framework for the Internet of Drones (IoDs) using...
blockchain. In this framework, the data is decoupled from the blockchain and does not affect its growth. The researchers use the shrinking block concept that ensures that the size of the block remains small on resource-constrained entities, such as drones. This framework is evaluated using simulations, and the results demonstrate its effectiveness. However, the authors did not consider the effect of the network behavior.

In [35], the authors propose a blockchain-based access control framework for estimating the location of unauthorized UAVs in IoMT. This scheme uses blockchain-based peer-to-peer authentication for user authorization. In addition, it uses CNN-based object location detection to prevent unauthorized access. The results show that the proposed framework works well and provides high detection accuracy.

In [36], the authors propose the usage of blockchain for IoD. The main objective of this work is to provide secure data dissemination with minimal overhead. The authors employ TPM to protect the keys and defend against the attacks targeted to manipulate the firmware of drones. The results show that the proposed technique works quite well for IoD.

In [37], researchers present a technique called HeuCrip for detecting malware in IoBT. HeuCrip uses feature selection, probability graph generation, graph to vector space conversion, and convolution neural network operations to detect malware. The experimental results show that HeuCrip effectively detects the malware with high performance. However, large-scale datasets are not considered in the experimentation.

Table 2 presents an abstract comparison of the reviewed techniques regarding blockchain platforms, evaluation matrices, and security features.

III. PROPOSED TECHNIQUE

Authentication is a critical issue in IoBT for users, sensors, ammunition, vehicles, robots, human-wearable devices, and other entities that collect, process, or execute received instructions. Entity authentication is further complicated by the heterogeneity of IoBT and the use of commercial equipment. In addition, commercial IoTs will likely lack standardization due to manufacturers’ desire to maintain market control. Military requires proper techniques and technologies to adapt to different vendors’ protocols, technologies, and IoT devices. IoBT is a heterogeneous, dynamic, and unpredictably data-rich environment with internal and external communications. This environment needs an approach to facilitate the authenticity of the IoBT or data source, and data integrity. In this work, we emphasize the authenticity of IoBT and data integrity so that the decision-makers can be certain that the data is obtained from a legitimate source and not one planted by the enemy.

The solutions presented for IoT generally have associated limitations (see Figure 1). Since the IoT environment is highly heterogeneous in terms of devices, platforms, network standards, and connectivity, this research aims to introduce trust, security, and privacy challenges with very little or negligible human involvement when battlefield entities send data to the CCC.

![FIGURE 1. Evolution and challenges of authenticity for IoT.](image-url)

A. ARCHITECTURE OF BloBT IN C3I

C3I communication systems allow mobile C3I assets to collaborate effectively during battlefield operations.

1) ABSTRACT VIEW OF THE C3I SYSTEM

In the battlefield scenario, the C3I command and control systems collect tactical data via various devices, such as users, quadcopters, and proximity sensors. With the assistance of a C3I intelligence unit, the control system processes raw data and provides classified information to the command system to achieve mission objectives and a plan by coordinating multiple military units, such as soldiers, helicopters, and armored tanks. Figure 2(a) shows an abstract representation of a C3I system for a military battlefield.

2) KEY PLAYERS

Key players of the BloBT are shown in Figure 2(b). These key players have the following responsibilities:

a: INFRASTRUCTURE REGULATOR

The infrastructure regulating node is the governing node responsible for registering IoBT nodes and creating, updating, and revoking their policies. It uses the Ethereum wallet module to authenticate the regulator devices, send the required Ether to the device to store its public key in the blockchain, and perform governing operations.

b: INFRASTRUCTURE OWNER

The infrastructure owner device is responsible for deploying the smart contract on the blockchain network and authorizing infrastructure regulators to perform governing operations. It uses the Ethereum wallet module to authenticate the devices and send the required Ether to the device to store its public key in the Ethereum blockchain. The infrastructure owner owns the smart contract during the lifetime of the BloBT. On accepting the smart contract at blockchain, the smart contract is recognized by a unique address in the blockchain.
network. All smart contracts’ interacting nodes need to know the unique contract address to communicate with the contract.

c: CONTROL UNIT
The C3I control unit node is responsible for collecting and processing received data from the IoBT and sending it to the command unit.

d: COMMAND UNIT
C3I command unit node generates an action plan according to the processed data to achieve C3I mission objectives.

