IEEE Open Journal of the Computer Society

Received 5 February 2024; accepted 13 March 2024. Date of publication 18 March 2024;
date of current version 18 April 2024. The review of this article was arranged by Associate Editor Qiang Ye.

Digital Object Identifier 10.1109/OJCS.2024.3378424

A Novel NFT Solution for Assets Digitization and Authentication in Cyber-Physical Systems: Blueprint and Evaluation

USMAN KHALIL [1], MUEEN UDDIN [2] (Senior Member, IEEE), OWAIS AHMED MALIK [1,3] (Senior Member, IEEE), AND ONG WEE HONG [1]

[1]School of Digital Science, Universiti Brunei Darussalam, Gadong BE1410, Brunei
[2]College of Computing and Information Technology University of Doha for Science and Technology, Doha 24449, Qatar
[3]Institute of Applied Data Analytics, Universiti Brunei Darussalam, Gadong BE1410, Brunei

CORRESPONDING AUTHOR: MUEEN UDDIN (e-mail: mueen.uddin@udst.edu.qa)

This work was supported by Qatar National Library.

ABSTRACT The blueprint of the proposed Decentralized Smart City of Things (DSCoT) has been presented with smart contracts development and deployment for robust security of resources in the context of cyber-physical systems (CPS) for smart cities. Since non-fungibility provided by the ERC721 standard for the cyber-physical systems (CPSs) components such as the admin, user, and IoT-enabled smart device/s in literature is explicitly missing, the proposed DSCoT devised the functionality of identification and authentication of the assets. The proposed identification and authentication mechanism in cyber-physical systems (CPSs) employs smart contracts to generate an authentication access code based on extended non-fungible tokens (NFTs), which are used to authorize access to the corresponding assets. The evaluation and development of the extended NFT protocol for cyber-physical systems have been presented with the public and private blockchain deployments for evaluation comparison. The comparison demonstrated up to 96.69% promising results in terms of execution cost, efficiency, and time complexity compared to other proposed NFT-based solutions.

INDEX TERMS Cyber-physical system/s, non-fungible tokens (NFTs), smart contract, web3 technology.

I. INTRODUCTION

In the context of Web3, decentralized cyber-physical systems in the smart city are an innovative urban concept that utilizes blockchain technology to enhance city operations and improve the QoL for its inhabitants [1]. Overall, a decentralized smart city in the context of Web3 holds significant promise for the future of urban development. By capitalizing the decentralized technologies, cities can create more efficient, transparent, and citizen-focused urban environments that are more democratic and secure [2]. Decentralized Smart City of Things (DSCoT) has been proposed in our earlier research in [3], [4], and [5] for the identification, authentication, and digitization of assets (admin, users, fog, and smart device/s) in cyber-physical systems (CPS/s). The proposal in [4] discusses the evaluation of the deployment on a private blockchain network while our research in [3] discusses the evaluation of a public blockchain network in comparison to the proposed solution in the literature.

This article, however, provides the design and evaluation of the functions and components of the proposed DSCoT over private and public blockchain testnet so that the required performance and security standards may be evaluated. As discussed comprehensively in [3] the non-fungible tokens (NFTs)-based solution in the literature is explicitly missing as none of the solutions provide non-fungibility of assets in the CPS/s context. The Ethereum Request for Comments-721 (ERC721) standard [6] (which defines NFTs) also does not cater to the CPS/s components hence the extended version i.e., the proposed DSCoT fills the research gap by devising the functionality through novel components in smart contracts for the identification and authentication of resources in the context of CPSs for smart cities. The code base created for

this research is globally available on GitHub [7] and be deployed on private as well as the public testnet. However, the novel solution has been deployed over the Goerli testnet to get insight in terms of monitoring and evaluation.

The proposed system architecture, as illustrated in Section IV, outlines the functionalities of the Digitized and Secure CPS through proposed extended NFTs for integration. The architecture ensures that resource owners exclusively initiate and execute operations related to NFT-based smart contracts, with unauthorized requests being systematically rejected. This approach not only safeguards the availability of resources for legitimate users but also guarantees that authorization is solely granted by the rightful owner of the resources. This intricate yet comprehensive system illustrates the secure digitization and authentication of assets within the proposed DSCoT framework, emphasizing the crucial and extended role of NFTs in ensuring robust user authorization and access control.

A. SECURITY AND AUTHENTICATION ISSUES OF IOT-ENABLED SMART ASSETS IN CYBER-PHYSICAL SYSTEMS

Specifically, considering a CPS in smart cities and an increasing number of IoT-enabled smart device/s connecting to the internet daily, the security and authentication of these devices have become inevitable. One of the recently carried out Cisco Annual Internet surveys (2018–2023) projected approximately 66% of the world's population will gain internet connectivity by 2023, showing a significant number of devices that might connect to the internet in the future [8].

Since the internet in Web2 uses traditional protocols (TCP/IP), the underlying architectures of the CPS/s inherit the security and authentication issues which open the doors to a possible breach for the networks themselves [2]. Additional factors that contribute to the vulnerability of customer premises equipment (CPE) include inadequate security features implemented by manufacturers, such as the use of weak SSL versions (e.g., v2, v3, and CBC mode), weak default login details, open ports, and unencrypted or self-signed security certificates, etc. The lack of proper security and access control mechanisms by these manufacturers increases the risk of exploitation in internet infrastructures, industrial settings, and related contexts. Thus, a need to develop secure architectures is inevitable that may cope with the security and authentication issues of IoT-enabled smart assets operating in the underlying smart city architecture.

II. RELATED WORKS

In an attempt to explore the capabilities of the non-fungible token (NFT), different solutions have been developed in various domains. Since the NFT has a strong capability to represent the digital identity in cryptocurrency, it attracts developers to explore it further to expand its capability. However, the overview of the literature concerning the NFT-enabled solutions proposed over recent times depicts that no architecture for cyber-physical systems (CPSs) in smart cities has been explored to extend the NFT capability. The digital identity attribute of NFT is much more suitable to represent IoT assets in smart cities. This section summarizes the solutions that have been proposed based on non-fungible tokens (NFT/s). Subsequently, a comparison highlights the novel aspects of the proposed solution in [3], [4] which bases the blueprint and evaluation of the proposed architecture in this article.

Authors in [9] present the extended version of ERC721 for NFTs which shows the authentication mechanism on a device level that relies on hardware upgrades i.e., Physical Unclonable Function (PUF). The presented results show performance issues in terms of computational complexity. However, the extension does not present a complete architecture for IoT assets such as Admins, Users, Fog devices, and IoT devices within a cyber-physical system.

Connect2NFT [10] utilizes the NFTs to associate social media sites (Twitter in this case) to provide digital ownership to its users. It deploys the NFT in its general form and utilizes the NFT default security mechanism.

The utilization of NFTs in [11] is no different than the study in [10] rather the association of NFTs has been realized with the decentralized storage of the InterPlanetary File System (IPFS). The implementation links the NFTs' metadata, with the IPFS hash which is stored on the chain. This solution also deploys the NFT in its general form and relies on the NFT and blockchain's default security mechanism. Since the solution is dependent on the decentralized framework, it inherits computational issues such as latency and scalability which may disrupt the solution's rigor and efficiency.

Authors in [12] present a general association of healthcare assets such as patient details, doctor's prescription, medicines, etc., however, it lacks novelty in terms of linking the healthcare IoT assets such as wearable health monitors, implantable medical devices, smart infusion pumps, smart beds, etc.

The NFT-Vehicle concept has been presented in [13] which involves divisibility in terms of associating a vehicle with the NFT to retain the digital identity for maintaining ownership rights. The proposed solution shows the association of related stakeholders such as vehicle owners, buyers, manufacturers, government, etc. However, the scope is limited to a particular domain and does not present the architecture for IoT assets in a smart city.

