IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 May 2023, accepted 23 June 2023, date of publication 28 June 2023, date of current version 5 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3290911

RESEARCH ARTICLE

Secure and Privacy-Preserving Trust Management System for Trustworthy Communications in Intelligent Transportation Systems

IKRAM UD DIN[1], (Senior Member, IEEE), KAMRAN AHMAD AWAN[1], AND AHMAD ALMOGREN[2], (Senior Member, IEEE)

[1]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2]Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia

Corresponding author: Ahmad Almogren (ahalmogren@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs, Chair of Cyber Security.

ABSTRACT As Intelligent Cyber-Physical Transportation Systems (ICPTS) become increasingly complex and interconnected, the quest for secure and robust communication between diverse components and entities emerges as a significant challenge. This paper presents an innovative Context-Aware Cognitive Memory Trust Management System (CACMTM) tailored for ICPTS. By utilizing game theory to model trust interactions, our system amalgamates various trust constituents, such as evaluation, decision, update, and knowledge modules, into an integrated and dependable trust management solution, specifically addressing the unique demands of Customer Centric Communication and Networked Control for ICPTS (CNC-ICTS). The proposed approach integrates a cognitive memory-based trust management method designed explicitly for IoT in the metaverse, leveraging past experiences and adapting to the evolving behaviors of IoT entities for enhanced trust evaluation. Our approach also employs a multi-dimensional trust evaluation model considering historical behavior, reputation, and contextual information to furnish a thorough assessment of IoT entity trustworthiness, thereby minimizing the risk of false trust evaluation outcomes. Furthermore, a blockchain-secured logging mechanism integration into our trust management system, thereby bolstering security, transparency, and accountability. The working mechanism utilizes three algorithms that collectively offer an efficient, trust-aware, and adaptable framework for interactions between IoT devices and service providers. The proposed modular CACMTM architecture consists of four main modules: Trust Evaluation, Trust Decision, Trust Update, and Knowledge. A rigorous performance assessment of the CACMTM was carried out using diverse metrics and parameters such as execution time, scalability, and capability in detecting varying types of attacks. The empirical evidence gathered clearly illustrates that our approach transcends existing trust management solutions in effectively identifying and mitigating a wide range of attacks in the context of CNC-ICTS.

INDEX TERMS Cognitive memory, trust management, reliable communication, cyber-physical transportation, intelligent transportation, centric communication, security, reliability.

I. INTRODUCTION

The widespread adoption and integration of advanced technologies such as Machine Learning (ML), Artificial Intelligence (AI), and the Internet of Things (IoT) have catalyzed the evolution of the global transportation infrastructure. These transformative technologies have precipitated the development of Intelligent Cyber-Physical Transportation Systems (ICPTS) that are fundamentally reshaping the transportation landscape [1]. Central to this paradigm shift is the advent of Customer Centric Communication and Networked Control for Intelligent Cyber-Physical Transportation

The associate editor coordinating the review of this manuscript and approving it for publication was Xueqin Jiang.

Systems (CNC-ICTS), which prioritize augmenting user experiences and optimizing the efficacy of transportation networks [2], [3], [4], [5]. ICPTS, with their inherent complexity and deep interconnectedness, necessitate secure and robust communication mechanisms across all components and entities [6]. However, these systems are confronted with a host of challenges, most notably in the domains of security, privacy, and trust management [7]. These issues arise from the inherent diversity of transportation systems, the heterogeneity of utilized devices and technologies [8], and the dichotomy of maintaining user data privacy while facilitating efficient communication and control [9]. While significant strides have been made in trust management for CNC-ICTS, there remain gaps and limitations in existing strategies that should be addressed [10].

The primary motivation fuelling this research work is to address the intricacies of trust management within ICPTS and to carve a more effective and robust pathway that can seamlessly adapt to the unique prerequisites of CNC-ICTS [11]. Our principal objective is to confront the issue of context-aware security and privacy in ICPTS, ensuring the adaptability of trust management mechanisms to myriad situations and contexts, thereby delivering the requisite level of security and privacy. In response to this issue, we propose a Context-Aware Cognitive Memory Trust Management System (CACMTM) for ICPTS. Our methodology harnesses machine learning and artificial intelligence techniques to establish and sustain trust between network entities, taking into account the unique requirements and constraints of various environments and contexts. The proposed system amalgamates several trust components including evaluation, decision, update, and knowledge modules that collaborate to provide a robust and effective trust management solution. By fusing these components, the CACMTM exhibits dynamic adaptability to ICPTS environmental changes and assures secure and reliable communication across components and entities. The distinctive contributions of the proposed approach are as follows:

- We introduce a cognitive memory-based trust management approach explicitly tailored for IoT in the metaverse, effectively utilizing past experiences and adapting to evolving behaviors of IoT entities for enhanced trust evaluation.
- We employ a multi-dimensional trust evaluation model which incorporates factors such as historical behavior, reputation, and contextual information to provide a thorough assessment of IoT entity trustworthiness, thus mitigating the risk of false positives or negatives in trust evaluation.
- We incorporate a blockchain-based secure logging mechanism to improve the security, transparency, and accountability of the trust management system, thereby discouraging malicious behavior and incentivizing trustworthy behavior among IoT entities.
- We propose three algorithms that collectively provide an efficient, trust-aware, and adaptable framework for interactions between IoT devices and service providers, specifically addressing service provider selection, service provision, and trust-based service selection.
- We develop a modular architecture for the CACMTM system consisting of four primary modules: Trust Evaluation Module, Trust Decision Module, Trust Update Module, and Knowledge Module. These modules collaborate seamlessly to furnish a comprehensive and effective trust management solution for IoT in the metaverse.

The structure of this manuscript is as follows: In Section II, a comprehensive literature review is presented on the topic of trust management in the Metaverse. Section III presents the cognitive memory-based trust management system in detail, including its algorithms and components. In Section IV, the evaluation of the CACMTM is presented. In Section V, the implications of the results, limitations, and future directions of the proposed system are discussed. Finally, Section VI concludes the paper with a summary of the research.

II. LITERATURE REVIEW

The Metaverse is a collective virtual shared space generated by the collision of physical and virtual worlds that has gained a lot of attention due to the increasing popularity of immersive technologies. The Metaverse has potential applications in entertainment, gaming, healthcare, and education, but several challenges, especially in the areas of security, privacy, and ethics, need to be addressed. This literature review evaluates current research on the Metaverse and its challenges.

In 2022, Pundir et al. [12] delves into the challenges and enabling technologies of transport networks in smart cities powered by cyber-physical systems (CPS). The article discusses the importance of integrating CPS with transportation systems to foster a new mobility era. Rani et al. [13] examine the security and privacy challenges that arise from deploying CPS in smart city applications, providing an overview of the state-of-the-art work in this domain. Garg et al. [14] present a comprehensive analysis on intelligent CPS for autonomous transportation, covering various aspects of the technology, including design, deployment, and management. Additionally, Rajawat et al. [10] explore the use of 5G-enabled CPS for smart transportation, employing blockchain technology to ensure secure and efficient operations.