3) CONNECTED COMPONENTS
As depicted in Figure 2(c), the proposed BIoBT architecture consists of the following connected components:

TABLE 2. Summary of the comparative analysis of the reviewed techniques.

| Ref | Blockchain Platform | Evaluation Matrices | Security Features |
|-----|---------------------|---------------------|------------------|
| S. Russell et al. [22] | - | - | - |
| D. K. Toshet et al. [23] | - | - | Audit |
| FastChain [24] | Sharding enabled blockchain | - | Trustworthiness |
| R. Doku et al. [25] | - | - | - |
| M. Golam et al. [27] | - | - | Malicious cyber-attacks and data loss |
| MR-block [28] | - | Transmission Time, Content Size | - |
| K. Kavya et al. [29] | - | CPU consumption | - |
| IoTChain [30] | Permissioned Blockchain | - | - |
| M. Masuduzzaman et al. [31] | Hyperledger Blockchain | Throughput, delay | - |
| ProBLess [32] | - | - | - |
| Sensor-Chain [33] | Permissioned Blockchain | Long run and scalability | - |
| M. Wazid et al. [34] | - | - | Secure Communication |
| B. Ghimire et al. [35] | - | - | - |
| R. Akter [38] | - | Latency, Throughput, Sensitivity, Specificity | - |
| M. Singh et al. [36] | - | - | Privacy of identities and integrity of data |
| I. A. Shah et al. [37] | - | Sensitivity, Specificity | Detection of malware |

FIGURE 2. Architecture of BIoBT in C3I environment.
CCC and IoBT so that source authentication and information integrity can be maintained during the exchange of information over the network. CCC sends and receives information only from the IoBTs associated with the CCC and considers every other IoBT malicious. Hence, in BIoBT, all IoBTs associated with the CCC are trusted. They are inaccessible and protected from non-associated IoBTs. We use a public blockchain that deploys contracts to achieve the required security objective. All interactions and communications with the IoBT are transactions validated by the blockchain for valid operations.

Figure 3 presents the abstract view of CCC_Sys creation of the BIoBT. CCC_Sys is the synchronization system and decentralized database that autonomously maintains privacy-preserved and temper-proof logs of the events of all the created and revoked associations of IoBTs. In the proposed system design, the operation that creates the CCC_Sys is named Tx-1.

Figure 4 shows the IoBT and CCC abstract view and association procedure. Each time a new association is created for IoBTs, a decentralized database and synchronization system (CCC_Sys) is updated consequently. The operation which creates this association in the CCC_Sys is named Tx-2.

Figure 5 presents authentication and integrity management for transmitting data from IoBTs to CCC. It is shown that E1 and E2 attempt to send data as malicious IoBTs. Moreover, ZZ IoBT attempt to send data to CCC_Sys. Although the validation of the transaction is true as it contains a valid unique public identity, ZZ’s SAK, the blockchain will reject this transaction as the association with CCC_Sys does not exist in the blockchain for this IoBT.

Similarly, the E2 error shows a malicious IoBT attempted to send information to CCC_Sys. In this case, the association (AA IoBTs) exists in the CCC_Sys at the blockchain level, so this malicious IoBT tries to impersonate an existing IoBT. This impersonation only allows it to steal the public identity of the AA; thus, the association’s authenticity will be rejected by the blockchain due to an invalid association. Hence, only the authentic IoBT, having an authentic association with CCC_Sys, allows sending the information considering every other IoBT as malicious. The IoBTs association can be created at any time. The number of IoBTs in CCC is unlimited.
since it relies on entirely decentralized architecture. It is noteworthy that IoBT cannot send data without association or with fake ones. In the proposed system design, the operation that authenticates and ensures integrity before data acceptance in the CCC_Sys is named Tx-3.