The association of pharmaceutical assets especially the supply chain has been presented in [14] where NFTs have been utilized in their standard form. The research did not present the interoperability challenges that can emerge when implementing NFT-enabled solutions across various IoT assets such as health tracking sensors, connected thermometers, blood pressure monitors, etc. from different manufacturers. It leads to the issue of standardized protocols which can obstruct the integration and communication between diverse assets.

Based on the solutions explored in this section, a comparative review has been carried out. Section V-C presents the analysis which shows that NFT has been explored in different domains however, the digital identity attribute that represents IoT assets in smart cities and authentication mechanism through NFTs is yet a research gap.

A. RESEARCH MOTIVATION

Given the aforementioned gaps, the significance of the proposed DSCoT lies in its ability to address the inherent challenges of representing and authenticating a vast array of IoT assets securely and efficiently. The research motivation was to come up with a robust architecture that may incorporate the following attributes for all the IoT assets in cyber-physical system/s (CPS/s) that currently pose a research gap.

1) SECURITY AND UNIQUENESS

As IoT assets in CPSs become more numerous and diverse, the need for a system that can guarantee the uniqueness and security of each asset is paramount. The proposed DSCoT addresses this by using extended NFTs to represent and authenticate each asset uniquely, enhancing security. The use of SHA-III encryption and the CIA including the AAA model (Confidentiality, Integrity Availability, Authorization, Authentication, Audit) helps ensure robust security features, safeguarding sensitive data, assets, and security audit to trace back the errors and loopholes to attain resilience.

2) INTEROPERABILITY

The proposed DSCoT ensures that these representations are interoperable, meaning they can be used seamlessly across different applications, fostering greater collaboration and efficiency in the CPS/s context.

3) EFFICIENCY

The architecture introduces innovative functions for querying the smart contract, ensuring no transaction cost (in Ether/Gwei). This efficiency is vital for the scalability and cost-effectiveness of CPS/s operations.

4) EVALUATION AND VALIDATION

The study provides an evaluation of the proposed functions and components, which is essential to validate the effectiveness and efficiency of the architecture. This is vital for real-world implementations in CPSs. It is evident that while various NFT-enabled solutions cater to different domains, the proposed solution's distinctive features make it a compelling choice for bolstering the security of IoT assets within smart cities. The motivation marks the contribution of the research as discussed in the upcoming section.

III. CONTRIBUTIONS

In real-world implementations within smart cities, the scalability of NFT-enabled solutions can be a significant challenge due to the potential volume of transactions and data generated by various IoT assets. While different solutions in the literature introduce NFTs but do not deeply address potential security challenges inherent in NFT implementation specifically in the context of CPSs. NFT security, including vulnerabilities related to token creation, management, and ownership verification, should be thoroughly examined to ensure the robustness of the proposed system. The presented contributions of the proposed NFT extension, however, address the concerns and presents;

1) A design based on blockchain tokenization that utilizes devised components to represent and digitize the assets in cyber-physical systems (CPSs).
2) The proposed architecture centers on the software-based digital signage, identification, and authentication of IoT-enabled smart devices. It eliminates the need for any improvements in hardware from the producer, as has been seen in the case of IoT assets with Physical Unclonable Functions (PUF).
3) We deployed the novel Web3-based components and functions for the identification and authentication of assets based on an expanded proposal in the Non-Fungible Tokens (NFTs) protocol.
4) We define additional and newly developed attributes to generate IoT-based NFTs for smart device representation.
5) We introduced mapping to bind the newly developed NFT attributes of Users, fog nodes, and edge nodes with the EOAs of respective devices.
6) We evaluate the proposed protocol deployment on an Ethereum-based public testnet (Goerli) and its comprehensive performance comparison with private blockchain deployment i.e., Hyper Ledger Besu and NFT-based solutions proposed in the literature.

The research paper highlights the limitations of the ERC721 standard attributes provided by NFTs for identifying and defining financial assets, as they do not address the identification and authentication needs of resources in cyber-physical systems (CPSs), including admin, users, and smart devices. To address these limitations, the research proposes and develops additional attributes that provide support for the identification and authentication of assets in CPSs for smart cities. Later, the deployment and evaluation of the solution were presented to showcase the research rigor and efficiency.

The paper is structured in the following manner. Section II presents the related works that employ the NFT-enabled solutions with a comparison to the proposed NFT extension in this paper. Research contributions have been presented in Section III while in Section IV, the details of the proposed system model which consists of devised components and functions are introduced. Section V presents the evaluation of the proposed architecture on a public blockchain testnet in addition to the private deployment over Hyper Ledger Besu along with security analysis. The threat model has been provided in Section VI. Finally, conclusions are given in Section VII highlighting possible extensions of this work for varied CPSs in smart cities.

IV. THE PROPOSED DIGITIZATION AND AUTHENTICATION MECHANISM

The system architecture of all the components referring to the required proposed DSCoT functionality has been presented in Fig. 1. As depicted in the figure, the resource owners can only initiate and perform the operations of the proposed NFT-based

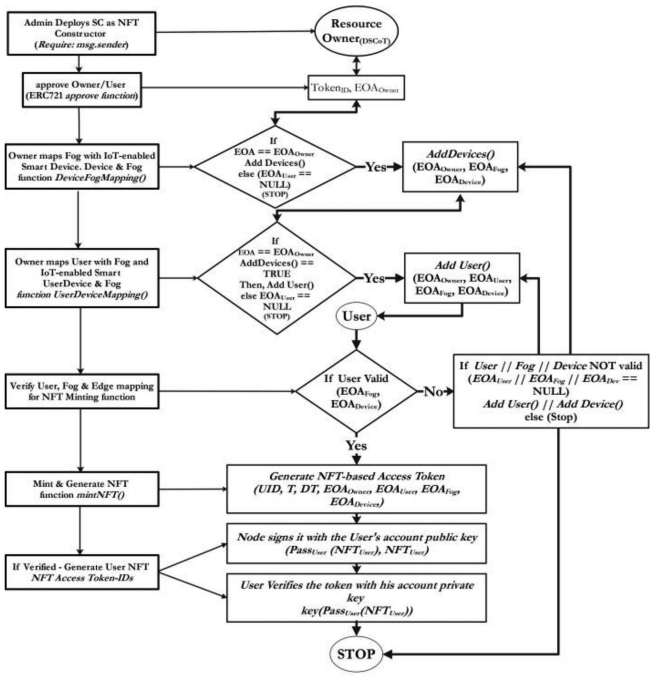

FIGURE 1. Proposed assets digitization and authentication system flow diagram.

smart contracts; otherwise, the request will be rejected. This property adds availability of the resources to legitimate users while authorization is achieved by the legitimate owner who owns the resources. The owner can only add other admins, fog, and IoT device/s realizing identification and binding of the assets. At this stage the verification for the mapped IoT device with fog device and the user will be performed and if no mapped devices are found the user mapping will not take place and the process start again for mapping the devices. Once the IoT-enabled smart devices are mapped with the fog device and the respective user, the NFT minting function must be triggered to authenticate users to access the devices.