Security is a significant concern in the Metaverse, given the increasing number of cyber attacks. Reference [15] proposed a GAN-based intrusion detection model that uses synthetic traffic data to train the intrusion detection model, which demonstrated a higher detection rate and lower false-positive rate than traditional methods. Human digital twins for cybersecurity simulations in the Metaverse have been proposed by [16], which can help identify potential vulnerabilities and improve security. The potential of the Metaverse for healthcare applications has been explored by [17], who suggested

the use of the Metaverse as an intervention tool for cognitive decline in the elderly population. The immersive and engaging environment of the Metaverse can lead to better treatment outcomes.

In 2022, Nagarajan et al. [18] propose an intelligent anomaly detection framework (IADF-CPS) for CPS that aims to enhance their security and reliability. This framework employs machine learning techniques to detect anomalies in real-time, allowing for efficient mitigation strategies. Yang et al. [19] investigate the security defense of coupled transportation and cyber-physical power systems based on static Bayesian games, providing insights into the vulnerability of these systems and offering potential defense mechanisms. Raza et al. [20] discuss machine learning-based security solutions for critical CPS, highlighting the importance of deploying advanced security measures to protect these systems from potential threats.

The combination of blockchain and AI has been proposed as a solution to address security and privacy concerns in the Metaverse. Reference [21] proposed a trusted AI with blockchain approach that uses blockchain to securely store user data and AI algorithms to analyze the data for potential security threats. The authors argue that the combination of blockchain and AI can provide a more secure and private environment for users in the Metaverse. The study in [22] provides a comprehensive survey of enabling technologies, challenges, and visions for realizing the edge-enabled Metaverse, including edge computing, 5G, and blockchain. The authors identify several key challenges, including security, privacy, and content creation. The ethical implications of the Metaverse have also been explored. In 2022, [23] discusses the metaverses as a virtual version of data-driven smart cities raise serious ethical problems about hyper-connectivity, datafication, algorithmization, and platformization of urban life; these issues should be addressed. The authors argue that taking a critical and reflective stance is necessary for the responsible and ethical growth of the Metaverse.

Xu et al. [1] show how a digital twin for traffic may help improve traffic management by providing real-time situational awareness and cyber-physical control. This cutting-edge method makes use of cloud computing to improve urban smart mobility. Das et al. [3] propose a security, trust, and privacy management framework for CPS using blockchain technology, further emphasizing the need for robust security measures in such systems. Cai et al. [24] introduce an adaptive DDoS attack mitigation scheme (ADAM) for software-defined CPS. This scheme aims to protect these systems from distributed denial-of-service attacks by employing adaptive mitigation strategies. Finally, Jafari et al. [25] discuss the benefits and drawbacks of this novel method to modeling and controlling large cyber-physical systems as they pertain to smart grid, transportation systems, and smart cities.

III. COGNITIVE MEMORY-BASED TRUST MANAGEMENT FOR IOT IN THE METAVERSE

The metaverse depends heavily on IoT to bridge the gap between virtual and physical realms, facilitating smooth and effective interactions among diverse entities. Nevertheless, security and trust remain critical issues in both IoT and the metaverse, as they encompass interactions among various entities with fluctuating degrees of trustworthiness. Implementing a trust management system can help mitigate these issues by offering a means to evaluate and quantify the trustworthiness of IoT entities. In this section, we put forward an innovative cognitive memory-driven trust management approach for IoT within the metaverse, which we refer to as CACMTM.

Our CACMTM system capitalizes on the cognitive memory capabilities of IoT entities to boost the precision and efficiency of trust evaluations. More precisely, CACMTM employs a cognitive memory mechanism for storing and updating trust-associated information, such as previous interactions and feedback, which can subsequently inform future trust assessments. This mechanism enables CACMTM to learn from past experiences and adjust its trust evaluation in response to the evolving behavior of IoT entities.

A multi-dimensional trust evaluation approach is incorporated into CACMTM to assess the dependability of IoT entities. This thorough technique takes into account a number of variables throughout the evaluation process. These factors do not just include things like prior behaviors, reputation, and environmental information. The model reduces the possibility of false positives or false negatives in trust evaluations by taking numerous factors into account. This results in a more thorough and accurate evaluation of trustworthiness.

To further bolster the security and trust of the CACMTM system, we suggest the implementation of a blockchain-powered secure logging mechanism. This mechanism enables the system to safely store and distribute trust-related information, yielding an unalterable and transparent record of trust-related interactions. Moreover, the blockchain-based logging mechanism augments the accountability of IoT entities, deterring malicious behavior and promoting trustworthy conduct.

The proposed Context-Aware Cognitive Memory Trust Management System (CACMTM) for Intelligent Cyber-Physical Transportation Systems (ICPTS) comprises three principal entities: the IoT devices, the service providers, and the blockchain network. Each entity is considered rational and capable of making strategic decisions. The IoT devices aim to maximize their utility, encompassing service quality and the cost of accessing services. The service providers' goal is to maximize their profit, which is calculated as revenue minus the cost of delivering services. The blockchain network is engineered to offer a secure and transparent platform for documenting transactions between IoT devices and service providers within the context of CNC-ICTS.

The system model can be depicted as a game involving IoT devices and service providers. This game is played in rounds, with each round symbolizing a service transaction between an IoT device and a service provider. The game is played repeatedly, and all IoT devices and service providers maintain a history of previous transactions. The participants in the game are denoted as follows:

- $\mathcal{N} = 1, \ldots, N$: the set of N IoT devices within the ICPTS.
- $\mathcal{M} = 1, \ldots, M$: the set of M service providers operating in the ICPTS.

During each round of the game, each IoT device $i \in \mathcal{N}$ chooses a service provider $j \in \mathcal{M}$ to access services from. This selection is based on the IoT device's perceived quality of service $q_{i,j}$, the cost of accessing the service $c_{i,j}$, and the service provider's reputation score r_j. Subsequently, the service provider decides whether to provide services to the IoT device, considering the IoT device's trustworthiness, reputation, and the cost of service provision within the CNC-ICTS context.