CCC_Owner is allowed to revoke association when required during the lifetime of IoBT. Figure 6 presents the abstract view of the revocation phase. It depicts the status of IoBT’s association status after the deletion of CC and DD’s association. The operation that deletes the association in the CCC_Sys is named Tx-4.

C. BIoBT SYSTEM DESIGN

Table 3 presents the symbols and their definitions used in BIoBT.

---

**FIGURE 4.** Association creation between IoBT and CCC_Sys at the blockchain.

**FIGURE 5.** Authentication and data integrity verification before data acceptance.
TABLE 3. Symbols and their definitions.

| Symbol         | Description                                      |
|----------------|--------------------------------------------------|
| AssociationID<sub>IoBT</sub> | IoBT’s auto-generated identity                  |
| AssociationID<sub>IoBT</sub> | IoBT’s identity for association creation         |
| h (.)          | Hash                                             |
| ID<sub>IoBT_Owner</sub>     | IoBT’s owner’s identity                          |
| ID<sub>IoBT</sub>           | IoBT identity                                    |
| ID<sub>CCC_SYS</sub>        | CCC_SYS’s identity                               |
| ID<sub>CCC_SYS</sub>        | CCC_SYS’s auto-generated identity                |
| ID<sub>CCC</sub>            | CCC’s identity                                   |
| SC<sub>BioBT</sub>          | BioBT’s Smart contract                          |
| Tx<sub>ω</sub>             | Transaction identity                             |
| ||                           | Concatenation                                    |

The technical working of BIoBT is divided into four phases, which are discussed as follows:

1) **CCC_SYS CREATION**

Figure 7 presents the flow of CCC_SYS creation at the blockchain. A single CCC manages multiple IoBTs. CCC owner performs the owner role and the infrastructure regulator role. CCC owners create SC<sub>BioBT</sub> and use IDCCC and PSCCCC to deploy SC on the Blockchain. CCC first compute ID<sub>CCC_SYS</sub> = h(ID<sub>CCC_Owner</sub> || ID<sub>CCC</sub>) and sends transaction, Tx<sub>1</sub> = {ID<sub>CCC_Owner</sub>, SC<sub>IoBT</sub>}, for the blockchain validation. At the Blockchain level, successful execution of consensus protocol generates a block and ID<sub>CCC_SYS</sub> for the CCC_SYS and sends the ID<sub>CCC_SYS</sub> to the CCC owner.

2) **IOBT ASSOCIATION AT BLOCKCHAIN LEVEL**

Figure 8 presents the flow of IoBT association creation with the CCC_SYS at the blockchain. CCC owner creates the IoBT’s owner’s identity ID<sub>IoBT_Owner</sub> and IoBT’s
A. Rashid, A. U. R. Khan: Blockchain-Based Autonomous Authentication and Integrity for IoBT in C3I System

FIGURE 8. Association creation between IoBT and CCC

identity ID<sub>IoBT</sub>. CCC computes AssociationID<sub>IoBT</sub> = h(ID<sub>IoBT_Owner</sub>|| ID<sub>IoBT</sub>) and send Tx2 = {ID<sub>CCC_SYS</sub>, AssociationID<sub>IoBT</sub>} for blockchain validation. At the blockchain level, the smart contract verifies the activation of CCC_SYS and the uniqueness of IoBTs. If the Tx2 integrity verification and association policy is satisfied, ID<sub>IoBT_Owner</sub>, ID<sub>IoBT</sub>, ID<sub>CCC_SYS</sub>, and TXID are sent to the corresponding IoBT. TXID represents the operation that IoBT can execute to send data to CCC. Blockchain generates the AssociationID<sub>IoBT</sub>* and stores association between AssociationID<sub>IoBT</sub>* and ID<sub>CCC_SYS</sub> and blockchain using SC<sub>IoBT</sub>.