As shown, the minting generates $\mathrm{NFT_{Pass}}$ which contains the devised attributes of the $\mathrm{NFT_{User}}$ such as User identification (*UID),* block timestamp, and change in the timestamp (*T,* ΔT*)* to track the transactions and oppose the replay attacks, EOAs of mapped User, Fog, IoT device/s, and User's public key (PK).

$$\mathrm{NFT_{Pass}} = \mathrm{Pass_{User}}\left(\mathrm{NFT_{User}}\right), \mathrm{NFT_{User}} \text{whereas,}$$

$$\mathrm{NFT_{User}} = (UID, T, \Delta T, EOA_{User}, EOA_{Device}, EOA_{Fog}, User_{PK}).$$

Finally, if verified, the NFT_{Pass} represents the user's non-fungible token generated by incorporating the user's token ($\mathrm{Token_{Id}}$), block timestamp, and change in block timestamp (*T,* ΔT*),* together with the externally owned accounts (EOAs) of user, fog, and IoT device/s which are based on proposed Non-Fungible Tokens (NFTs) and the user's EOA private key ($\mathrm{User_{IK}}$) as shown in Fig. 1. It generates a user authentication access token to access the devices and for the authentication process, every time the user accesses the nodes assigned as shown below.

$$\mathrm{NFT_{Pass}} = \mathrm{Pass_{User}}\left(\mathrm{NFT_{User}}\right) \text{whereas, } \mathrm{NFT_{User}} = \left(\mathrm{Token_{Id}}, T, \Delta T, \mathrm{EOA_{User}}, \mathrm{EOA_{Device}}, \mathrm{EOA_{Fog}}, \mathrm{User_{IK}}\right)$$

The user signs the token with the account's private key ($\mathrm{User_{IK}}$), and the user is authenticated to access the mapped devices.

A. DEVELOPMENT AND DEPLOYMENT

According to the set objectives, the development of the proposed extended version of NFTs via smart contracts (SCs) and deployment on distributed technology utilizing the Ethereum blockchain is presented here. The motivation was to design a protocol based on a Web3-based distributed platform so all the assets including nodes at the edge and fog layer may operate in a distributed manner. To come up with a distributed blockchain platform for the research, the SCs were deployed on a public blockchain testnet that uses Ethereum as a public network. Goerli testnet, in this case, has been utilized to test the functionality, identify and fix bugs, and validate the proposed smart contracts before deployment on the Ethereum mainnet.

1) DECENTRALIZED FRAMEWORKS

The proposed decentralized application (dapp) uses smart contracts (SCs) that are developed in a client-side application. It utilizes public and private Ethereum-based blockchains for deployment. These smart contracts are coded in Solidity, which functions similarly to JavaScript. The proposed mechanism is compiled and deployed using Remix IDE (v0.23.3) and is an expansion proposal of the ERC721 standard for IoT assets in DSCoT. Node.js framework (v14.17.6 & npm v6.14.15) is an open-source server environment that allows JavaScript to run on the server and has been deployed together with JsonRPC which helps in the realization of communication between nodes and blockchain and encode/decodes data to be interpreted by developing an interface [15].

B. THE PROPOSED SMART CONTRACTS DEPLOYMENT

The proposed smart contracts provide a function-based interface to build an expansion proposal of non-fungible (NFTs) on the Ethereum blockchain which devises the identification and authentication of resources in CPSs for smart cities. The proposed smart contracts were successfully deployed on the public ledger using Remix which can be can be identified through their cryptographic address. In this context, the address corresponds to an identified entity in the expanded proposal of the ERC-721 standard. MetaMask wallet was configured with a personal account and network settings to connect with the Goerli testnet which allows the connection to the blockchain and interaction with the smart contracts for its development. The wallet was connected to the Remix IDE and was used to deploy the proposed SCs. The wallet address is the externally owned address of the SC owner (EOA_{Owner}). The

TABLE 1. Components & Functions of the Proposed DSCoT Architecture

Proposed Functions	Functions Titles, Types & Payload
F(No. of Admins NFT EOAs, add admin)	approve(address _approved, uint256 _tokenId) external payable;
	No_ofAdmins() external view returns (uint256);
	adminAdd() external view returns (address[] memory);
	delAdmin (address admin) external;
F(IoT, Fog)	DeviceFogMapping(address fog, address device) external;
	delDev(address fog) external;
F(Users)	UserDeviceMapping(address user, address device,address fog) external;
	delUser(address user) external;
F(check balance, owner, and issued token)	balanceOf(address _owner) external view returns (uint256);
	ownerOf(uint256 _tokenId) external view returns (address);
	tokens_Issued()public view returns (Token[] memory);
Mint F(User and Devices Authentication Mechanism)	mintNFT(address device, address fog) external;

deployed SC can be tracked by its address ($EOA_{Contract}$) while all the proposed components and functions were evaluated by posting the transactions over the public testnet.

The transactions (Tx) metadata was verified by deploying proposed SCs over address: *0x504C7FAb97AFb2642Bb00Fff8520AbA0857E3544 w*hich helps verify the data in posting Tx to the blockchain. The status of the posted transactions through a smart contract can be tracked via public blockchain explorer at *https://goerli.etherscan.io/address/0x504c7fab97afb2642bb00fff8520aba0857e3544* while the status of the posted transactions by the SC owner (*EOAOwner:0x90B7A5D5A96d4206E1BDa9baEC1019ACCCdb1bbA*) can be tracked via public blockchain explorer at *https://goerli.etherscan.io/address/0x90B7A5D5A96d4206E1BDa9baEC1019ACCCdb1bbA* . Table 1 on the other hand depicts the ramified components with functions presented in the smart contract type of interface, which contains function signatures, it defines the external interface of the proposed smart contract where the main functions were implemented. The main components in the proposed smart contracts enable the functions of identification and authentication for the admin, the user, the fog device, and the IoT device/s. The table further depicts the proposed functions metadata such as *approve(), addDeviceFogMapping(), addUserDeviceMapping(), mintNFT(),* etc., followed by the evaluation of deployed functions over the public ledger in upcoming sections.

1) APPROVE(), ADMINADD() AND NO_OFADMIN()

Since all the proposed components and functions were to be evaluated, the deployed SCs were tested by triggering the proposed functions in the extended version of ERC721. The Tx payload for the *approve()* function approved EOA: *0x5b38da6a701c568545dcfcb03fcb875f56beddc4* as an EOA_{Owner}. The transaction was successfully mined on block no. 8361404 and the EOA was added as an EOA_{Owner} by generating the events for the added EOA as EOA_{Owner} presented in Fig. 2(a).

The added EOA_{Owner} can carry out all the activities as that of an SC Owner. To validate the Tx payload, efficient call methods have been devised to query the NFT registry without costing the computational overhead in the proposed SCs such as *adminAdd()*, *no_ofAdmins()*, *Tokens_Issued()*, *user_devices()*, and *fog_devices().*

The transaction metadata for *adminAdd() and No_of Admin()* queries the NFT registry for added EOA as an EOA_{Owner}: *0x5b38da6a701c568545dcfcb03fcb875f56beddc4* referred to as [*topic 1*] and number of added admins respectively as shown in Fig. 2(a).

This shows the importance of devised call methods for validation purposes of Tx payloads in the proposed DSCoT protocol. Since the proposed SCs can be initiated by the EOA_{Owner} only, the transaction metadata shows EOA_{Owner} as "0*x90B7A5D5A96d4206E1BDa9baEC1019ACCCdb1bbA*" referred to as [topic 2]" and transaction hash as [topic 0] in Fig. 2(a).