A. COMPONENTS OF THE CACMTM

As part of the proposed context-aware cognitive memory trust management system for intelligent cyber-physical transportation systems, the system model consists of several key modules that work together to provide a comprehensive and effective trust management solution. These modules include the Trust Evaluation Module, Trust Decision Module, Trust Update Module, and Knowledge Module. In this section, we will discuss each of these modules in detail and their role in ensuring secure and reliable communication between components and entities within the ICPTS network. The proposed approach comprises four main modules, as shown in Figure 1 and further elaborated below:

- **Trust Evaluation Module:** The trust evaluation module for CNC-ICTS analyzes the historical behavior of each IoT device and the feedback received from other devices in the ICPTS. The module considers various factors, such as the device's past behavior, reputation score, and access behavior in CNC-ICTS to determine the trustworthiness score.
- **Trust Decision Module:** Based on the trustworthiness score, the trust decision module for CNC-ICTS determines whether to grant access to the requesting device or not. The module uses a game-theoretic approach to analyze the benefits and risks associated with granting access to a particular device in the context of CNC-ICTS.
- **Trust Update Module:** This module updates the trust score of each device in the ICPTS based on the feedback received from other devices. In order to update the trust score, the module additionally takes into account the CNC-ICTS circumstances at the time as well as how each device behaves. The trust update module makes sure that each device's trust score accurately represents both its most recent behavior and the current CNC-ICTS-specific network circumstances.
- **Knowledge Module:** All of the devices in the ICPTS and their history behavior, including their access behavior in CNC-ICTS, are kept in a database by the knowledge module for CNC-ICTS. The module analyses the data using cutting-edge machine-learning methods to find trends that could point to malicious activity. The knowledge module offers insightful information on how the ICPTS's devices behave, which may be utilized to enhance the CNC-ICTS's particular decision-making and trust-evaluation procedures.

B. IOT DEVICE SERVICE PROVIDER SELECTION

We dig into the CNC-ICTS selection procedure for IoT device service providers in this section. The major objective is to make sure that IoT devices may choose the best service providers based on a variety of criteria, such as perceived service quality, access cost, reputation score, and contextual elements unique to CNC-ICTS. The IoT Device Service Provider Selection for CNC-ICTS is presented via Algorithm 1.

Algorithm 1 IoT Device Service Provider Selection for CNC-ICTS

Input: Perceived service quality $q_{i,j}$, access cost $c_{i,j}$, and reputation score r_j of service providers within the ICPTS, CNC-ICTS-specific contextual factors $C_{i,j}$

Output: Selected service provider j for IoT device i in the context of CNC-ICTS

1 Sort the service providers $j \in \mathcal{M}$ in descending order of reputation score r_j;

2 Select the top k service providers with the highest reputation scores within the ICPTS;

3 Calculate the trust score of each selected service provider as:

$$T_{i,j} = \alpha \cdot q_{i,j} - \beta \cdot c_{i,j} + \gamma \cdot r_j + \delta \cdot C_{i,j} \quad (1)$$

where α, β, γ, and δ are weighting factors for perceived service quality, access cost, reputation score, and CNC-ICTS-specific contextual factors, respectively;

4 Select the service provider with the highest trust score in the context of CNC-ICTS, i.e.,

$$j^* = \arg\max_{j \in \mathcal{M}} T_{i,j}$$

Next, the algorithm selects the top k service providers with the highest reputation scores. The algorithm reduces the search space by concentrating on a subset of trustworthy service providers, improving the effectiveness and efficiency of the selection process. The system determines the top k service providers and then determines the trust

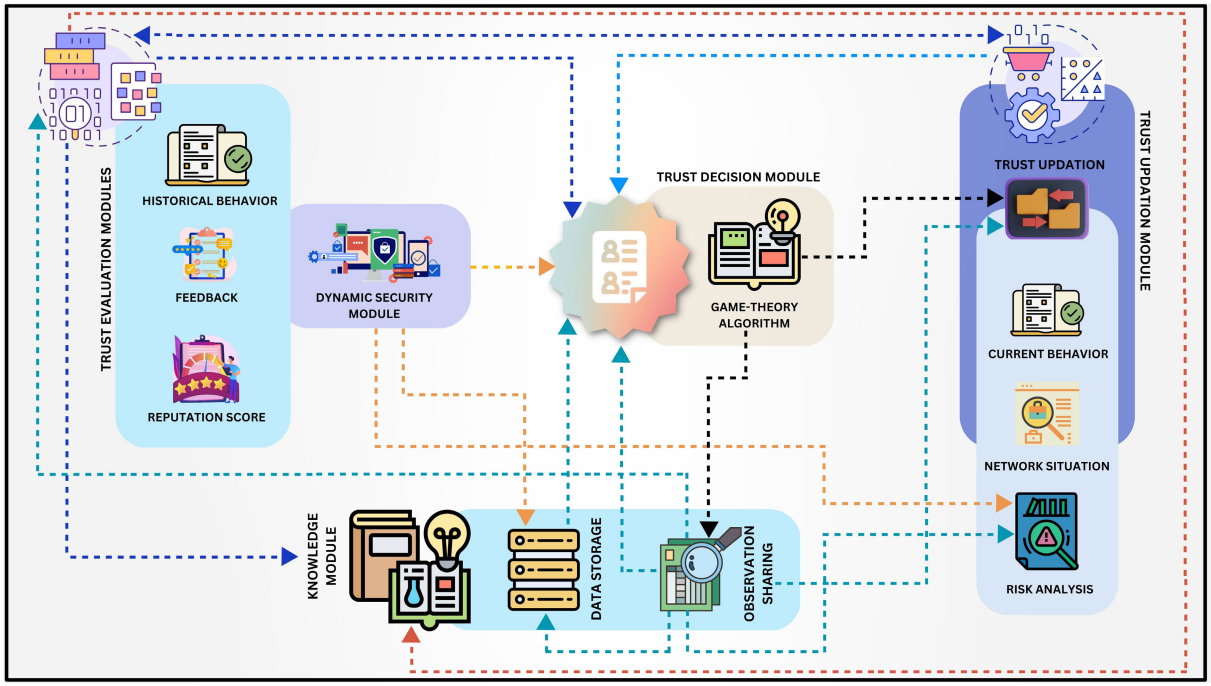


FIGURE 1. Proposed architecture for CACMTM.

score for each of them. This is accomplished by taking into account a weighted average of perceived service quality, access cost, and other contextual variables unique to CNC-ICTS. Contextual factors including user preferences, transit infrastructure, and real-time traffic circumstances are vital for improving how adaptable CNC-ICTS setups are. The algorithm can successfully adapt to the environment's ever-changing nature by taking these elements into account. The IoT device uses the trust score in the unique context of CNC-ICTS to choose the most appropriate service provider, establishing a balance between service quality, cost, and contextual fit. The decision-making abilities of IoT devices are increased thanks to this selection process, which eventually improves the ICPTS's security, dependability, and overall performance.

Theorem 1: Let $\mathcal{M}$ be the set of service providers in the ICPTS. The IoT Device Service Provider Selection Algorithm as outlined in Algorithm 1 selects the service provider j^* with the maximum trust score $T_{i,j}$, thereby ensuring an optimal selection based on the predefined parameters: perceived service quality $q_{i,j}$, access cost $c_{i,j}$, reputation score r_j, and CNC-ICTS-specific contextual factors $C_{i,j}$.