3) AUTHENTICATION AND DATA TRANSMISSION

Figure 9 presents the flow of authentication and integrity assurance before data acceptance at the blockchain. If an IoBT belonging to CCC wants to send data, it will provide its identification credentials together with the data. By sending a transaction Tx3 = {ID<sub>CCC_SYS</sub>, AssociationID<sub>IoBT</sub>, Data} for blockchain validation. Smart contracts perform authentication before sending the transaction to the blockchain and authenticate the device if AssociationID<sub>IoBT</sub> = AssociationID<sub>IoBT</sub>*. Blockchain validates the provided credentials and Tx3's integrity. If Tx3's integrity verification and credentials are invalid, the IoBT will not be allowed by the blockchain to send information.

4) REVOKING ASSOCIATION

The proposed technique prevents the association of malicious or misbehaving IoBTs. If an associated IoBT gets compromised, then CCC can revoke its association at any time. The CCC sends Tx4, which contains the identity of misbehaving IoBT. If Tx4's integrity verification is satisfied at the blockchain level, then the smart contract revokes the association of the compromised IoBT, deletes the association stored in the CCC_SYS, and updates the CCC_SYS. Figure 10 presents the flow of IoBT association deletion with the CCC_SYS at the blockchain.

IV. IMPLEMENTATION, PERFORMANCE EVALUATION, AND DISCUSSIONS

In order to evaluate the BIoBT, we developed a PoC implementation of the proposed system. We implemented our prototype on a public Ethereum network. Extensive analysis and benchmarking of the platform and its clients’ performance and scalability capabilities are provided in the literature. Therefore, we ignore the Ethereum network’s evaluation and target only the new components introduced in our framework.
that are not part of the Ethereum network, such as the BiIoBT owner and IoBT. We evaluate how introducing the BiIoBT owner and IoBT in the blockchain system affects the architecture’s overall computational effort and transaction fee.

### A. EXPERIMENTAL ENVIRONMENT

To test and evaluate the proposed BiIoBT system, a smart contract is implemented on the Ethereum platform. The contract is used because it is convenient for updating a distributed data store and because the code is immutable after deployment, promoting trust in the system. All contract interactions described in Section III are tested in a full version where all the information is stored on the contracts, and other contracts can access its information. This section evaluates the operations of BiIoBT in which the hashed public keys recognize all the entities. Table 4 shows the hashed public keys of all the interacting entities used for the experimentation and evaluation of the solution.

| Entities   | Identities of the Entities used in the evaluation                                      |
|------------|----------------------------------------------------------------------------------------|
| BiIoBT Owner | 0x4afaa26bc482b80ee7a0b348206927a6d2b8b50a3ca9f70e                                     |
| IoBT        | 0x4267a9a2b1a184b6443b3eb47820d7465167e70                                           |

All the experiments were performed on a laptop with the following specification:

- **BiIoBT Owner**: Intel®Core™i7-8550U CPU @ 1.80 GHz 1.99 GHz, 8 GB RAM, and 64-bit Operating System.
- **IoBT**: Intel®Core™i7-8550U CPU @ 1.80 GHz 1.99 GHz, 8 GB RAM, 64-bit Operating System.

All the interacting participants are enabled for this experiment with Ethereum Wallet modules. We have considered the laptop as a BiIoBT device. To measure the approximate costs of running various transactions of BiIoBT, we ran the transactions of our implemented prototype in the Ethereum test network. We measured the approximate computational steps in Ethereum’s gas and approximate cost in ETH for creating the BiIoBT blockchain contract and for each transaction supported by the contract. We tested the interaction with transactions on 3rd August 2022. A transaction fee is paid at the rate of Base: 0.000000007 Gwei, Max: 2.500000014 Gwei, and Max Priority: 2.5 Gwei per gas.