2) ADDDEVICEFOGMAPPING()

One of the important components is mapping the fog device with IoT-enabled smart device/s so that authorized users may be assigned to these devices to access the assets. Since the proposed SCs owner as shown in Fig. 2(b), "EOA_{Owner}: *0x90B7A5D5A96d4206E1BDa9baEC1019ACCCdb1bbA*" referred to as [*topic 3*] is the authorized entity to initiate the *addDeviceFogMapping()*, the component was triggered and minted with the Tx payload of the IoT assets such as EOA_{Fog}: *0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB*, referred as [*topic 1*] and EOA_{Device}: *0x617F2E2fD72FD9D5503197092aC168c91465E7f2* [*topic 2*] at block no. 8361412 so that these devices may be mapped and undergo the process of authentication in the next step. Fig. 2(b) shows the Tx metadata for the *addDeviceFogMapping()*

FIGURE 2. **Transactions status of the proposed functions over goerli testnet.**

function that was successfully mined and generated events for the added EOA_{Fog} and EOA_{Device}. It is important to note that the process of authentication will not trigger if the devices are not found mapped with each other and the Tx will be denied. This was tested by posting the transactions which resulted in canceled transactions. Shown via public BC explorer at *https://goerli.etherscan.io/address/0x504c7fab97afb2642bb00fff8520aba0857e3544* are the posted transactions over the public ledger, the transactions (Tx 6 and 14) were denied since the devices were not mapped which shows the rigor of the devised functions and the solution overall.

3) ADDUSERDEVICEFOGMAPPING()

The next important component of the proposed DSCoT is to map the user with the already mapped fog device with IoT-enabled smart device/s from step 2) i.e., *addDeviceFogMapping()* so that authorized user may be assigned to the mapped devices to gain access. As shown in Fig. 2(c) an authorized entity "EOAOwner" initiated the *addUserDeviceFogMapping()*, and the component was triggered and minted with the transaction (Tx) metadata at block no. 8365162 which shows the Tx payload of the *EOAUser: 0x660c71144f38dd39d1f78cf52ed03e34c3f9fe9c* referred to as [topic 1], EOA_{Fog}*: 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB* referred as [topic 3], EOA_{Device}*: 0x617F2E2fD72FD9D5503197092aC168c91465E7f2* referred to as [topic 2], so these mapped devices may undergo the process of authentication in the next step.

It is important to note that the process of authentication will not trigger if the mapped devices are not found mapped with each other (Step 1) or to the authorized user (Step 2) the Tx will be denied. Table 1 presents the *addUserDeviceFogMapping()* metadata with payload and events.

4) MINTNFT()

The DSCoT SCs provide security in terms of authorization to users as only the user will be able to mint the DSCoT *mintNFT()* function, not even EOA_{Owner} can mint the authentication NFT until added as a user in the Tx

payload. The *mintNFT()* function was triggered and the transaction was verified with the payload of the EOA_{User}:*0x660c71144f38dd39d1f78cf52ed03e34c3f9fe9c* referred to as [*topic 2*], EOA_{Fog}: *0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB* referred as [*topic 3*], EOA_{Device}: *0x617F2E2fD72FD9D5503197092aC168c91465E7f2* referred as [*Addr*] as highlighted in Fig. 2(d). Since the devices were mapped with each other (Step 1) and a user was assigned as an authorized user (Step 2) the *mintNFT()* undergoes the process of authentication. The *mintNFT()* function was successfully minted on block no. 8372806 by the EOA_{User} which generates the authentication access token *_tokenID*:"*0xe226eb92af43fda20a8963f600f7b66ef4718d1da92b92dd370cee000836b423*" referred to as [*topic 1*] with a "timestamp": "*1674634596*" for the user, fog, and IoT-enabled smart device as stated in Fig. 2(d).

The *mintNFT()* function authenticates a user to access the devices and generates the user NFT authentication access token for the authentication process every time the user accesses the mapped devices. Table 1 presents the *mintNFT()* metadata with payload and events. The Tx metadata for all the posted transactions with the transaction hashes can be verified on the publicly available Goerli BC explorer [16].

5) ACCESSING THE DEPLOYED CONTRACTS

Once the smart contracts are established on a blockchain network, they are posted permanently and can be accessed at any point in time. The proposed DSCoT SCs were posted on the Ethereum-based public Goerli testnet as shown in *https://goerli.etherscan.io/address/0x504c7fab97afb2642bb00fff8520aba0857e3544* at contract address ($EOA_{Contract}$):*0x504C7FAb97AFb2642Bb00Fff8520AbA0857E3544* with owner address (EOA_{Owner}): *0x90B7A5D5A96d4206E1BDa9baEC1019ACCCdb1bbA*. Once the testbed completed the validation of the methods imposed by DSCoT, the proposed smart contracts were evaluated in terms of efficiency in processing the transactions on a public testnet namely Goerli.

V. EVALUATION AND VALIDATION

A. EFFICIENCY EVALUATION OF EXTENDED ERC721 ON A PUBLIC BLOCKCHAIN TESTNET

Once the testbed was deployed, the effectiveness of the proposed NFT methods utilizing SCs required validation by analyzing the execution cost in terms of Gas consumption during posting transactions on the Goerli testnet platform. Validating the Gas consumption of the proposed NFT methods is crucial in assessing their efficiency and scalability in managing CPS assets. By evaluating the Gas consumption of the proposed components and functions, stakeholders can identify potential bottlenecks and inefficiencies in the proposed NFT methods. This analysis allows for informed decision-making on the optimal deployment scenarios for the NFT methods, thereby ensuring cost-effectiveness and scalability in managing assets in CPSs for smart cities.

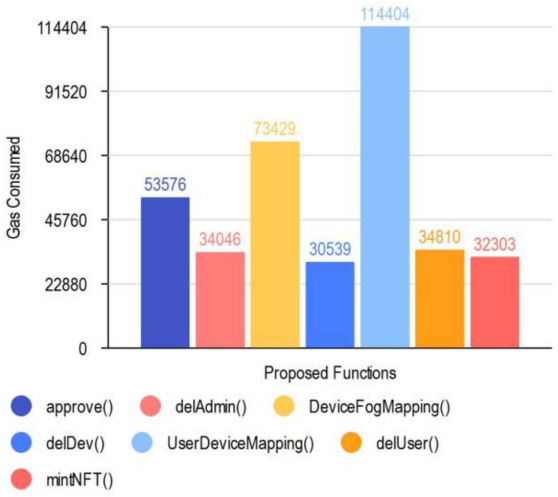

FIGURE 3. Gas consumption of proposed functions over Goerli Testnet.

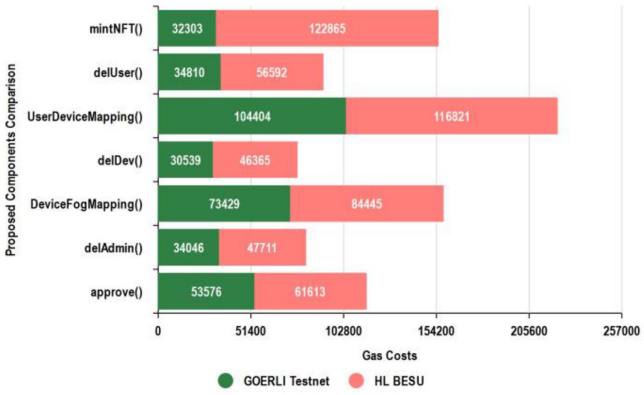

FIGURE 4. Comparison evaluation → Goerli Testnet ~ HL Besu.

The proposed DSCoT was evaluated over the Goerli testnet to analyze the Gas consumption of its main components. As depicted in Fig. 3, the *UserDeviceMapping()* function has the highest execution cost, as expected, due to the mapping of users and devices. Additionally, the *DeviceFogMapping()* function, which maps the fog device to the IoT nodes, also incurred a significant amount of Gas consumption.

In contrast, for the remaining functions, including *approve()*, *delAdmin()*, *delDev()*, *delUser()*, and *mint()*, the gas consumption was found to be nearly identical on average. Especially *mint()* which has been observed with a very low gas consumption depicting an efficient minting mechanism. These findings provide valuable insights into the Gas consumption patterns of the DSCoT components, which can be used to optimize the NFT deployment scenarios and improve the efficiency of managing the cyber-physical systems (CPS/s assets.