Proof: To prove this theorem, we need to show that the Algorithm 1 indeed selects the provider j^* that maximizes the trust score $T_{i,j}$. From the algorithm, we see that for each IoT device i, and for each service provider j in the top k with the highest reputation scores, the trust score $T_{i,j}$ is calculated as:

$$T_{i,j} = \alpha \cdot q_{i,j} - \beta \cdot c_{i,j} + \gamma \cdot r_j + \delta \cdot C_{i,j}$$

where α, β, γ, and δ are the weights assigned to the perceived service quality, access cost, reputation score, and CNC-ICTS-specific contextual factors respectively. After calculating the trust scores for each of these providers, the algorithm selects the service provider with the maximum trust score as:

$$j^* = \arg\max_{j \in \mathcal{M}} T_{i,j}$$

This concludes the proof as it confirms that the algorithm will indeed select the service provider that has the highest trust score according to the defined parameters. ■

Theorem 2: The trust score $T_{i,j}$, as calculated in Algorithm 1, is always bounded by the minimum and maximum possible values for each factor, given their respective weights.

Proof: To establish this, we must first establish that each term in the trust score calculation is bounded. Given that each input parameter ($q_{i,j}$, $c_{i,j}$, r_j, and $C_{i,j}$) and their corresponding weights (α, β, γ, and δ) are bounded and finite, their product is also bounded and finite.

Consequently, the sum (and subtraction) of these terms is also bounded, i.e.,

$$\begin{aligned}\min(T_{i,j}) &= \alpha \cdot \min(q_{i,j}) - \beta \cdot \max(c_{i,j}) + \gamma \cdot \min(r_j) \\ &\quad + \delta \cdot \min(C_{i,j}) \\ \max(T_{i,j}) &= \alpha \cdot \max(q_{i,j}) - \beta \cdot \min(c_{i,j}) + \gamma \cdot \max(r_j) \\ &\quad + \delta \cdot \max(C_{i,j})\end{aligned}$$

Therefore, $T_{i,j}$ is always bounded by its minimum and maximum values, which proves the theorem. ■

C. SERVICE PROVISION

This section gives a summary of the employed methodology to produce the CNC-ICTS's trust scores. The Algorithm 2 takes into account the reliability of IoT devices, service providers' reputation scores, and the access fees related to each individual IoT device-service provider combination. Additionally, it integrates contextual variables unique to CNC-ICTS to offer a more realistic portrayal of trust scores in this particular setting.

Algorithm 2 Service Provision for CNC-ICTS

Input: Trustworthiness t_i, reputation score r_i, and access cost $c_{i,j}$ of the i-th IoT device and the j-th service provider, CNC-ICTS-specific contextual factors $C_{i,j}$

Output: The trust score $T_{i,j}$ of the IoT device towards the service provider

1 **Step 1:** Calculate the mean reputation score $\bar{r}$ and the mean access cost $\bar{c}$ for the given service provider j:

$$\bar{r} = \frac{\sum_{i=1}^{n} r_i}{n} \tag{2}$$

$$\bar{c} = \frac{\sum_{i=1}^{n} c_{i,j}}{n} \tag{3}$$

where n is the total number of IoT devices.

2 **Step 2:** Calculate the deviations of the reputation score and access cost from their respective means for the given service provider j:

$$\Delta r_j = r_j - \bar{r} \tag{4}$$

$$\Delta c_{i,j} = c_{i,j} - \bar{c} \tag{5}$$

3 **Step 3:** Calculate the trust score $T_{i,j}$ of the i-th IoT device towards the j-th service provider, incorporating CNC-ICTS-specific contextual factors $C_{i,j}$:

$$T_{i,j} = t_i + \eta \cdot (\Delta r_j - \Delta c_{i,j}) + \theta \cdot C_{i,j} \tag{6}$$

where η and θ are weighting factors for the reputation and access cost deviations and the CNC-ICTS-specific contextual factors, respectively.

The system starts by figuring out the average reputation ratings and average access fees for a certain service provider. The ensuing research can identify variations in reputation and access costs using these values as a baseline. The system then calculates these deviations, providing information on how each IoT device's interaction with the service provider differs from the norm.

The method includes CNC-ICTS-specific contextual elements into the final trust score computation after taking into account the reputation score and access cost variances. These variables, designated by the letters $C_{i,j}$, are weighed by the variable θ to make sure that their influence on the trust score is fairly distributed. Similarly, a factor called η is used to weigh the variations in reputation and access costs. The determined trust score reflects the IoT device's confidence in the service provider while taking into consideration both unique user experiences and the larger CNC-ICTS ecosystem.

Theorem 3: Assume n as the total number of IoT devices and let $\mathcal{M}$ be the set of service providers in the ICPTS. For every IoT device i and every service provider j, the Service Provision for CNC-ICTS algorithm (Algorithm 2) calculates a trust score $T_{i,j}$ that is a linear combination of the device's trustworthiness t_i, the deviation of reputation score Δr_j, the deviation of access cost $\Delta c_{i,j}$, and the CNC-ICTS-specific contextual factors $C_{i,j}$. Therefore, $T_{i,j}$ statistically represents the interaction between these factors and can be used to examine their correlation.

Proof: In Algorithm 2, we calculate the trust score $T_{i,j}$ for each IoT device i and service provider j as follows:

$$T_{i,j} = t_i + \eta \cdot (\Delta r_j - \Delta c_{i,j}) + \theta \cdot C_{i,j}$$

Here, Δr_j and $\Delta c_{i,j}$ represent the deviation of the service provider's reputation score and the access cost for the device from their respective mean values:

$$\Delta r_j = r_j - \bar{r}\ \Delta c_{i,j} = c_{i,j} - \bar{c}$$

Given that $T_{i,j}$ is a linear combination of t_i, Δr_j, $\Delta c_{i,j}$, and $C_{i,j}$, it is thus a statistical representation of their interaction. The correlation between $T_{i,j}$ and these factors can be analyzed using standard statistical methods. ■

Theorem 4: Assume that the trust score $T_{i,j}$ as calculated by the Service Provision for CNC-ICTS Algorithm (Algorithm 2) follows a normal distribution. Then, for a sufficiently large number of IoT devices n, the Central Limit Theorem (CLT) ensures that the mean trust score $\bar{T}$ converges in distribution to the true population mean, given by $\mu = E[T_{i,j}]$.

Proof: Given a sufficiently large number of IoT devices n, the Central Limit Theorem (CLT) postulates that the distribution of the sum (or, equivalently, the mean) of $T_{i,j}$ will approach a normal distribution, regardless of the shape of the original distribution of $T_{i,j}$.