### B. PERFORMANCE ANALYSIS

When battlefield entities exchange information, the IoBT’s highly heterogeneous environment challenges trust, integrity, and privacy. This section evaluates the operations of BiIoBT in terms of performance and security features. Performance evaluation includes two matrices; (i) the computational effort in terms of gas unit consumption, and (ii) the transaction fee in ETH required for the execution.

Figure 11 shows the successful deployment of the compiled SC_{BiIoBT} on the Ethereum blockchain by the CCC owner node and the creation of CCC_Sys. Figure 12 shows the successful execution of the IoBT association created for the unique IoBT by the IoBT Owner on the Ethereum blockchain. Figure 13 shows the successful execution of authentication and integrity verification before data acceptance on the Ethereum blockchain. Figure 14 shows the successful execution of the IoBT association deletion on the Ethereum blockchain. Lastly, Figure 15 depicts the successful execution of the deactivation of the CCC_Sys on the Ethereum blockchain.

Figures 16 shows the result of the computational effort of the deployment of CCC_Sys (Tx-1), IoBT association creation (Tx-2), autonomous authentication and integrity verification before data acceptance from the associated IoBT (Tx-3), deletion of associated IoBT (Tx-4), and deactivation (Tx-5) of the CCC_Sys with and without optimization enabled, in terms of gas unit consumption. A comparison of the BiIoBT, with and without optimization enabled, shows that enabled optimization has reduced the gas unit consumption in executing the deployment transaction. Contract publishing...
has consumed the highest gas units compared to other transactions of the BIoBT. This is because it needs the entire compiled BIoBT contract to be deployed on the blockchain network.
FIGURE 15. Ethereum output of successful CCC_SYS deactivation transaction.

FIGURE 16. Estimated gas Units consumption for various operations of BiOTB.

Figures 17 show the result of the transaction fee of the implemented prototype for BiOTB, with and without optimization enabled, in terms of ETH required to pay for the transaction execution. The result shows that enabled optimization has reduced the ETH required for executing various operations of IoBT. Similar to Figure 16, contract publishing requires the highest ETH compared to other transactions of the BiOTB. This is because it needs the entire compiled BiOTB contract to be deployed on the blockchain network. From Figure 17, we conclude that barring fluctuations in the gas limit, gas price, or price of Ether, it is financially and technically feasible to deploy the BiOTB in the Ethereum blockchain.

C. SECURITY FEATURES

This section discusses how BiOTB achieved its aimed security features. The achieved security features are discussed as follows:

1) AUTONOMOUS AUTHENTICATION

In the BiOTB authentication, the IoBT utilizes parameters like AssociationID_{IoBT} and AssociationID_{IoBT}^*. The blockchain aborts the authentication process in case any parameter is invalid. Alternatively, the CCC autonomously authenticates the IoBT through parameters such as AssociationID_{IoBT} and AssociationID_{IoBT}^*, where AssociationID_{IoBT} = h(ID_{IoBT_Owner} || ID_{IoBT}) and AssociationID_{IoBT}^* is a blockchain’s generated identity for the CCC’s associated IoBT. Furthermore, the parameter AssociationID_{IoBT}^* is known by smart contract at the blockchain level and is an unclonable and immutable identity; therefore, it can be considered a challenge parameter for autonomous authentication. For authentication of IoBT, the smart contract autonomously verifies AssociationID_{IoBT} = AssociationID_{IoBT}^* at the Blockchain level before sending the transaction Tx-3 to the miner for the mining process. Thus, the authentication is autonomous, fast, and free of cost.
2) INTEGRITY ASSURANCE
BiOBT provides an end-to-end integrity assurance and maintains the data trustworthiness, accuracy, consistency, and reliability over the entire life cycle. BiOBT collects data after the autonomous authentication of the originator of the data, i.e., IoBT. BiOBT ensures the validity of the data by storing the message digest on the blockchain immutably. After verifying $Tx_3$ by the blockchain, CCC stores data in private storage, cloud, or IPFS and logs message-digest events on the blockchain, thus ensuring data integrity.