B. EFFICIENCY ~ COMPARATIVE EVALUATION OF EXTENDED ERC721 OVER PUBLIC AND PRIVATE BLOCKCHAIN DEPLOYMENTS

In Fig. 4, the execution cost comparison of the proposed DSCoT components is presented, highlighting the difference

TABLE 2. Comparative Efficiency Evaluation of NFT-Enabled Solutions

Ref	Year Proposed	Domain	NFT MINT Execution Cost	Comparison ~ PROPOSED MINT EFFICIENCY	Overall EFFICIENCY of NFT-based Solutions	Comparison ~ PROPOSED SOLUTION EFFICIENCY
[9]	2021	NFT-based IoT Security	167263	80.68%	602223	39.70%
[10]	2022	NFT-based Social Media	***Not Reported***	100%	***Not Reported***	100%
[11]	2022	NFT-metadata over IPFS	***Not Reported***	100%	***Not Reported***	100%
[12]	2022	NFT-based HealthCare Services	183260	82.37%	1221693	70.27%
[13]	2023	NFT-Vehicle	121141	73.33%	10972911	96.69%
[14]	2022	NFT-based Supply Chain for HealthCare	***Not Reported***	100%	***Not Reported***	100%
Prop. Sol	2022	Extended NFT (DSCoT) for CPSs	32303	Threshold Value	363107	Threshold Value

in gas consumption between the deployment on a private blockchain network, specifically HL Besu in [3], and the public Goerli testnet in this article. All functions show an increase in execution cost when deployed on the private network, particularly the *mint()* function, which caters to the encryption and authentication payload of resources. The *DeviceFogMapping()* and *UserDeviceMapping()* functions also consume more gas on the private blockchain network. Although the gas consumption for the other components, such as *approve(), delAdmin(), delDev(), and delUser()* were observed to be almost the same on average, an increased execution cost is observed on the private deployment. This indicates that the proposed DSCoT architecture is better suited for public blockchain networks.

Deployment on a public testnet can be faster than deployment on a private blockchain setup in some cases, but it depends on the specific circumstances. Public testnets generally have more nodes and a larger user base, which can result in faster transaction processing times and quicker confirmation of blocks. However, this can also lead to network congestion and slower transaction processing times during periods of high activity [17], [18], [19]. However, the increased execution cost of the private deployment may be due to the block size, which increases or decreases based on network demand. The analysis of the Gas consumption of the DSCoT components over the Goerli testnet versus private deployment in [3] opens effective NFT-based methods for development in different scenarios. These insights present the development of cost-effective NFT deployment scenarios that are scalable and efficient in managing assets in cyber-physical system/s for smart cities.

C. EFFICIENCY ~ COMPARATIVE EVALUATION OF EXTENDED ERC721 WITH NFT-ENABLED SMART CITIES SOLUTIONS

The first part of this section (Section A) presents the efficiency evaluation in terms of execution costs of all the devised components over public and private deployments however, to take away the bias, the efficiency comparison of the proposed NFT extension has also been evaluated considering the NFT minting execution costs and overall execution costs of the proposals among the proposed solutions in the literature. Although none of the solutions presents the complete architecture of smart IoT assets digitization and NFT-based novel

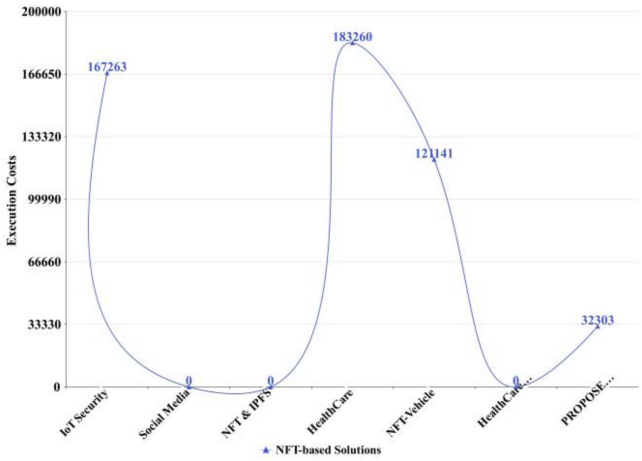

FIGURE 5. Execution costs comparison ~ proposed solution.

authentication mechanism for cyber-physical systems in smart city infrastructure, still the comparison shows insights into the minting process and the execution costs analysis in respective domains as illustrated in the following Table 2.

The efficiency analysis reveals distinct patterns in execution costs across these solutions. DSCoT, however with its utilization and deployment over Hyperledger Besu and Goerli public ledger, emerges as a cost-efficient alternative, displaying significantly lower NFT mint execution costs and overall execution costs compared to other solutions (Table 2, Col 5 and 7). Further depicted in Fig. 5 certain solutions did not provide explicit data for NFT mint costs therefore, the efficiency in terms of minting costs compared to these solutions was noted as 100% efficient. Considering the research in [9], [12], and [13] the execution of the devised minting component of the proposed solution was observed at 80.68%, 82.37%, and 73.33% more efficient than the other solutions respectively.

The efficiency analysis reveals distinct patterns in execution costs across these solutions. DSCoT, however with its utilization and deployment over Hyperledger Besu and Goerli public ledger, emerges as a cost-efficient alternative, displaying significantly lower NFT mint execution costs and overall execution costs compared to other solutions in literature (Table 2, Col 5 and 7).

It shows DSCoT's cost-effectiveness which aligns well with its commitment to securing IoT assets within the complex context of cyber-physical systems (CPS/s) infrastructure.

TABLE 3. Comparative Security Analysis of the Proposed Solution with NFT-Enabled Solutions

Ref	Year Proposed	Domain	Proposed NFT Extension	Default NFT mechanism	Proposed Auth Mech	Security Services	
						CIA	AAA
[9]	2021	NFT-based IoT Security	✓	-	✓	[I]	[Auth]
[10]	2022	NFT-based Social Media	×	✓	×	[I]	×
[11]	2022	NFT-metadata over IPFS	×	✓	×	[I]	×
[12]	2022	NFT-based HealthCare Services	×	✓	×	[A]	×
[13]	2023	NFT-Vehicle	×	✓	×	[I]	×
[14]	2022	NFT-based Supply Chain for HealthCare	×	✓	×	[C], [I]	×
Proposed Solution	2022	Extended NFT (DSCoT) for CPSs	✓	-	✓	[C], [I], [A]	[Ath], [Auth], [Aud]
Key: Security Services	[CIA] → [C] Confidentiality, [I] Integrity, [A] Availability					[AAA] → [Ath] Authorization, [Auth] Authentication, [Aud] Audit	

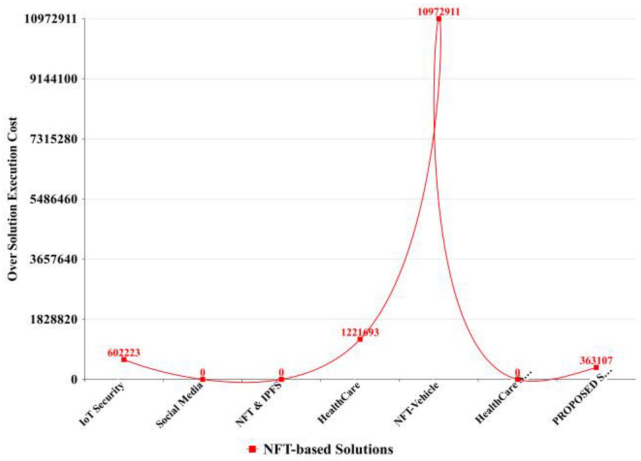

FIGURE 6. Overall solutions costs comparison ~ proposed solution.

The overall efficiency of the extended NFT-enabled was measured for the given overall efficiency of solutions in this research and was found to be 39.70%, 70.27%, and 96.69% cost-effective respectively while the zero indicates that no data for execution costs was revealed by these solutions as shown in Fig. 6. Since the execution costs were not reported by a few NFT-based studies the overall efficiency of the solution could not be measured therefore, the overall efficiency of the proposed solution compared to these solutions was noted as 100% efficient.

This comparison underscores DSCoT's potential as a practical and economical solution for fortifying cyber-physical systems scalability. By prioritizing both cost efficiency and robustness, DSCoT sets itself apart as a compelling option for addressing the intricate challenges linked to NFT minting and overall execution costs. These findings reinforce the importance of tailored solutions that strike a balance between security and financial feasibility, ultimately contributing to the advancement of secure and efficient smart city ecosystems.

D. SECURITY ANALYSIS

The motivation for achieving a high level of rigor lies in the emphasis on the robustness and resilience of security services. The security analysis of the proposed NFT architecture constitutes a critical examination of the robustness and efficacy of its security mechanisms that have been designed in multi-functioned stepwise security layers. As discussed in the preceding section and depicted in Table 3 (Col 3 and 5), NFTs have been utilized from an implementation point of view in a few domains while the proposals in the literature have predominantly relied on default security and NFT mechanisms as defined in ERC721 standard without addressing comprehensive CIA and AAA models. No further divisibility in the modules and authentication or authorization mechanisms have been provided which makes these solutions prone from an adversarial point of view.

Table 3 further depicts that the proposed solution was the only solution to achieve CIA and AAA security services comprehensively achieving a high level of rigor as far as security and privacy of data and IoT assets are concerned.

The discussion below provides proof of how the devised modules achieve the security services (CIA and AAA) to attain the proposed NFT architecture's rigor for the integration of IoT-enabled smart assets which necessitates a meticulous assessment of potential vulnerabilities and the effectiveness of protective measures.

1) APPROVE(), ADDDEVICEFOGMAPPING(), ADDUSERDEVICEFOGMAPPING(), MINTNFT()

Since the resource owner (RO) is the creator and is the only entity that owns and deploys the DSCoT SCs as devised in the constructor and modifier, it offers security rigor from the attack vector. The resilience of the extended version of the ERC721 standard can be arbitrated by the devised modules that are dependent on each other. If EOA details, approvals, and mappings do not match or do not exist in the respective lists, any request to access the DSCoT SCs will be rejected. Since the DSCoT SCs are initiated by the resource owner (Fig. 1), the devised *approve()* module as a first step provides functionality to approve EOAs of the owners, fog and IoT devices, and the users. This does not permit unauthorized control, access or manipulation of SCs and IoT assets since the EOA_{Device} and EOA_{Fog} need to be the approved EOA/s that would undergo a mapping process, or, the system will deny any further proceedings by rejecting the TX/s from an unapproved EOA by the EOA_{Owner} enforcing strong confidentiality of relevant data (Table 4).

Once approved, the *addDeviceFogMapping()* module (IV.B.2) as a second step maps the EOAs of the IoT assets

TABLE 4. Threat Model Security Measures of the Proposed Solution

Security Aspect	Threat Description	Potential Risks	Analyze, Prioritize & Mitigate Risks	Mitigation Strategy
Confidentiality	Unauthorized initiation attempts by malicious External Owned Account (EOA) entities, apart from the designated EOAOwner.	- Unauthorized Access - Authorization Bypass	– Impact: Unauthorized control or manipulation of SCs and IoT assets. – Likelihood: Moderate. – Risk Level: High. – Mitigation: Strong access controls, and continuous monitoring.	Implementation of a constructor and a modifier for the users in the Smart Contract (SC) ensures confidentiality. Only the SC's Creator (EOA_{Owner}) and user (EOA_{User}) are authorized to initiate and perform operations, rejecting requests from unauthorized entities.
Integrity	Threats to data integrity, such as eavesdropping, data spoofing, and replay attacks compromise the legitimacy and reliability of information.	- Data Tampering - Data Spoofing	– Impact: Compromised integrity of data leading to misinformation. – Likelihood: Low. – Risk Level: Moderate. – Mitigation: Strong encryption, and cryptographic controls.	The adoption of third-generation SHA encryption (SHA-III) for one-way encryption ensures data integrity. This cryptographic measure prevents tampering, guaranteeing the authenticity of information.
Availability	Attempts to compromise the availability of IoT assets and user data through unauthorized access or mapping by entities not approved by the SC Owner.	- Eavesdrop - Track and Trace - Unauthorized Access	– Impact: Unauthorized control or manipulation of SCs and IoT assets. – Likelihood: Moderate. – Risk Level: High. – Mitigation: Strong access controls, and continuous monitoring.	Utilization of a private blockchain platform (Hyperledger Besu and Goerli) with IBFT 2.0 consensus ensures consistent availability. Access to IoT assets is restricted to the SC Owner's mapping and approval of users, further authentication access NFT is required for availability.
Authorization	Unauthorized access attempts by External Owned Accounts (EOA) that are not approved by the SC Owner, aiming to interact with the system or gain access to IoT assets.	- Unauthorized Access to IoT Assets - Unauthorized Access to IoT Data - Authorization Bypass	– Impact: Unauthorized entities gaining access to resources. – Likelihood: Moderate. – Risk Level: Moderate. – Mitigation: Strong authorization policies, and role-based access control.	Implementation of authorization mechanisms, including modifiers like "OnlyOwner," ensures strict access control. Access is granted only to authorized SC Owner and approved users, rejecting attempts from unauthorized EOAs.
Authentication	Attempts to bypass or compromise the authentication process for accessing IoT devices, particularly during the mintNFT() function.	- Access Control - Unauthorized Access - Authorization Bypass	– Impact: Compromised authentication leading to unauthorized access. – Likelihood: Moderate. – Risk Level: Moderate. – Mitigation: Devised authentication mechanism, and regular security audits.	Extension of the NFT standard for CPS/s architecture adds an authentication layer. The mintNFT() function authenticates users to access devices and generates user NFT authentication access tokens for each access instance.
Audit	The lack of a comprehensive security audit, leads to potential vulnerabilities being overlooked, compromising the trustworthiness of the system.	- Audit Data Manipulation - Audit Trail Manipulation	– Impact: Compromised trustworthiness of the audit trail. – Likelihood: Low. – Risk Level: Low. – Mitigation: Immutable audit logs, and third-party audit checks.	Conducting a thorough security audit, as outlined in [6] and [8], to evaluate specific features of DSCoT's security architecture. The audit includes an examination of smart contract function execution, NFTs' role in authentication, and cryptographic protocols for data protection. The insights gained contribute to refining security features and informing broader discussions on securing IoT assets.

to confine the IoT-enabled smart devices to a respective fog device. The *addUserDeviceFogMapping()* module (IV.B.3) triggers as a third step and this further confines the fog and IoT-enabled smart devices to a respective user. The proposed mapping of IoT devices and further assigning respective user/s to permit access offers authorization and confidentiality of IoT assets within CPS/s.

The final step authenticates a user to access the devices and generates the user NFT authentication access token for the authentication process every time the user accesses the mapped devices through the devised *mintNFT()* module (IV.B.4). The proposed authentication of mapped IoT assets to respective user/s implies 3rd generation of encryption protocol that offers data integrity omitting data tampering for authorization bypass and unauthorized access (Table 4).