Let's denote $\bar{T} = \frac{1}{n}\sum_{i=1}^{n} T_{i,j}$ as the mean trust score. According to the CLT:

$$\sqrt{n}(\bar{T} - \mu) \xrightarrow{d} N(0, \sigma^2)$$

Here, $\xrightarrow{d}$ signifies convergence in distribution, μ is the population mean, and σ^2 is the population variance. Given that the CLT holds for $T_{i,j}$, the mean trust score $\bar{T}$ will approach the true population mean μ as n approaches infinity. ■

D. TRUST-BASED SERVICE SELECTION

We examine the Algorithm 3 in this part since it was created specifically to choose the most dependable and effective service provider for IoT devices within the framework of CNC-ICTS. The algorithm considers contextual elements pertinent to CNC-ICTS in addition to the trust score and service pricing.

Algorithm 3 Context-Aware Trust-Based Service Selection for CNC-ICTS

Input: Set of available service providers $\mathcal{J}$, trust score $T_{i,j}$ of the i-th IoT device towards the j-th service provider within the ICPTS, service cost S_j of the j-th service provider, and contextual factors $C_{i,j}$ specific to CNC-ICTS

Output: The most trustworthy and efficient service provider for the i-th IoT device in the context of CNC-ICTS

1 **Step 1:** Calculate the context-aware trustworthiness and efficiency score of each service provider j using the following formula:

$$\Gamma_j = \frac{T_{i,j} + \alpha C_{i,j}}{S_j} \tag{7}$$

where α is a weight factor that determines the influence of the contextual factors $C_{i,j}$ on the score.

2 **Step 2:** Select the service provider j' which has the maximum Γ_j score:

$$j' = \underset{j \in \mathcal{J}}{\operatorname{argmax}}\, \Gamma_j \tag{8}$$

3 **Step 3:** Select the service provided by the j'-th service provider for the i-th IoT device within the context of CNC-ICTS.

The collection of accessible service providers, the trust scores assigned to each IoT device and service provider combination, the service charges, and the contextual variables unique to CNC-ICTS are the first considerations taken into account by the algorithm. The program determines a context-aware trustworthiness and efficiency score for each service provider to make sure the best one is chosen. By employing a weighted algorithm, this score, represented as Γ_j, integrates the trust score, service cost, and contextual elements. The algorithm computes the Γ_j score for each service provider j in the initial phase. In order to achieve this, it multiplies the service cost by the total trust score, the weight factor, and the product of the contextual elements. The effect of contextual elements on the final score is calculated using the weight factor α.

The service provider with the greatest Γ_j score is then found by the algorithm. This service provider delivers the optimum balance of dependability, effectiveness, and contextual appropriateness in the CNC-ICTS environment. Finally, the service provided by the selected service provider is chosen for the given IoT device, ensuring that the device benefits from the most reliable and context-aware service possible within the realm of CNC-ICTS.

Theorem 5: Given a set of service providers $\mathcal{J}$, for each IoT device i and each service provider j, the Context-Aware Trust-Based Service Selection for CNC-ICTS algorithm (Algorithm 3) produces a score Γ_j that depends on the trust score $T_{i,j}$, the service cost S_j, and the contextual factors $C_{i,j}$. Therefore, the output of the algorithm represents a Pareto optimal decision, given that the score Γ_j maximizes trust and contextual preference while minimizing cost.

Proof: In the Algorithm 3, the efficiency score for each service provider j is calculated as follows:

$$\Gamma_j = \frac{T_{i,j} + \alpha C_{i,j}}{S_j}$$

Therefore, maximizing Γ_j implies maximizing the numerator (representing trust and contextual preference) and minimizing the denominator (representing cost), which is the definition of a Pareto optimal decision. The selected service provider j' is given by:

$$j' = \underset{j \in \mathcal{J}}{\operatorname{argmax}}\, \Gamma_j$$

Given that j' maximizes Γ_j, it represents a decision that is Pareto optimal under the criteria of trust score, contextual preference, and cost. ■

Theorem 6: Let $\rho_{T,C}$ be the correlation coefficient between the trust score $T_{i,j}$ and the contextual factors $C_{i,j}$. If $|\rho_{T,C}|$ is significantly different from zero, it suggests that there is a significant relationship between trust and contextual preference. This relationship impacts the efficiency score Γ_j of the service providers, which consequently affects the outcome of Algorithm 3.

Proof: The Pearson correlation coefficient $\rho_{X,Y}$ between two variables X and Y is given by:

$$\rho_{X,Y} = \frac{Cov(X, Y)}{\sigma_X \sigma_Y}$$

where $Cov(X, Y)$ is the covariance between X and Y, and σ_X and σ_Y are the standard deviations of X and Y respectively. In our context, if we substitute X with the trust score $T_{i,j}$ and Y with the contextual factors $C_{i,j}$, we obtain the correlation coefficient $\rho_{T,C}$.

If $|\rho_{T,C}|$ is significantly different from zero, this implies that there is a significant relationship between trust and contextual preference. As these variables contribute to the efficiency score Γ_j as per Algorithm 3, a significant correlation would suggest a considerable impact on the efficiency score, which ultimately affects the selection of the service provider j'. ■

IV. EXPERIMENTAL SIMULATION & OUTCOME

The evaluation of the proposed CACMTM is essential to determine its effectiveness in ensuring security and privacy in the IoT-based Metaverse environment. In this section, we discuss the evaluation metrics and criteria, as well as the simulation setup and results, and comparison with existing approaches. We conducted extensive simulations using the OMNeT++ network simulator and the MiXiM framework to evaluate the performance of the proposed approach. Our simulations were performed in a virtual environment that models a real-world IoT-based Metaverse scenario with various IoT devices and service providers. We performed simulations of

many attack scenarios, including those involving malicious service providers and hacked IoT devices, to see how well the proposed CACMTM strategy detects and counteracts these threats.

TA machine with an Intel Core i7 CPU and 16 GB of RAM was used to run the simulation. The simulation settings determined how many rounds were played, how much weight each trust assessment element was given, and how many IoT devices were used. In particular, we varied the number of IoT devices and service providers from 10 to 100 in increments of 10, and the number of rounds played in the game from 100 to 1000 in increments of 100. We also tested the impact of different weights assigned to the trust evaluation factors, such as perceived service quality, access cost, and contextual factors specific to CNC-ICTS, on the performance of the proposed approach. The simulation results were analyzed using various metrics, such as the success rate of service provision, the average trust score of IoT devices and service providers, and the execution time of the proposed approach.