3) PRIVACY-PRESERVING
BiOBT is a privacy-preserving solution for CCC, IoBT identities, processes, and operations. In BiOBT, all the entities are owned and recognized by random-looking identities. Thus, it is impossible to differentiate whether the identity represents the CCC, IoBT, or any other entity on the blockchain. Similarly, all the operations are carried out using hashed inputs or message digests ($h$). Thus, it provides privacy to the operations on the blockchain. It is impossible to recognize whether the operation is performed for association creation, data transmission, or association deletion.

4) DECENTRALIZED TRUST
BiOBT distributed the trust in all the nodes in the blockchain network. The validation and verification of all the operations are performed in a decentralized manner. This ensures that BiOBT protects the system from a single point of failure and data loss.

V. COMPARISON WITH THE EXISTING TECHNIQUES
As no similar mechanism provides an autonomous and intelligent blockchain-enabled authentication mechanism for IoBT use cases, it is technically infeasible to compare the proposed technique with the related works. However, we have compared the BiOBT with the related works regarding their security features, PoC implementation, tools used for the PoC implementation, and transparency in verification, validation, and regeneration of results (see Table 5). Moreover,
we compare it with other authentication methods that rely on association (see Figure 18).

Figure 18 compares the number of messages required to create an association by different techniques. The scheme presented in [6] requires seven messages for the device-to-device association. The scheme presented in [8] requires five messages for pairing and five for authentication. The techniques presented in [7] and [10] require five, and [11] requires four messages for association creation. The techniques presented in [19] and [20] require three messages, including initialization and setup for association creation. Although the techniques presented in [19] and [20] mention two messages, these are without the initialization and association phase. Zone of Trust [21] and RC_AAM [39] have shown the best performance by utilizing only one message for association creation for zone and role authenticity.

Some techniques [40], [41] rely on the association phase and require eight and four messages, respectively. In [23] and [42], the researchers present the Datagram Transport Layer Security (DTLS) protocol based on IoT two-way authentication security scheme. Their association phase requires eight messages to establish secure communication between things. In [54], the researchers present an authentication scheme for Wireless Sensor Networks (WSNs). Their protocol relies on Elliptic Curve Cryptography (ECC). Although the scheme’s association phase requires five messages to establish secure communication, the requirement to use a gateway can further increase the number of messages. In [43], the authors propose a lightweight mutual authentication scheme for the IoT environment. Their proposed protocol validates the identities of the devices before engaging them in communication.

Compared to the techniques discussed in this section, BIoBT requires only one Tx for association creation, making it less energy and computation intensive. Moreover, the association is performed through the ECDSA scheme. ECDSA is known to be lightweight and well suited for resource-constrained devices [43], [44].

VI. CONCLUSION AND FUTURE WORK

This work presented a blockchain-based autonomous authentication scheme for IoBT. The proposed technique provides authentication, data integrity, and non-repudiation. A prototype is created, deployed, and tested on the Ethereum test network, and the results show that the proposed technique satisfies the security requirements of a distributed environment for IoBT. It is concluded that barring fluctuations in the gas limit, gas price, or price of Ether, it is financially and technically feasible to deploy the proposed BIoBT in the Ethereum blockchain. In the future, we plan to evolve the proposed BIoBT for biometric authentication, optimize the implemented mechanism by defining boolean functions, and design a protocol for optimizing the miner’s number in a defined system by employing the Proof of Authority (PoA) consensus protocol. The proposed authentication mechanism can also be applied to other use cases, such as identity authentication, data authentication, and digital certificate issuance and management in PKI. Lastly, we plan to implement BIoBT on other blockchain platforms to reduce the transaction time and cost.