If any details are missing in the stepwise proceedings against the approval and mapping access policy defined in the devised modules as presented in Table 1, the request/s will be denied. The EOA/s that are not approved, may not be able to access the SCs, and IoT assets in the architecture may be safeguarded in terms of eavesdropping, data spoofing, and replay attacks. In case, the attack vector gets the access, it may not be able to map the IoT devices and users which restricts the access to the IoT assets. The creator is the only entity that can approve EOAs of IoT assets and users which are further authenticated using a devised mintNFT module that generates access NFT to access the devices.

VI. THREAT MODEL

The security threat model has been critically crafted to attain the rigor of the proposed scheme since prior proposals examined in Section II have often overlooked essential security services, namely, confidentiality, integrity, availability (CIA), authentication, authorization, and audit (AAA). The threat model in Fig. 7 has been designed to address the unique challenges posed by the integration of IoT-enabled smart devices within the context of smart city architectures.

A. SCOPE

In contrast, the proposed architecture in this study takes a proactive approach by encompassing security services (CIA & AAA) as a core focus, in addition to robust authentication and authorization mechanisms devising Novel NFT-enabled architecture as shown in Fig. 7. This proactive stance signifies a substantial advancement in the security landscape. Fig. 7 further illustrates how the threat model's scope defines the system/application boundaries, explicitly extending to cyber-physical systems

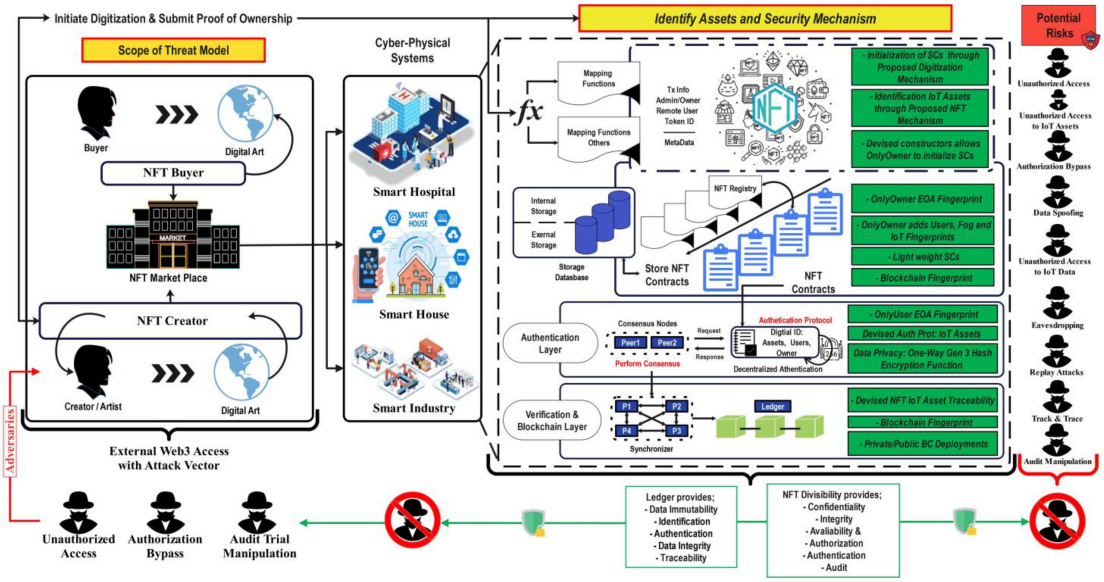

FIGURE 7. Security Threat Model of the Proposed NFT-enabled Networklike smart hospitals, houses, and industries. The scope, detailed in Table 4, comprehensively addresses the security aspects of the extended version of the NFT-enabled solution, focusing on essential services for the identified IoT assets within the proposed DSCoT.

B. IDENTIFY ASSETS

The process of identifying critical assets starts when the resource owner/creator/admin (EOA_{Owner}) initiates the DSCoT smart contracts (SCs) as shown in Fig. 7. The assets include IoT assets (EOA_{Fog}, $EOA_{IoT\ Devices}$, and EOA_{Users}), sensitive data, infrastructure components (private BC deployment, NFT registry, NFT storage database), and key functionalities (devised modules) of the SCs. Every asset of the proposed DSCoT has importance which adds potential impact to each asset.

C. IDENTIFY POTENTIAL RISKS

Brainstorming is of sheer importance every time to identify potential threats to the proposed DSCoT. As shown in Fig. 7 unauthorized access, unauthorized access to IoT assets, authorization bypass, data spoofing, and breaches, unauthorized access to SCs data, eavesdropping, replay attacks, track and trace, and audit manipulation are the identified potential risks that could exploit vulnerabilities in the proposed solution. Table 4 further details the security aspects of the threat model of all the identified risks with analysis and mitigation strategies for clarity. As discussed in Section IV, inadequate access controls and insufficient input validation have been critically taken care of while coding the proposed DSCoT SCs in terms of choosing a coding, deployment platform (IV.A), devising modules for IoT assets, a novel authentication mechanism (IV.B), testing and validation platform (V), and security analysis (0). This detailed consideration provides a robust understanding of the security landscape to fortify against potential exploits.

D. ANALYZE, PRIORITIZE, AND MITIGATE RISKS

An evaluation of the potential impact and likelihood of each identified threat to DSCoT has been analyzed as shown in Table 4. Factors such as potential damage, ease of exploitation of existing security controls, and historical incident data have been presented in terms of impact, likelihood, and risk level which helps assess the overall risk associated with each threat to prioritize subsequent actions.

E. VALIDATE AND UPDATE

The DSCoT SCs have been developed and deployed foreseeing the countermeasures and security controls to mitigate or reduce identified risks as the system evolves. An effort to continuously validate and update the threat model will be acquired with a regular reassessment of the emerging threats and changes to the smart city architecture which may assist in adjusting the threat model accordingly.

VII. CONCLUSION AND FUTURE WORK

The proposed DSCoT stands out for its groundbreaking approach to addressing challenges in cyber-physical systems (CPS/s) architecture. Notable achievements include leveraging blockchain for enhanced security and extended NFT standards through innovative smart contracts to ensure a comprehensive security model caters to the complexities of CPS/s operations. The architecture enforces robust security policies, manages authentication for IoT assets, and introduces extended Non-fungible Tokens (NFTs) for unique and secure digital identities. The achievements are substantiated through a thorough comparative analysis, validating DSCoT's distinct features and improvements over alternatives. Rigorous testing over public/private deployments contributes to advancing

decentralized blockchain solutions, ensuring up to 96.69% promising results in execution cost, efficiency, and time complexity. The threat model for DSCoT focuses on safeguarding its architecture, covering CIA and AAA models to ensure the security of IoT assets. The future research directions outline a holistic roadmap for advancing the security, efficiency, and interoperability aspects of the DSCoT architecture within the context of smart cities. Concurrently, the optimization of DSCoT in future works for diverse CPS/s applications may allow the dynamic nature of smart city contexts, fostering adaptability and resource efficiency.

CONFLICT OF INTEREST

The author(s) declared no potential conflicts of interest concerning this article's research, authorship, and/or publication.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] U. Khalil, O. A. Malik, M. Uddin, and C. - L. Chen, "A comparative analysis on blockchain and centralized authentication architectures for IoT-enabled smart devices in smart cities: A comprehensive review, recent advances, and future research directions," *Sensors*, vol. 22, no. 12, pp. 1–52, 2022.

[3] U. Khalil, O. A. Malik, O. W. Hong, and M. Uddin, "Decentralized smart city of things: A blockchain tokenization-enabled architecture for digitization and authentication of assets in smart cities," in *Proc. ACM Int. Conf.*, 2022, pp. 38–47.