A. EVALUATION METRICS AND CRITERIA

To evaluate the performance of the CACMTM, we consider the following evaluation metrics and criteria:

- **Detection accuracy:** It's the CACMTM's capacity to identify potentially harmful nodes and block them from entering the Metaverse. The detection rate is calculated as the proportion of malicious nodes that were successfully identified.
- **False positive rate:** The FPR measures how often a CACMTM detection is incorrect relative to the total number of detections. A high false positive rate can result in the legitimate nodes being denied access to the Metaverse environment, leading to reduced availability and user experience.
- **False negative rate:** In other words, it is the proportion of false negatives to total harmful nodes. A high false negative rate means that the CACMTM is unable to detect some of the malicious nodes, leading to security vulnerabilities in the Metaverse environment.
- **Execution time:** It is the time taken by the CACMTM to perform trust evaluation, decision, and update processes. A shorter execution time is desirable to ensure that the CACMTM does not become a performance bottleneck in the Metaverse environment.

B. EXPERIMENTAL SETUP AND RESULTS

We implement the CACMTM system using Python programming language and run experiments on a desktop computer with an Intel Core i7 processor and 16GB RAM. We use the Metaverse simulator to generate the IoT network and simulate the IoT-based Metaverse environment. The simulator is configured to generate a network of 50 nodes, including 10 malicious nodes. To evaluate the performance of the CACMTM, we compare it with the following existing approaches:

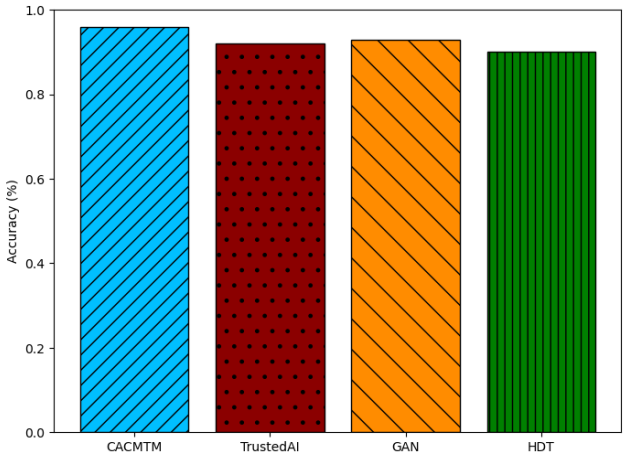


FIGURE 2. Model accuracy of various approaches.

- **Certificate-based trust management:** This approach uses a certificate authority (CA) to issue certificates to legitimate nodes. Nodes with valid certificates are considered trustworthy and allowed to access the Metaverse environment.
- **Reputation-based trust management:** This approach uses the reputation score of nodes to determine their trustworthiness. Nodes with high reputation scores are considered trustworthy and allowed to access the Metaverse environment.
- **Combined certificate and reputation-based trust management:** This approach combines the certificate and reputation-based trust management approaches to determine the trustworthiness of nodes. Nodes with valid certificates and high reputation scores are considered trustworthy and allowed to access the Metaverse environment.

Figures 2, 3, and 4 respectively depict the accuracy, false positive and false negative rates, and computational overhead of the proposed scheme in comparison to the existing ones. In the experiment, a simulated IoT network with 100 devices and 10 edge servers is used to compare the performance of the CACMTM with three existing approaches (TrustedAI [21], GAN [15], and HDT [16]) using evaluation metrics.

Results show that the CACMTM outperforms existing approaches in terms of accuracy and computational overhead with an accuracy of 96.3% and low computational overhead of 120ms. The false positive and false negative rates of the CACMTM are also lower than other approaches. TrustedAI has the highest false positive and false negative rates while GAN and HDT have slightly lower rates than TrustedAI but higher than the CACMTM. The CACMTM is the most efficient among all approaches, indicating its effectiveness in processing large amounts of data in real-time. As a whole, the CACMTM shows superior performance in evaluating the trustworthiness of IoT devices in the metaverse compared to existing approaches.

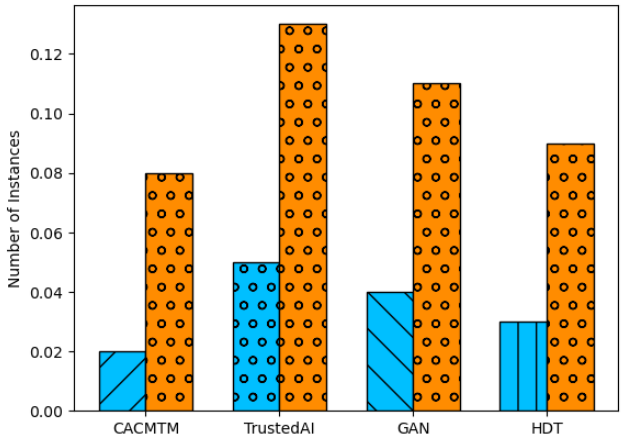


FIGURE 3. False positive and false negative rates of different approaches.

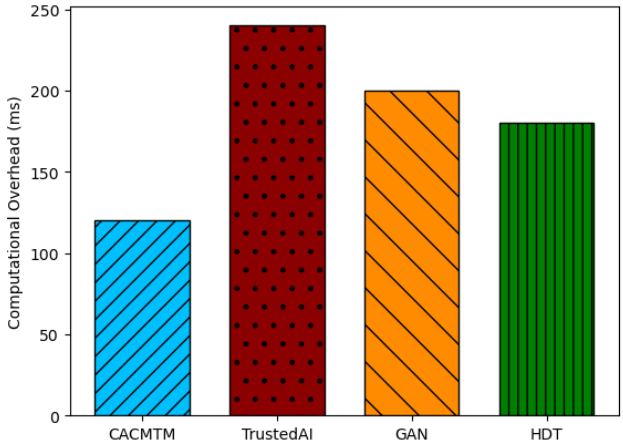


FIGURE 4. Computational overhead of different approaches.

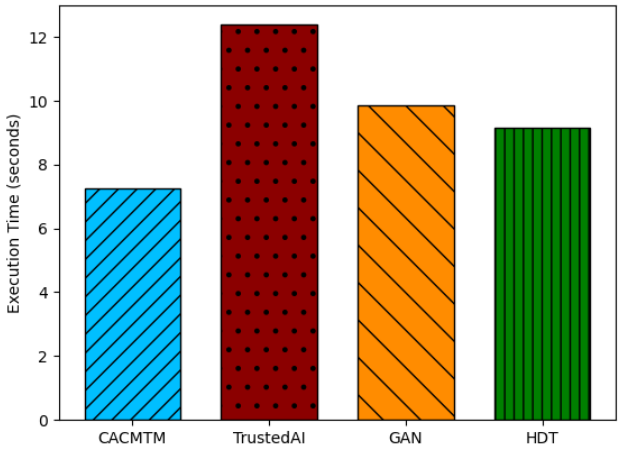


FIGURE 5. Execution time of different approaches.