### TABLE 5. Summary of the comparative analysis of the reviewed techniques and BIoBT.

| Ref | AA | PP | IA | DT | PoC | Tools for PoC | Transparency in Results |
|-----|----|----|----|----|-----|--------------|-------------------------|
| S. Russell et al. [22] | × | × | × | × | × | NA | NA |
| D. K. Toshet et al. [23] | × | × | × | √ | | NA | NA |
| FastChain [24] | × | × | × | × | | NS3 Simulator | - |
| R. Doku et al. [25] | × | × | × | | | pyNDU | - |
| M. Golam et al. [27] | × | × | × | | | Matlab, Python | - |
| MR-block [28] | × | × | × | | | | × |
| K. Kayya et al. [29] | × | × | × | | | | × |
| IoTChain [30] | × | × | × | | | NA | NA |
| M. Masuduzzaman et al. [31] | × | × | × | | | Parrot bebop 2 as UAV, Raspberry Pi 4 * | |
| ProBLESS [32] | × | × | × | | | - | × |
| Sensor-Chain [33] | × | × | × | | | - | × |
| M. Wazid et al. [34] | × | × | × | × | | NA | NA |
| B. Ghimire et al. [35] | × | × | × | | | NA | NA |
| R. Akter [38] | × | × | × | | | Python, Raspberry Pi 3 model b+ | - |
| M. Singh et al. [36] | × | × | × | | | Gazebo using the robotic operating system. | - |
| I.A. Shah et al. [37] | NA | NA | NA | NA | NA | Machine Learning | NA |
| BIoBT | √ | √ | √ | √ | | Ethereum blockchain, Smart Contract | ✓ |

**Legend:**
- AA: Autonomous Authentication
- PP: Privacy Preserving
- IA: Integrity Assurance
- DT: Decentralized Trust
- PoC: Proof of Concept
- NA: Not Applicable
- ∗: Required information not available.

VOLUME 10, 2022

IEEE Access

91585
REFERENCES

[1] Statista. *IoT Connected Devices Worldwide*. Accessed: Jun. 11, 2022. [Online]. Available: https://www.statista.com/statistics/1083457/iot-connected-devices-worldwide/

[2] A. U. R. Khan and R. W. Ahmad, “A blockchain-based IoT-enabled E-Waste tracking and tracing system for smart cities,” *IEEE Access*, vol. 10, pp. 86256–86269, 2022.

[3] Q. F. Hassan, S. A. Madani, and A. R. Khan, *Internet of Things: Challenges, Advances, and Applications*. Boca Raton, FL, USA: CRC Press, 2017.

[4] A. Shafique, A. Mehmoond, M. Alawida, A. N. Khan, and A. U. R. Khan, “A novel machine learning technique for selecting suitable image encryption algorithms for IoT applications,” *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–21, Jul. 2022.

[5] M. F. Aziz, A. N. Khan, J. Shuja, I. A. Khan, F. G. Khan, and A. U. R. Khan, “A lightweight and compromise-resilient authentication scheme for IoTs,” *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, Mar. 2022, Art. no. e3813.

[6] M. N. Aman, K. C. Chua, and B. Sikdar, “Mutual authentication in IoT systems using physical unclonable functions,” *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327–1340, Oct. 2017.

[7] A. Esfahani, G. Mantas, R. Matishek, F. B. Saghezchi, J. Rodriguez, A. Bicakcu, S. Makstui, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for M2M communications in industrial IoT environment,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 298–306, Feb. 2019.

[8] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, and J. Shen, “A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server,” *Comput. Elect. Eng.*, vol. 63, pp. 168–181, Oct. 2017.

[9] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, “Proximity based IoT device authentication,” in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, May 2017, pp. 1–9.

[10] W. Feng, Y. Qin, S. Zhao, and D. Feng, “AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS,” *Comput. Netw.*, vol. 134, pp. 167–182, Apr. 2018.

[11] B. Gong, Y. Zhang, and Y. B. Wang, “A remote attestation mechanism for the sensing layer nodes of the Internet of Things,” *Future Gener. Comput. Syst.*, vol. 78, pp. 867–886, Jan. 2018.

[12] P. Gope and B. Sikdar, “Lightweight and privacy-preserving two-factor authentication scheme for IoT devices,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.

[13] P. Roychoudhury, B. Roychohadury, and D. K. Saikia, “Provably secure group authentication and key agreement for machine type communication using Chebyshev’s polynomial,” *Comput. Commun.*, vol. 127, pp. 146–157, Sep. 2018.

[14] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balusamy, and P. G. Shynu, “Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks,” *Future Gener. Comput. Syst.*, vol. 78, pp. 943–955, Jun. 2016.

[15] A. Bicakcu, S. Makstui, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for M2M communications in industrial IoT environment,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 298–306, Feb. 2019.

[16] A. Bicakcu, S. Makstui, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for M2M communications in industrial IoT environment,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 298–306, Feb. 2019.

[17] A. Bicakcu, S. Makstui, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for M2M communications in industrial IoT environment,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 298–306, Feb. 2019.

[18] A. Bicakcu, S. Makstui, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for M2M communications in industrial IoT environment,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 298–306, Feb. 2019.

[19] A. Bicakcu, S. Makstui, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for M2M communications in industrial IoT environment,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 298–306, Feb. 2019.

[20] A. Bicakcu, S. Makstui, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for M2M communications in industrial IoT environment,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 298–306, Feb. 2019.

[21] A. Bicakcu, S. Makstui, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for M2M communications in industrial IoT environment,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 298–306, Feb. 2019.
[41] M. A. Jan, P. Nanda, X. He, Z. Tan, and R. P. Liu, “A robust authentication scheme for observing resources in the Internet of Things environment,” in Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput. Commun., Sep. 2014, pp. 205–211.

[42] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, “A DTLS-based end-to-end security architecture for the Internet of Things with two-way authentication,” in Proc. 37th Annu. IEEE Conf. Local Comput. Netw. Workshops, Oct. 2012, pp. 956–963.

[43] E. D. Win, S. Mister, B. Preneel, and M. Wiener, “On the performance of signature schemes based on elliptic curves,” in Proc. Int. Algorithmic Number Theory Symp., 1998, pp. 252–266.

[44] K. Lauter, “The advantages of elliptic curve cryptography for wireless security,” IEEE Wireless Commun., vol. 11, no. 1, pp. 62–67, Feb. 2004.

Aqsa Rashid received the M.C.S. degree (Hons.) in computer science and the M.S. degree in computer science with a specialization in information security from IUB, BWP, in 2013 and 2015, respectively. She is currently a Ph.D. Scholar with the Department of Information Security, NUST, Pakistan. She is also working on blockchain-based solutions to cater to autonomous security services problems. Her research interests include but are not limited to information security, cryptography, computer security, blockchain for C3I military systems, role engineering, healthcare, and security. She is an Active Member of the IEEE Blockchain and Cybersecurity Community. She received the IBM Blockchain Badge from IBM Blockchain Platform and Certified QAP Certification from NUST, in 2018.

Atta Ur Rehman Khan (Senior Member, IEEE) is currently an Associate Professor at the College of Engineering and Information Technology, Ajman University, United Arab Emirates. In the past, he has worked as a Postgraduate Program Coordinator at Sohar University, the Director of the National Cybercrime & Forensics Laboratory, Pakistan, and the Head of the Air University Cybersecurity Center. He also serves as a domain expert for multiple international research funding bodies and has received multiple awards, fellowships, and research grants. His research interests include cybersecurity, mobile cloud computing, ad-hoc networks, and the IoT. He is a Senior Member of ACM and a steering committee member/the track chair/a technical program committee (TPC) member of over 85 international conferences. He is serving as an Associate Editor for IEEE Access, Journal of Network and Computer Applications (Elsevier), an Associate Technical Editor for IEEE Communications Magazine, and an Editor for Journal of Cluster Computing (Springer), The Computer Journal (Oxford), IEEE SOFTWARE DEFINED NETWORKS NEWSLETTER, KSII Transactions on Internet and Information Systems, and Ad Hoc & Sensor Wireless Networks journal. For more information visit the link (www.attaurrehan.com).

* * *