[4] U. Khalil, O. A. Malik, W. H. Ong, and M. Uddin, "DSCOT: An NFT-based blockchain architecture for the authentication of IoT-enabled smart devices in smart cities," 2022. [Online]. Available: https://ssrn.com/abstract=4355848

[5] U. Khalil, O. A. Malik, O. W. Hong, and M. Uddin, "Leveraging a novel NFT-enabled blockchain architecture for the authentication of IoT assets in smart cities," *Sci. Rep.*, vol. 13, no. 1, pp. 1–26, Nov. 2023.

[6] W. Entriken, D. Shirley, J. Evans, and N. Sachs, "Erc-721 non-fungible token standard," Ethereum Foundation, Jan. 2018.

[7] U. Khalil, "GitHub - uskhalil/decentralized-smart-city-of-things-DSCoT," 2022. Accessed: May 01, 2023. [Online]. Available: https://github.com/uskhalil/Decentralized-Smart-City-of-Things-DSCoT

[8] "Cisco: 2020 CISO benchmark report," *Comput. Fraud Secur.*, vol. 2020, no. 3, p. 4, 2020. [Online]. Available: https://doi.org/10.1016/S1361-3723(20)30026-9

[9] J. Arcenegui, R. Arjona, R. Román, and I. Baturone, "Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFs," *Sensors*, vol. 21, no. 9, 2021, Art. no. 3119.

[10] J. Bellagarda and A. M. Abu-Mahfouz, "Connect2NFT: A web-based, blockchain enabled NFT application with the aim of reducing fraud and ensuring authenticated social, non-human verified digital identity," *Mathematics*, vol. 10, no. 21, Oct. 2022, Art. no. 3934.

[11] H. R. Hasan et al., "Incorporating registration, reputation, and incentivization into the NFT ecosystem," *IEEE Access*, vol. 10, pp. 76416–76433, 2022.

[12] A. Musamih, I. Yaqoob, K. Salah, R. Jayaraman, M. Omar, and S. Ellahham, "Using NFTs for product management, digital certification, trading, and delivery in the healthcare supply chain," *IEEE Trans. Eng. Manage.*, vol. 71, pp. 4480–4501, 2024.

[13] J. C. López-Pimentel, L. A. Morales-Rosales, I. Algredo-Badillo, and C. Del-Valle-Soto, "NFT-vehicle: A blockchain-based tokenization architecture to register transactions over a vehicle's life cycle," *Mathematics*, vol. 11, no. 13, Jun. 2023, Art. no. 2801.

[14] F. Chiacchio, D. D'urso, L. M. Oliveri, A. Spitaleri, C. Spampinato, and D. Giordano, "A non-fungible token solution for the track and trace of pharmaceutical supply chain," *Appl. Sci.*, vol. 12, no. 8, Apr. 2022, Art. no. 4019.

[15] O. J. Foundation, "Node.js," 2021. Accessed: Sep. 15, 2021. [Online]. Available: https://nodejs.org/en/

[16] G. Testnet, "Görli testnet," 2018. Accessed: May 27, 2022. [Online]. Available: https://goerli.net/

[17] L. Vinet and A. Zhedanov, "A 'missing' family of classical orthogonal polynomials," *J. Phys. A: Math. Theor.*, vol. 44, 2011, Art. no. 085201.

[18] N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris, and G. C. Polyzos, "Secure IoT access at scale using blockchains and smart contracts," in *Proc. IEEE 20th Int. Symp. A World Wireless, Mobile Multimedia Netw.*, 2019, pp. 1–6.

[19] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities," *J. Netw. Comput. Appl.*, vol. 181, 2021, Art. no. 103007.

USMAN KHALIL received the M.S. and Ph.D. degrees in computer science from Universiti Brunei Darussalam, Bandar Seri Begawan, Brunei, in 2024 and 2019, respectively. He is currently a Researcher with the Mathematical and Computing Sciences, School of Digital Sciences, Universiti Brunei Darussalam. With more than fourteen years of professional experience in the telecom industry in Pakistan and Malaysia, Usman Khalil previously was a Telecom professional. His research interests include exploratory pattern recognition algorithms for the analysis, data mining, clustering, integration of the Internet of Things with cloud computing, and the integration of the Internet of Things with blockchain. He is a Reviewer of reputed journals, including IEEE ACCESS, *Journal of Electrical Engineering & Technology*, *SN Applied Sciences*, *Bulletin of Electrical Engineering, and Informatics*, *PLOS ONE*, and *Measurement Sensors*.

MUEEN UDDIN (Senior Member, IEEE) received the B.S. and M.S. degrees in computer science from Isra University, Hyderabad, Pakistan, in 2005 and 2008, respectively, and the Ph.D. degree in information systems from Universiti Teknologi Malaysia, Skudai, Malaysia, in 2013. He possesses a strong research and publication profile and was a Research Fellow of his previous assignments with Khalifa University, Abu Dhabi, UAE, and IIUM Malaysia, Kuala Lumpur, Malaysia. He is currently an Associate Professor with the Department of Cybersecurity and Data Sciences, College of Computing and Information Technology, University of Doha for Science and Technology, Daha, Qatar. He has fifteen years of professional academic experience in several universities in Malaysia, Saudi Arabia, UAE, Pakistan, and Brunei Darussalam and has been teaching various courses in the domains of Cybersecurity and forensics, Information and Network Security, Cloud Computing Infrastructures, and Information Systems. He has completed five research grants in his previous academic and research positions. He was on many editorial boards and is an active reviewer of many international reputable journals and conferences. He has reviewed more than 100 research articles. Some journals include IEEE ACCESS, *Renewable, and Sustainable Energy Reviews*, IEEE CLOUD COMPUTING, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE SYSTEMS JOURNAL, *Computing Journal Springer*, *International Journal of Global Warming*, and *Journal of Supercomputing*. He was a technical committee member and session chair of various international and local conferences in Computer Sciences and Information Systems. He has authored or coauthored more than 160 research papers in high-quality journals and conferences. His research interests include cybersecurity and forensics, blockchain, information and network security, energy efficient cloud infrastructures, and information systems.

OWAIS AHMED MALIK (Senior Member, IEEE) received the M.S. degree in computer science from KFUPM, Dhahran, Saudi Arabia, in 2002, and the Ph.D. degree in computer science from Universiti Brunei Darussalam, Bandar Seri Begawan, Brunei, in 2015. He is currently a Senior Assistant Professor of mathematical and computing sciences with the Department of Digital Sciences, University Brunei Darussalam. He is currently a Computer System Engineer from NED, Pakistan in 1998. He has more than ten years of progressive experience in academia and research in computer science and engineering. He has been teaching various undergraduate courses, including machine learning, data mining, machine perception, programming fundamentals, design and analysis of algorithms, software engineering, and operating systems in different national/international universities. He has authored or coauthored several articles in internationally reputable journals and conferences. His research interests include designing and exploring different intelligent/pattern recognition algorithms to analyze and classify biodiversity and cyber-security data, applied biomechanics, bio-signal processing, and Big Data analytics.

ONG WEE HONG is currently an Assistant Professor of computer science with the Universiti Brunei Darussalam, Bandar Seri Begawan, Brunei (UBD). In 2007, he joined the UBD. Before joining the UBD, he taught with the Jefri Bolkiah College of Engineering from 1998 to 2007. His research interests include developing intelligent systems for personal robots and ambient intelligence. In particular, he explores applying artificial intelligence techniques and info-communication technologies in developing intelligent systems. He is leading the Robotics and Intelligent Systems Laboratory (Robolab). Current projects include unsupervised human activities recognition, storage cloud-based IoT systems, mobile robot navigation, human emotion perception for human-robot interaction, and self-supervised object recognition.