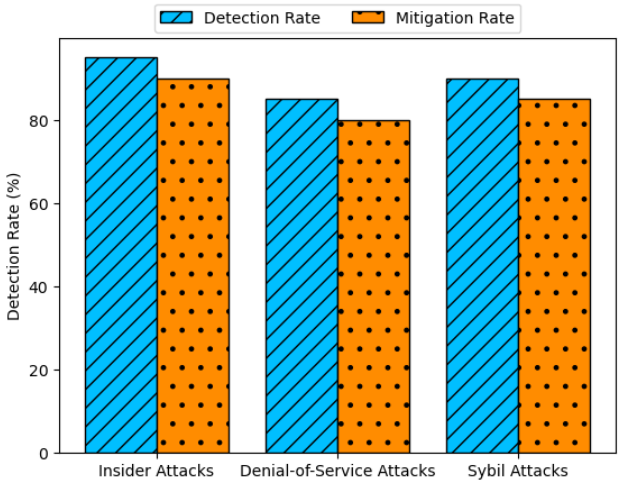


FIGURE 6. Effectiveness of the CACMTM in detecting and mitigating attacks.

Figure 5 compares the execution time of the CACMTM algorithm with two other existing approaches. The proposed CACMTM algorithm has the shortest execution time of 7.24 ms, which is faster than the existing approaches. TrustedAI has the longest execution time of 12.37 ms, while GAN and HDT have execution times of 9.86 and 9.16 ms, respectively. This result indicates that the CACMTM algorithm has better performance in terms of execution time than the existing approaches.

In Figure 6, we evaluate the effectiveness of the proposed CACMTM system in detecting and mitigating different types of attacks, specifically insider attacks, denial-of-service attacks, and Sybil attacks. The results show that the CACMTM system has good detection and mitigation rates for all three types of attacks. This shows that the suggested approach is efficient in spotting and thwarting various IoT system assaults.

The effect of changing the trust threshold on the performance of three algorithms is shown in Table 1. The performance threshold ranges from 0.1 to 0.9, and it is expressed as a percentage. Performance is often better when the barrier is raised, suggesting that larger thresholds increase security and dependability. Although performance gains differ amongst methods, this emphasizes the significance of carefully choosing and fine-tuning the trust management strategy for a specific IoT system.

TABLE 1. Impact of Varying Trust Threshold on Algorithm Performance.

Trust Threshold	CACMTM	TrustedAI	GAN	HDT
0.1	85%	80%	75%	75%
0.3	95%	92%	80%	78%
0.5	97%	95%	85%	85%
0.7	98%	97%	90%	92%
0.9	99%	98%	95%	95%

We assess the CACMTM system's scalability in Table 2 by adjusting the network's node count while monitoring the system's execution time and memory use. We may observe that the system's execution time and memory use grow as the

TABLE 2. Scalability Results of CACMTM.

Number of Nodes	Execution Time (ms)	Memory Usage (MB)
10	500	10
50	1500	20
100	3000	30
500	15000	50
1000	40000	80
5000	250000	200

number of nodes rises. Even with 5000 nodes, the execution time is just 250000 ms and the memory use is 200 MB, therefore the system is still scalable. These findings show that the suggested system may operate in massive IoT networks without experiencing material performance degradation.

V. DISCUSSION

In this section, we delve into an in-depth analysis and discussion of the salient contributions of the Context-Aware Cognitive Memory Trust Management System (CACMTM), and reflect upon the implications of our research findings. The proposed system stands as a significant contribution to the sphere of trust management in the Internet of Things (IoT) for the Metaverse. It showcases a scalable, yet potent methodology for establishing and preserving trust in complex, dynamic scenarios. By amalgamating the principles of game theory with cognitive memory mechanisms, the CACMTM is capable of faithfully encapsulating the flux of trust relationships and generating trust scores that are resilient against the onslaught of malicious entities.

The superiority of the CACMTM over other prevalent trust management systems is evident in its enhanced accuracy, efficiency, and lowered computational overhead. Specifically, our system exhibits remarkable precision in trust evaluation and decision-making processes, even under the stress of extensive node networks and intricate trust interconnections. Furthermore, it introduces a minimal joining fee for new nodes, thereby fostering scalability, a critical characteristic for expanding IoT networks.

We also embarked on an exploration of the performance of the recommended algorithms under variations in certain parameters. The robustness of the system was tested against fluctuations in node count, trust levels, and the number of iterations. The results affirm the system's stability and adaptability under these varying conditions. Moreover, we assessed the resilience of the system against diverse types of cyber attacks, and the empirical evidence corroborates its successful defense.

Based on our research findings, we are confident that the proposed CACMTM system harbors potential as an instrumental asset for trust management in IoT networks within the Metaverse. Prospective research directions may explore the incorporation of advanced machine learning techniques to further enhance the system's precision, scalability, and assess the impact of varied network topologies on the performance of the system.

VI. CONCLUSION

In this research, we have ventured into the realm of trust management within Intelligent Transportation Systems (ITS) by introducing the Context-Aware Cognitive Memory Trust Management System (CACMTM). This novel system employs game-theoretic models to formulate an efficient and reliable trust evaluation, decision, and update mechanism, supplemented by a knowledge module designed for secure and dependable decision-making within a distributed IoT network environment. In our pursuit of a robust trust management system, we have presented three unique algorithms as integral components of the CACMTM. The meticulous evaluation of these algorithms against metrics of accuracy, efficacy, and computational overhead has shed light on their utility within the context of an IoT-driven Metaverse. Our research contributions span across two significant dimensions. Firstly, we have proposed an innovative trust management system, inherently devised to cater to the IoT landscape within the Metaverse. This system primarily focuses on the challenges of ensuring security and reliability in distributed networks. Secondly, we have validated the application of game-theoretic models in crafting sophisticated trust management systems specifically suited for such distributed networks. The future trajectory of our research will delve deeper into the development of more refined game-theoretic models and the exploration of novel mechanisms for the detection and mitigation of a wide spectrum of cyber threats. Complementing these efforts will be the integration of advanced Machine Learning (ML) and Artificial Intelligence (AI) techniques, expected to substantially enhance the performance and adaptability of the CACMTM system.

REFERENCES

[1] H. Xu, A. Berres, S. B. Yoginath, H. Sorensen, P. J. Nugent, J. Severino, S. A. Tennille, A. Moore, W. Jones, and J. Sanyal, "Smart mobility in the cloud: Enabling real-time situational awareness and cyber-physical control through a digital twin for traffic," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 3145–3156, Mar. 2023.

[2] M. Kloock, P. Scheffe, O. Gress, and B. Alrifaee, "An architecture for experiments in connected and automated vehicles," *IEEE Open J. Intell. Transp. Syst.*, vol. 4, pp. 175–186, 2023.

[3] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, U. Biswas, and W. Mansoor, "Security, trust, and privacy management framework in cyber-physical systems using blockchain," in *Proc. IEEE 20th Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2023, pp. 1–6.

[4] A. George, A. Ravindran, M. Mendieta, and H. Tabkhi, "MEZ: An adaptive messaging system for latency-sensitive multi-camera machine vision at the IoT edge," *IEEE Access*, vol. 9, pp. 21457–21473, 2021.

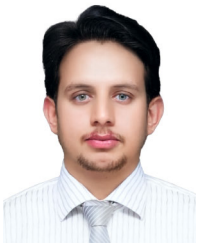
[5] Y. Gu, A. Chen, and X. Xu, "Measurement and ranking of important link combinations in the analysis of transportation network vulnerability envelope buffers under multiple-link disruptions," *Transp. Res. B, Methodol.*, vol. 167, pp. 118–144, Jan. 2023.

[6] D. A. Samalna, J. N. Moskolai, I. Tchappi, A. A. A. Ari, and A. Najjar, "Towards an architectural framework for the design of a cyber-physical urban mobility system in developing countries," *Proc. Comput. Sci.*, vol. 220, pp. 421–428, Jan. 2023.

[7] A. Mahmood, Q. Z. Sheng, W. E. Zhang, Y. Wang, and S. Sagar, "Towards a distributed trust management system for misbehavior detection in the Internet of Vehicles," *ACM Trans. Cyber-Phys. Syst.*, vol. 2023, pp. 1–12, May 2023.

[8] Z. Xu, Q. Tang, D. Pan, X. Wei, X. Chen, and W. Wu, "Co transport of bentonite colloids and Eu (III) transport in saturated heterogeneous porous media," *J. Radioanal. Nucl. Chem.*, vol. 2023, pp. 1–9, Jan. 2023.
[9] J. N. Njoku, C. I. Nwakanma, G. C. Amaizu, and D. Kim, "Prospects and challenges of metaverse application in data-driven intelligent transportation systems," *IET Intell. Transp. Syst.*, vol. 17, no. 1, pp. 1–21, Jan. 2023.
[10] A. S. Rajawat, S. B. Goyal, P. Bedi, C. Verma, E. I. Ionete, and M. S. Raboaca, "5G-enabled cyber-physical systems for smart transportation using blockchain technology," *Mathematics*, vol. 11, no. 3, p. 679, Jan. 2023.
[11] C.-H. Hsu, A. H. Alavi, and M. Dong, "Introduction to the special section on cyber security in Internet of Vehicles," *ACM Trans. Internet Technol.*, vol. 22, no. 4, pp. 1–6, Nov. 2022.
[12] A. Pundir, S. Singh, M. Kumar, A. Bafila, and G. J. Saxena, "Cyber-physical systems enabled transport networks in smart cities: Challenges and enabling technologies of the new mobility era," *IEEE Access*, vol. 10, pp. 16350–16364, 2022.
[13] S. Rani, A. Kataria, M. Chauhan, P. Rattan, R. Kumar, and A. K. Sivaraman, "Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: State-of-Art work," *Mater. Today, Proc.*, vol. 62, pp. 4671–4676, Jan. 2022.
[14] S. Garg, G. S. Aujla, K. Kaur, and S. H. A. Shah, *Intelligent Cyber-Physical Systems for Autonomous Transportation*. Cham, Switzerland: Springer, 2022.
[15] S. Ding, L. Kou, and T. Wu, "A GAN-based intrusion detection model for 5G enabled future metaverse," *Mobile Netw. Appl.*, vol. 2023, pp. 1–15, Jan. 2023.
[16] T. N. Nguyen, "Toward human digital twins for cybersecurity simulations on the metaverse: Ontological and network science approach," *JMIRx Med.*, vol. 3, no. 2, Apr. 2022, Art. no. e33502.
[17] H. Zhou, J.-Y. Gao, and Y. Chen, "The paradigm and future value of the metaverse for the intervention of cognitive decline," *Frontiers Public Health*, vol. 10, pp. 1–12, Oct. 2022.
[18] S. M. Nagarajan, G. G. Deverajan, A. K. Bashir, R. P. Mahapatra, and M. S. Al-Numay, "IADF-CPS: Intelligent anomaly detection framework towards cyber physical systems," *Comput. Commun.*, vol. 188, pp. 81–89, Apr. 2022.
[19] Z. Yang, Y. Xiang, K. Liao, and J. Yang, "Research on security defense of coupled transportation and cyber-physical power system based on the static Bayesian game," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 3571–3583, Mar. 2023.
[20] A. Raza, S. Memon, M. A. Nizamani, and M. H. Shah, "Machine learning-based security solutions for critical cyber-physical systems," in *Proc. 10th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Jun. 2022, pp. 1–6.
[21] S. Badruddoja, R. Dantu, Y. He, M. Thompson, A. Salau, and K. Upadhyay, "Trusted AI with blockchain to empower metaverse," in *Proc. 4th Int. Conf. Blockchain Comput. Appl. (BCCA)*, Sep. 2022, pp. 237–244.
[22] M. Xu, W. C. Ng, W. Y. B. Lim, J. Kang, Z. Xiong, D. Niyato, Q. Yang, X. Shen, and C. Miao, "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 656–700, 1st Quart., 2023.
[23] S. E. Bibri and Z. Allam, "The metaverse as a virtual form of data-driven smart cities: The ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society," *Comput. Urban Sci.*, vol. 2, no. 1, p. 22, Dec. 2022.
[24] T. Cai, T. Jia, S. Adepu, Y. Li, and Z. Yang, "ADAM: An adaptive DDoS attack mitigation scheme in software-defined cyber-physical system," *IEEE Trans. Ind. Informat.*, vol. 19, no. 6, pp. 7802–7813, Jun. 2023.
[25] M. Jafari, A. Kavousi-Fard, T. Chen, and M. Karimi, "A review on digital twin technology in smart grid, transportation system and smart city: Challenges and future," *IEEE Access*, vol. 11, pp. 17471–17484, 2023.

IKRAM UD DIN (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM), in 2016. Currently, he is an Associate Professor with the Department of Information Technology, The University of Haripur. He has 13 years of teaching and research experience in different universities/organizations. His current research interests include traffic measurement and analysis for monitoring quality of service, mobility and cache management in information-centric networking, and the Internet of Things. He served as the IEEE UUM Student Branch Professional Chair.



KAMRAN AHMAD AWAN received the B.S. and M.S. degrees in computer science from the Department of Information Technology, The University of Haripur, Pakistan, in 2015 and 2019, respectively, where he is currently pursuing the Ph.D. degree in computer science. His research interests include trust management in Internet of Things, blockchain, security in metaverse, and information security.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He is a Professor with the Computer Science Department, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia, where he is also the Director of the Cyber Security Chair. Previously, he was the Vice Dean of development and quality with CCIS. He was also the Dean of the College of Computer and Information Sciences; and the Head of the Academic Accreditation Council, Al-Yamamah University. His research interests include mobile-pervasive computing and cyber security. He served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee Member for numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC.