IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 January 2024, accepted 29 January 2024, date of publication 1 February 2024, date of current version 8 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3361407

RESEARCH ARTICLE

Improving the Robustness of IoT-Powered Smart City Applications Through Service-Reliant Application Authentication Technique

JAMIL ABEDALRAHIM JAMIL ALSAYAYDEH[1], (Member, IEEE), IRIANTO[2], MOHANAD FAEQ ALI[3], MOHAMMED NASSER MOHAMMED AL-ANDOLI[4], AND SAFARUDIN GAZALI HERAWAN[5]

[1]Department of Engineering Technology, Fakulti Teknologi and Kejuruteraan Elektronik and Komputer (FTKEK), Universiti Teknikal Malaysia Melaka (UTeM), Durian Tunggal, Melaka 76100, Malaysia
[2]Department of General Education, Faculty of Resilience, Rabdan Academy, Abu Dhabi, United Arab Emirates
[3]Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM), Durian Tunggal, Melaka 76100, Malaysia
[4]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Durian Tunggal, Melaka 76100, Malaysia
[5]Industrial Engineering Department, Faculty of Engineering, Bina Nusantara University, Jakarta 11480, Indonesia

Corresponding author: Jamil Abedalrahim Jamil Alsayaydeh (jamil@utem.edu.my)

ABSTRACT In applications related to smart cities, the Internet of Things (IoT) promotes service scalability regardless of variations in user density. Many customers require several safety procedures to supply reliable and effective application services. Undependable user identity was the cause of the current case of Permanent Denial of Service (PDoS). The article discusses service-dependent application authentication (SRAA), a defense against PDoS attacks, in the context of smart cities. This authentication method uses the controlled access distribution mechanism to provide application security. The user application's link connectivity and synchronization capabilities with the user device are used in the monitored access distribution. Backpropagation (BP) learning is used to find errors in the user device, implementation, and verification connections. BP learning minimizes the given weights using the anomaly learned from the initial access distribution phase. The anomaly has been identified in order of earlier training eras to enable coordinated authorization for the distributed services. PDoS causes fewer weights to become disconnected from the service, diminishing the number of service failures for linked devices. The experimental findings have been implemented, and the suggested SRAA model lowers computation overhead by 18.14% and false rate by 10.96%, access success by 9.07%, authenticating duration by 15.38% and synchronization failure by 8.94% compared to other existing models.

INDEX TERMS Access distribution, BP learning, IoT, service authentication, smart city.

I. INTRODUCTION

Smart cities with specific characteristics for real-time decision-making benefit from a real-time data stream that powers their services in day-to-day operations [1], [2]. Some attributes of intelligent services include being customer-centric, information-driven, productivity-focused, and real-time. Urban and city services applications' usefulness in examining IoT-enabled smart cities [3], [4]. To connect the best services and applications with the existing systems, urban smart city systems require a System of Systems (SoS). The application domains for which smart city services systems are designed include recovery from catastrophes, agriculture, transportation, medical care and others [5]. Some characteristics of smart city service systems made possible by IoT include modularity, innovation, value co-creation, heterogeneity, productivity focus, and technology intensiveness. The lifecycle of smart city service systems covers deployment ability, disability, operability, etc. Infrastructure at the time, middleware, software, and application layers are the three

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

layers that make up smart city services [6], [7]. One of the difficult problems in IoT is service management. Devices are accessed by devices in smart city applications to transmit data and initiate certain actions; authentication provides security for interactions between sensors and actuators [8], [9], [10]. One of the traditional requirements for IoT-based smart cities is access control. The type of device does not affect access control with multifunctional features [11], [12], [13]. Four attributes of service access control are application-scoped, delegated, flexible, and client-independent. One typical structure for access control is an access control list (ACL) [14]. Service access control has four characteristics: flexibility, delegated, application-scoped, and client-independent. An access control list (ACL) is a common structure for access control [14]. Role-based access control reduces the workload on the access control list. The advantages of access control involve, among other things, monitoring the method of authentication and having fewer security issues. Access control criteria must be strictly enforced and fine-graded for sensitive IoT data. Versatility in data access control provides adaptive policy enforcement [15], [16]. The service requirement of an IoT smart network is based on the type of application and security for the application based on integrity, confidentiality, and authentication. For a long time, smart cities have used fingerprint-based identification and authentication techniques [17]. Observing some characteristics can distinguish devices by the fingerprint process in cyber security [18]. The cross-layer transmission features implement device authentication in fingerprint-based authentication for IoT devices. An efficient authentication protocol is necessary for securing smart city IoT services for various users with demands on different Internet of Things services [19]. To secure user information in service, authentication is supported by service-oriented authentication. The enhanced authentication profile secures the mobile network by achieving authentication between the network and the user. Various authentication protocols are used for key arrangement and authentication between the users and the IoT network. Authentication factors, procedures, architectures, and token use are authentication techniques for IoT authentication schemes [20], [21].

The main contribution of the paper is

- Designing the service-dependent application authentication (SRAA) for predicting defense against PDoS attacks, in the context of smart cities.
- Using an authentication method for the controlled access distribution mechanism to provide application security.
- The experimental outcomes have been performed, and the suggested SRAA model reduces the computation overhead, false rate, access success, authenticating duration and synchronization failure.

The remainder of this paper shall be arranged in the following manner: Section II will introduce the related research. Section III describes the proposed service-reliant application authentication. The weight assignment process is motivated and described in Section IV, followed by the learning process in Section V, and the backpropagation process is explained in Section VI. Section VII presents the related analysis and discussion. Finally, conclusions and future research directions are presented in Section VIII.

II. RELATED WORKS

Internet of Things attribute-based access control system was proposed by Ding et al. [22] using a blockchain. Blockchain technology prevents data manipulation and single-point failure [23]. The access control procedure amplifies the necessity for great efficiency and minimal processing [24]. The suggested work demonstrates that security and performance analyses withstand various analyses and are used in Internet of Things systems [25]. Dammak et al. [26] looked at DLGKM-AC or decentralized lightest group management of keys to control changing access controls. Subscriber group management reduces the rekeying overhead at the key distribution centre and many subkeys [27]. Data transfer with processing charges is maintained within a limit throughout joint activities. Secure group communication is protected from collusion attacks by DLGKM-AC. The proposed strategy avoids overheads connected to storage, processing, and communication.

Chen et al. [28] developed HAC, or high-efficient access control for information-centric IoT. The network caching process and receiver-driven framework of ICN improve distribution capacity. A mechanism that verifies instructions based on attributes makes IoT edge and resource-constrained applications more effective. The recommended strategy has been evaluated using real-world experiments and theoretical security assessment [29]. The suggested work is more secure and effective when weighed against the latest algorithm. For 5-G-based IoT, Behrad et al. [30] recommended a new scalable authentication and access control mechanism. Flexibility and modularity increase in the 5G network by decreasing the provider's load that connects the CN through an authentication mechanism and access control of IoT devices. Open-air interface (OAI) provides the feasibility of the system. The evaluation is compared with the present AAC technique, allowing the cellular networks to control security.

Chen et al. [31] implemented channel reserved medium access control (ChRMAC) for edge computing-based IoT. The proposed protocol reduces the latency of response and collision in edge computing. The efficacy is improved in ChRMAC by the latency constraint-aware scheme and collision control. A cross-layer framework is employed for the smooth functions of ChRMAC. NS-3 is used to evaluate the proposed scheme, and the performance is increased.

Belguith et al. [32] devised an attribute-based encryption that supports updating access policies and can be verified to preserve privacy for IoT applications with cloud assistance. The suggested method lowers user-side computational overhead. The suggested method reduces the de-encryption overhead and verifies the accuracy of the data arriving from the edge server. An extensive theoretical and experimental

investigation is undertaken, the results are compared with competing schemes, and the study's functionality, computation overhead, and communication are all demonstrated. Cicconetti et al. [33] In MEC systems for IoT, serverless computing access is shown as uncoordinated. The proposed work creates an opportunity for the heterogeneity network and load condition. Propose work is used to achieve a smaller delay in edge node allocation. An in-network and device components fraction is required, and network resources are effectively used and obtained due to the proposed technique. Wang et al. [34] designed the narrowband Internet of Things (NB-IoT) to be made more effective by using the proposed protocol. The performance of the MSG3 (initial layer three messages) and MSG1 is examined using stochastic geometry. Because of the enhanced likelihood of NB-NORA (NB-IoT orthogonal random access), the throughput of MSG1 is maximized. Reference [35] proposes a decentralized, lightweight blockchain-based authentication solution for IoT devices. The proposed mechanism is constructed using public blockchain theory and fog computing technologies. The proposed solution outperforms the most recent state-of-the-art blockchain-based authentication methodology. The suggested mechanism can be modified to accommodate complex situations. Location-aware wireless security access control (LaSa) is suggested by Lu et al. [36] for IoT systems. By finding and accepting unique signal patterns, the LaSa detects the entry and exit of users. By conducting experiments in the real world, the proposed scheme will increase the accuracy of identifying the unauthorized user by decreasing the false blocking rate.

For a risk-based access control approach, Atlam and Wills [37] established an efficient method for estimating security risks for the Internet of Things. The proposed work aims to assess the security risk posed by access control operations in IoT systems. Security professionals certify both the fuzzy method and the proposed method. The proposed technique is put into practice using router access control scenarios. Comparing the recommended method to existing ones, it works effectively and is reliable. In [38], Fuzzy logic with expert judgment is designed for access control with the knowledge of the security risks. Analysis of the sensitivity, user risk, action severity, and access request results in the access decision. Smart contracts are employed to identify harmful activity to stop security violations during the access portion. Fuzzy inference systems handle the risk estimation process, and the standard risk estimation technique is presented.

A blockchain-based framework was utilized by Makhdoom et al. [39] to secure and protect data in smart cities. The embedded access control rules in smart contracts regulate user data access within the channel. Privacy data encryption and collection are employed to secure and isolate the data. Privy coins facilitate data sharing between users and stakeholders. In [40], a software-defined networking-based context-aware privacy-preserving technique is created for an Internet of Things-based smart city. The simulation approach uses MININET-WIFI, and the suggested work's efficacy is assessed. The flow of data packets is managed by an efficient privacy-preserving method. In smart city applications, the proposed is applicable, and the performance based on the accuracy, penetration rate and overhead is compared with existing privacy techniques002E.

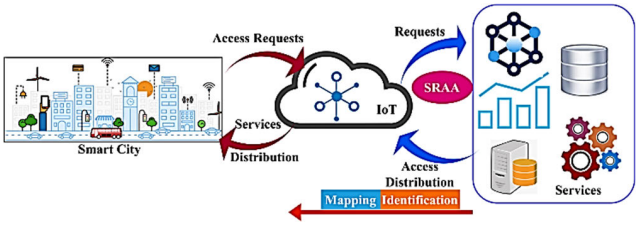

FIGURE 1. SRAA for IoT-based Smart Cities.

To ensure the safety and privacy of smart city users and systems, Awotunde et al. [41] proposed a hybrid Convolutional Neural Network (CNN) with Kernel Principal Component Analysis (KPCA) that is powered by blockchain technology. The findings of the experimental assessment demonstrate that smart cities enabled by the Internet of Things perform better in terms of the accuracy of danger predictions, leading to enhanced privacy, security, and maintainability.

Based on the survey, there are several issues with existing works in attaining reduced computation overhead, false rate, access success, authenticating duration and synchronization failure. The article discusses service-dependent application authentication (SRAA), a defense against PDoS attacks, in the context of smart cities.

III. PROPOSED SERVICE-RELIANT APPLICATION AUTHENTICATION (SRAA)

The services secure the many IoT services in an intelligent city distributed to the applications. By using the SRAA approach, which deploys the user device's synchronization, the PDoS issue is here overcome. This paper aims to reduce false rate, synchronization failure, and delay while enhancing dependable access authentication. The SRAA approach was developed to solve these issues and provide security for the network. The SRAA is shown in an IoT-based smart city setting in Fig. 1.

The load on the access control list is lessened. Compared to traditional identity-based access control (IBAC), RBAC performs better. Access control capabilities include, among other things, the ability to govern the authentication process and have fewer security risks. Access control criteria must be strictly enforced and fine-graded for sensitive IoT data. Having flexible data access control enables adaptive policy enforcement. Implementing this allows for quick communication between all end users. The first stage identifies whether a user's device is linked to the application and the service. The anomaly resulting in a disconnect between the three frameworks is designated PDoS. Three frameworks are chosen to address this issue, and the following equation is

used to evaluate how well they are interconnected.

$$\alpha = \left(\frac{\sum_h' l_0}{d_i + n_a + e'}\right) * \prod_{\tau} \left(x_c + \frac{w'}{s_j}\right) - t_m + \left({}^{x_c}/_{e_n}\right) * c_e \tag{1}$$

The device, application, and service connectivity are deployed by equating the equation above (1), and the result is denoted as τ. The connectivity for the various services is periodically verified, and it will be shown as e′, and the number of services is termed as e_n. An identifying process is represented in the form of α, and the recognizing event is denoted in the form of l_0, that is employed to find the PDoS also deploys the abnormal activities termed as b'. The equipment is depicted as d_i The demand application is referred to as n_a as well as the communication of the form x_c, that provides the end-to-end user w'. The connection is made for the device's application; evaluation and establishment of a connection are carried out on time and provide authentication. In a smart city, the estimated interconnection between the app and its services verifies the user's multiple services. In this instance, the communication is deployed, and the service is distributed to the consumer, and it is identified as $\left(x_c + \frac{w'}{s_j}\right)$ The distribution form can be shown as s_j. The time duration is given as t_m, the connection request in the form of c_e, h' as a permission access variable provided in response to a consumer application. From start to finish, the communication among individuals in the IoT is assessed using equation (2).

$$v_x(x_c) = \begin{cases} \left(\frac{\sum(\tau+\alpha)}{d_i}\right) + n_a * e' \left(\delta + w'\right) \\ \qquad -p_v, \in \textit{Connected} \\ \prod_{e'} \delta + \left(l_0 - \frac{e'}{\alpha}\right) * n_a + d_i \\ \qquad -w', \in \textit{Disconnected} \end{cases} \tag{2}$$

End-to-end users communicate with each other to deploy authentication for the various services the smart city offers. The connection derived in the first derivation is assessed, and the communication is examined using this prior state. The end-user's disconnection from the service is linked to the second derivation. Here, the examination is carried out, and it is denoted as $\boldsymbol{v_x}$ And establishes the communication link. The previous state is termed as $\boldsymbol{p_v}$ that matches the established communication before processing and deploying the pursuing state. When a problem arises in communication, it is mapped to the prior state for detection, and the authentication is examined to identify the disconnect. The disconnect results from a mismatch between the service and the processing history in smart city applications. The authentication is denoted as $\boldsymbol{\delta}$, which deploys the identification process and disconnects the service if it does not match the history of the service. As a result, the end-to-end user connected to the IoT authentication procedure can communicate. The distribution of access to the user is accomplished by establishing communication and is done so using the equation below.

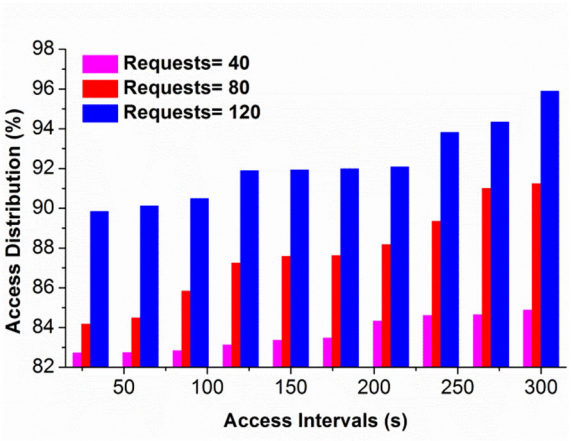

FIGURE 2. Access distribution %.

$$s_j = \left(\frac{d_i * x_c}{\prod_{l_0} v_x}\right) + t_m * \left[(n_a + d_i) + \left(\frac{h'}{{}^{e'}/_{q_0}}\right)\right] + (l_0 - \tau) * (x_c + p_v) - w'\,(t_m) \tag{3}$$

The user demands the services that deploy user devices, applications, and services sent out to the user's gadgets in the Internet of Things framework. The service is provided to the user by formulating. $\left(\frac{h'}{{}^{e'}/_{q_0}}\right)$, the pursuing is denoted as q_0 and balance the authentication. When communication between end users begins, this distribution stage gets evaluated based on the quantity of services the user requests. As communication grows, it becomes possible to identify when services are connected and disconnected and when they start functioning, maintaining the security level. In this distribution phase, access is provided to the authenticated user in the smart city, and the communication is established reliably. Here, the end-user provides the security that improves the performance by formulating $(l_0 - \tau) * (x_c + p_v)$. The distribution of access is done for the varying services and devices in this method. If the communication is connected, then the distribution is followed. The authentication is maintained in the smart city by processing this, and the interconnection is examined periodically. The weight is assigned to the services that deploy the linked devices. In Fig. 2, the access distribution and in Fig. 3, the mitigation % for different access intervals is illustrated. IoT device makers should consider authentication and identification before releasing devices to the public. One must have a means of authenticating the identities of devices and individuals involved in communications to prevent man-in-the-middle attacks, which include passing on false information while mimicking another device or a person. Regarding the Internet of Things (IoT), identity spoofing attacks are simple to implement. If an identity spoofing attacker knows the real user's media access control

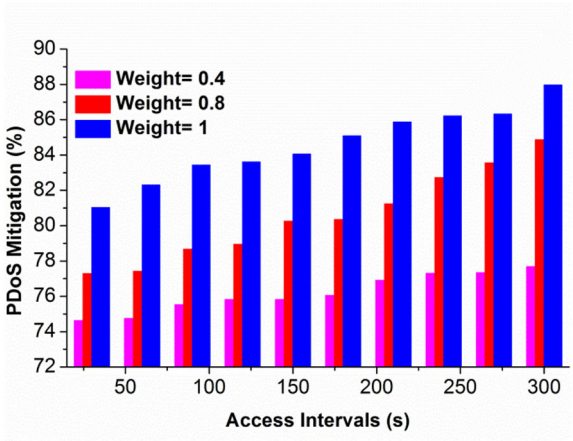

FIGURE 3. PDoS mitigation %.

(MAC) or internet protocol (IP) address, they may pose as another real IoT device.

The access interval varies for access distribution percentage that deploys the user request for different services. According to this request's access distribution, the value varies from low to high. The access distribution drops when the request decreases and reverses, with the access interval indicating a higher range, as depicted in Fig. 2. According to Fig. 3, the access interval for the different PDoS reduction percentages extends from low to high. The weights are computed when the access interval widens, and the PDoS identification is reliably made. Compared to weight 0.4, the PDoS mitigation decreases, whereas, for one, it shows a higher value, and the access interval also increases.

IV. WEIGHT ASSIGNMENT PROCESS

The initial configuration of a machine learning model is determined by the weight assignment stage, making it a vital step in the process. Several practitioners use random weight initialization to combat the inherent symmetry of neural networks. Without properly initializing weights, the model cannot generalize to new patterns in the input, as all neurons would learn the same characteristics throughout training. Increasing the likelihood that the model will develop a more robust data representation, this study include variety by allocating weights at random. The various services are given relative weight, and end-to-end user communication is established. At first, the services are given a higher weight. By carrying out this assigning phase, the authentication is strengthened, and the weight varies, indicating the lower range if the abnormal increases. This evaluation addresses the PDoS and grants access to the verified user. The weight assignment is derived using the following equation.

$$a_0 = \left(\frac{1}{e_n}\right) * \left(\frac{v_x}{l_0/p_v}\right) + \sum_{s_j} \left(h' + x_c\right) * \left(c_e + k_b\right) * \left(\frac{g_i + w'}{\prod_{v_x} e'}\right) \quad (4)$$

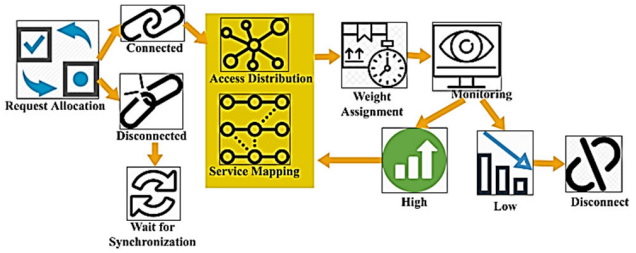

FIGURE 4. Abnormal service identification process.

Weights are assigned to the services that allow communication between the end users. Here, the weights are denoted as g_i and assigning is termed as a_0In this process, communication is established for the varying users. The weighting method differs for IoT devices and tackles the delay by choosing the connection. Examining the connection between the devices here protects users' capacity to communicate. The access distributed to the service that deploys by equating $\sum_{s_j} \left(h' + x_c\right) * \left(c_e + k_b\right)$, here the linkage of service is evaluated, and it is denoted as k_b. The distribution of access to the requested user is used to deploy the communication between users. Here, the weights are assigned in the initial stage and provide access to the number of services. This interconnection of three frameworks is used to evaluate the weight, and it is represented as $\left(\frac{g_i + w'}{\prod_{v_x} e'}\right)$. The following calculation can be used to find the odd IoT services by mapping onto the previous state.

$$\alpha\left(b'\right) = \left(\frac{s_j}{\sum_{c_e} \tau}\right) * \sum_{q_0}^{p_v} \left(\alpha + k_b\right) + \left[\left(\frac{e'/a_0}{g_i}\right) * \left(\frac{x_c}{v_x/l_0}\right)\right] + c_e\left(e_n\right) - t_m \quad (5)$$

The abnormal detection is performed by evaluating the above equation associated with access to different services. In this identification process, the services are linked with the weights assigned and formulated as $\left(\frac{s_j}{\sum_{c_e} \tau}\right)$. Here, the access is distributed to the number of services; assigning is evaluated to the authenticated user. The service, connected to detecting both usual and unusual services, is made available to the authenticated user. In Fig. 4, the abnormal service identification process is illustrated.

The abnormal detection is evaluated in a reliable manner that deploys the assigning weights to the devices represented as $\left[\left(\frac{e'/a_0}{g_i}\right) * \left(\frac{x_c}{v_x/l_0}\right)\right]$. The access is distributed to the authenticated user by providing security to the number of services, and the connection is established to perform better communication. This abnormality is identified by equating the above equation, addressing it initially, and reliably providing security. The following section performs the backpropagation; weights are assigned to ensure security.

V. LEARNING PROCESS

As a part of the learning process, the model's weights are adjusted according to the discrepancy between the expected and actual results. Optimization methods, such as gradient descent, are often used. The main rationale for learning is the model's capacity to evolve and improve with time. The model converges on a solution that captures the underlying patterns in the training data by repeatedly modifying the weights to minimize the error. This step is critical for the model's generalizability to new data since it is based on mathematical optimization concepts. The neural network that passes the requested service to the other neuron layers and examines the normal and abnormal services is defined as the chain rule. Here, the forward pass is derived by assigning the weights to the number of neuron layers that deploy the access distribution. If the abnormality increases, the weights decrease, whereas the authentication decreases. This BP examines communication for the varying services and promptly provides results. To determine the training weight for various services and enhance authentication, apply the equation below.

$$v_x = \prod_{k_b} (s_j + e') * \left(\frac{l_0/\tau}{\alpha} \right) + \left(\delta * h'/f_w \right) * \left(\frac{s_j (h')}{\sum_{a_0} g_i} \right) + \sum_{c_e} x_c * \alpha (b') \quad (6)$$

In the above equation, the examination of services is carried out to deploy security for the number of services and evaluate communication. The examination is evaluated to provide the authentication for the services; here, the training. t_r of service is carried out by evaluating the BP. The input neuron acquires the services, reliably provides the communication, and forwards to the second neuron. The abnormal detection associated with the assigned weight is evaluated by performing this. The weights are assigned to the services that deploy the varying applications in the smart city and identify the abnormal services. The BP effectively instructs the service by comparing the current service state with a previous one.

In the IoT environment, the related service is examined, and the end-to-end user communication has been looked at; it states the current state of the neuron, and it is denoted as $\left(\delta * h'/f_w \right)$. The forwarding pass is represented as f_w and provides authentication for the services and examines the communication. The forward pass is carried out by determining the interconnection between the smart city devices and reliably provides security. BP is used to evaluate the training set of services by forwarding the services to the next stage of the neuron state. The following equation calculates the forward pass that deploys the neuron's state in BP.

$$f_w = \left(\frac{a_0 (g_i)}{\sum_{t_r} (n_a + e' + d_i)} \right) * \prod_{s_j}^{h'} \left(l_0 + \frac{q_0}{p_v} \right) + (\alpha * \delta) * \left(\frac{p_v/t_r}{w'} \right) \quad (7)$$

The forward pass is determined in BP associated with the varying service in the smart city that deploys the state of the neuron by assigning the weight. In this processing, the weight is assigned to the number of services, and it is represented as $\left(\frac{a_0(g_i)}{\sum_{t_r} (n_a + e' + d_i)} \right)$ Here, the interconnection of the three frameworks is examined. Here, the previous state of service is evaluated by equating. $\left(l_0 + \frac{q_0}{p_v} \right) + (\alpha * \delta)$ in this, authentication is maintained for every step of processing.

The forward pass in BP determines the abnormal services, distributes device access, and ensures security. This forwarding of services is determined by computing the above equation associated with the access distribution to the services. The previous state of mapping is done to ensure security reliably, and the following equation is used to evaluate gradient descent in BP. The parameter is used to evaluate the error function for the three frameworks.

$$\rho = \prod_{\tau} (a_0 * g_i) + \left(e' + \frac{s_j + x_c}{h'} \right) * \left(b' * d_e/n' + f_w \right) + \sum_{\delta} (l_0 * w') - t_m \quad (8)$$

The device's interconnection, application, and service are deployed while BP's weight is updated using machine learning's gradient descent technique. Here, the services are given relative importance, and access is swiftly granted to the verified user, improving security. The gradient descent is represented as ρ, and determines if the service is normal; the forward pass is carried out else the connection is denied, and it is denoted as $\left(b' * d_e/n' + f_w \right)$. This authentication is performed to recognize the PDoS attackers in the smart city and reliably provides security. Gradient descent is used to grant access to the user, and the communication between end users related to authentication is examined.

Here, the access distribution is used to monitor the past state of the service while also evaluating the BP synchronization mechanism. The identification step of PDoS attackers is evaluated in this work using SRAA, and access to the services is granted. For all IoT processing types, weights are assigned, gradient descent is performed, and the odd service is discovered and deactivated. User device, app, and service synchronization has been noted, disconnected, and is now being investigated. The authentication is sent by reviewing the BP strategy connected to the security process.

The service identification and calculation of time in different eras are shown in Figs. 5 and 6.

In the context of the Net of Everything, multiple eras are used to identify normal and abnormal services. It displays the service in normal and abnormal circumstances, with values ranging from low to high. By identifying the attackers, the normal service displays a greater range than abnormal services if the epochs increase, as shown in Fig. 5. The epochs are estimated for the varying computation overheads that

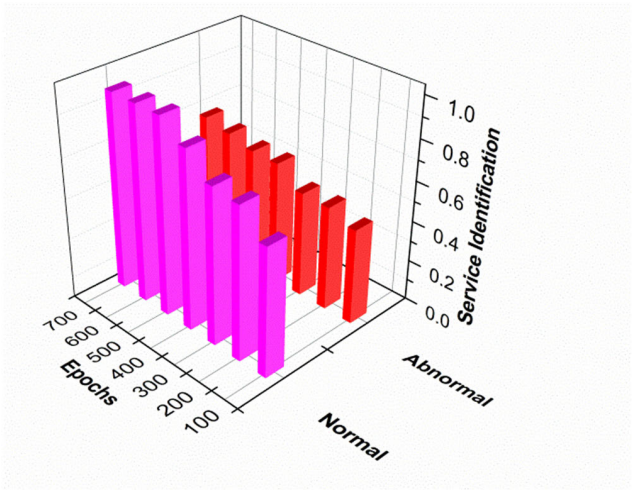

FIGURE 5. Service identification.

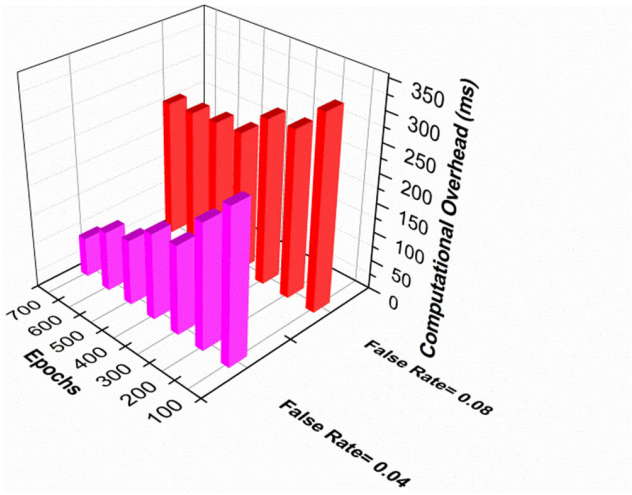

FIGURE 6. Computational overhead.

deploy promptly. It shows a high to low range, as shown in Fig. 6. The epochs are evaluated for the false rate in the proposed work, which shows 0.0.4-0.08. Compared to 0.04, 0.08 shows a higher false rate in this proposed work, and the epochs are estimated for the services.

VI. BACKPROPAGATION PROCESS

One of the most important parts of learning is backpropagation, which helps the model to alter its weights effectively. To use this method, one must first determine the error's gradient relative to the model's weights and then change the weights so that the gradient is negative. Backpropagation is mainly based on the fact that it updates weights across the network efficiently and effectively. Each weight contributes to the aggregate error as the mistake propagates backwards through the network, allowing for a more focused and accurate modification. This method updates weights systematically and computationally efficiently by using the chain rule of calculus. The SRAA technique, which distributes access to the numerous facilities the smart city provides, is used in the current work to evaluate BP. This BP performs the initial pass, and based on the security, an accurate analysis of the regular and irregular services is provided. In this case, we may examine the gradient descent by analyzing the forward movement connected to the weight distribution. The equation below looks at errors in amenities within the smart city.

$$j' = \left(\frac{b'(\alpha) + x_s}{\prod_{s_j} e'}\right) * \left(\frac{k_b + e'}{p_v}\right) + \sum_{n_a}^{d_i} \alpha(\tau) * (a_0 + \delta) * \left(\frac{v_x + t_m}{\rho / f_w}\right) + g_i\,(a_0) \tag{9}$$

The error function improves the security of the interconnected framework associated with finding abnormal services. The above equation examines the application and user devices and deploys reliable communication between end-users by promptly delivering accurate services. This examination is periodically associated with BP's training service and derives efficient communication.

If an abnormal service that improves authentication is found, the weight is updated using the gradient descent method. The function utilized to identify error is represented using j'. After the authentication is completed for the linked devices, giving the user access, it is depicted as $\alpha(\tau) * (a_0 + \delta)$. It serves to compare the security and services in the prior condition and is designated to be $\left(\frac{v_x + t_m}{\rho / f_w}\right)$ that relates to time. The security of the authenticated user is ensured by the hidden layers, which check the connected devices according to their weighting factor. The following formula evaluates the layers concealed in this BP approach.

$$\left.\begin{aligned} s_j\,(e_0) &= \alpha\left(d_i(0) + \left(\tfrac{t_r}{s_j * h'}\right) * \beta_0\right. \\ s_j\,(e_1) &= s_j\,(e_0) + \alpha\left(d_i(1) + \left(\tfrac{t_r}{s_j * h'}\right) * \beta_1\right. \\ &\vdots \\ s_j\,(e_n) &= s_j\,(e_1) + \alpha\left(d_i(n) + \left(\tfrac{t_r}{s_j * h'}\right) * \beta_{n-1}\right. \end{aligned}\right\} \tag{10}$$

$$\begin{aligned} a_0\,(g_i)\,e_0 &= v_x\,(x_s) * \left(l_0 / q_0\right) + d_i\,(0) * \beta_0 \\ a_0\,(g_i)\,e_0 &= v_x\,(x_s) * (l_0/q_0) + d_i(0) * \beta_0 \\ a_0\,(g_i)\,e_1 &= v_x\,(x_s) * (l_0/q_0) + d_i(0) * \beta_0 \\ &\quad + v_x\,(x_s) * (l_0/q_0) + d_i(1) * \beta_1 \\ &\vdots \\ a_0\,(g_i)\,e_n &= v\_x\,(x\_s) * (l_0/q_0) + d_i(0) * \beta_0 \\ &\quad + v_x\,(x_s) * (l_0/q_0) + d_i(1) * \beta_1 \\ &\quad + v_x\,(x_s) * (l_0/q_0) + d_i(n) * \beta_{n-1} \end{aligned} \tag{11}$$

In equations (10) and (11), the hidden layers deploy the BP that transmits the products or services to the final consumer.

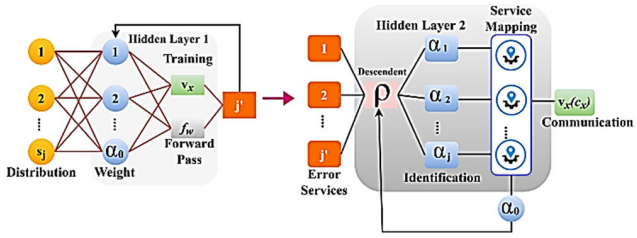

FIGURE 7. Backpropagation learning representation.

Training is done by assessing the weight assignment, including gradient descent, to update the performances. In this state, the distribution process is carried out and detects the error by evaluating machine learning. The term β is used to represent hidden layers, associated with its count is termed as β_n. This is associated with the ways services are distributed and given respective weights. In varying services and applications, the weights are assigned and ensure the safety and reliability of the authenticated individual. Fig. 7 illustrates the backpropagation learning.

The input is taken in by the primary layer of neurons, which also recognizes aberrant functions and prepares them for further processing. In a different scenario, the input is obtained in the neuron's initial state and then passed to the second layer, where the services are trained using the hidden layers. The service is defined using the error function, and BP is carried out for the various services, deploying the authentication. This approach uses the hidden layers to assess the services and guarantee IoT security. The next formula distinguishes between regular and irregular services, thereby mitigating the impact of PDoS attacks.

$$i' = d_i\left(\beta_n\right) * \left(\frac{e_n + h' + s_j}{\sum_{g_i} a_0}\right) + j' * b'\left(\alpha\right) - \left(p_v + f_w\right) * w' \tag{12}$$

The PDoS mitigation i' is carried out in equation 12; in this case, the aberrant services are addressed using erroneous mechanisms. In this case, the expressed services determine the distribution of access. $\left(\frac{e_n+h'+s_j}{\sum_{g_i} a_0}\right)$. BP's forward pass is evaluated as part of the identification process, and abnormal services are disconnected. By providing consumers with access, it improves authentication by reducing weight. In this case, the prior condition is employed for identifying the aberrant and error function procedure, and the BP method uses weight training for this purpose. The synchronization is examined, and mitigation is carried out in the SRAA if an abnormal service is found. As shown in the equation below, the linked weight is allocated for the different services through mapping using the historical data.

$$k_b\left(e'\right) = \left(\frac{\sum s_j\left(h'\right)}{d_i}\right) + v_x\left(x_c * a_0\left(g_i\right)\right) + \left(\frac{f_w * \rho}{\beta\left(n\right)}\right) + i' - b' - p_v \tag{13}$$

TABLE 1. Synchronisation factor of service error and mitigation in percentage.

Synchronization Factor	Service Error (%)	Mitigation (%)
0.6	21.1	73.75
0.7	9.94	81.92
0.8	8.89	85.21
0.9	8.99	87.53
1	5.2	87.97

The numerous linked amenities in a smart city are given different weights associated with the allocation of entry in this proposed work. Here, the gradient descent is used for these weight-related services and performs the allocation according to typical and abnormal activities. Periodically reviewing the exchange of information and responsibility assignment helps to mitigate the aberrant service, which is indicated as $\left(\frac{e_n+h'+s_j}{\sum_{g_i} a_0}\right)$. The history of analysis is carried out that is associated with the varying devices, applications, and IoT application services. In the above equation, the linked services are evaluated by assigning the weights to the services. Three frameworks are examined for synchronization using the following equation, and authentication ensures security.

$$v_x\left(z_r\right) = \left(d_i + e' + n_a\right) + n' * \left(x_c + w'\right) + f_w * \left(\frac{l_0}{\prod_{s_j} h'}\right) * \left(p_v - t_m\right) \tag{14}$$

The synchronization is tracked in the equation above and is denoted as z_r The user gadgets, the application, and the service connection have been set up here. Through analysis, this results in the standard service being forwarded to the neuron state, where PDoS attackers are detected and connected to smart city services that are portrayed accordingly $f\_w * \left(\frac{l_0}{\prod_{s_j} h'}\right)$. The dependable user receives access, and weight fluctuations in the program determine the unusual condition. In the first phase, PDoS attackers are dealt with, and the end users involved in the synchronization can communicate. Table 1 shows the service error and mitigation percentage for various synchronization factors.

The mistake identification and reduction process involves examining the synchronization for various service percentages. In this case, the error function is calculated, and the range of values for both the error rate and mitigation is modest to high. Improved synchronization is shown in Table 1 by the process whereby a rise in error also increases mitigation. The IoT is periodically inspected to ensure synchronization for all users, and this operation reduces the delay factor. Implementing the forward pass in BP simplifies authentication and separates normal and odd services. The security level is successfully and immediately raised when an authenticated user provides a service. The SRAA technique is applied to

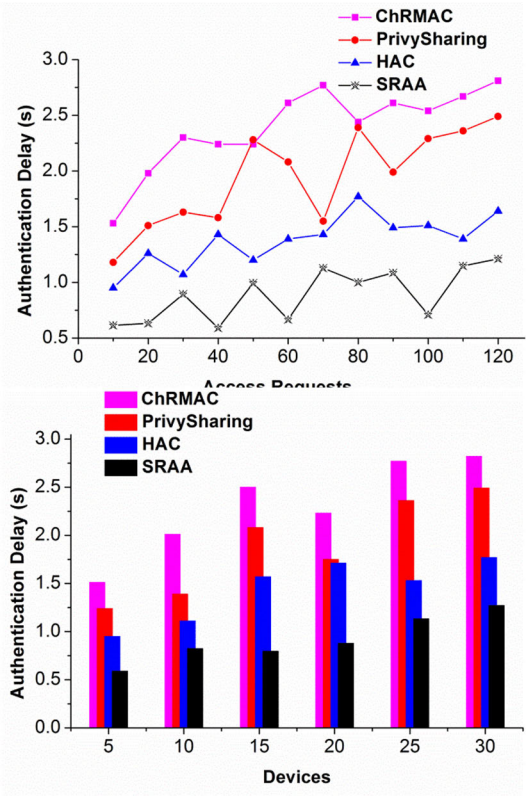

FIGURE 8. Device and access request authentication delay.

quickly grant access to the end user, analyze the BP, and draw an accurate assessment.

VII. DISCUSSION

The results of the suggested SRAA implementation are shown in this section. The modelling retrieves services from the IoT platform using thirty IoT devices. The 2TB capacity of the cloud service provider is used to respond to access requests. There are 120 device requests during each access interval, ranging from 30 to 300 seconds. An encrypted socket-layer certificate is used in this process to guarantee authentication throughout the access interval. The performance metrics include access success rate, computation overhead, synchronization failure, false rate, and authentication delay. The suggested SRAA for the metrics above is used in conjunction with the current ChRMAC [20], PrivySharing [28], CNN-KPCA [41] and HAC [18] techniques for comparative analysis.

A. AUTHENTICATION DELAY

The authentication delay for the proposed work decreases by varying access requests and the number of devices. Here, it deploys the interconnection of user devices, authentication, and service, and it is computed as $t_m + \left({}^{x_c}/_{e_n}\right) * c_e$. This process estimates the time to analyze the PDoS attackers in the network. The abnormal services are detected, and security is ensured by evaluating the communication between the final

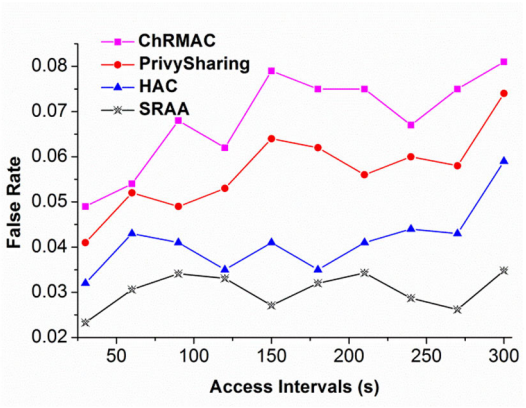

FIGURE 9. False rate for access intervals.

consumers. This training service aims to lower the erroneous functions that the BP technique revealed. The user is given weights, which are then used to analyze the synchronization of services used to assess gradient descent. Here, the weight for the various services in the IoT environment is updated using gradient descent. The requested application in the smart city receives the authentication, providing an estimated processing time. In this evaluation, the interconnection among the three frameworks is used to detect the abnormal service defined as $(n_a + d_i) + \left(\frac{h'}{{}^{e'}/_{q_0}}\right)$. The allocation of access to the user includes an examination of the mapping using the connection's first processing state. When end-to-end user connectivity is established, unusual services are found, and no authentication is required. This effectively addresses and reduces the authentication delay, as shown in Fig. 8.

B. FALSE RATE

The false rate for varying access intervals decreases by evaluating the BP method that assigns the weights to the varying services. The mapping is done with the previous state and detects the PDoS attack. This authentication is verified for every step of computation utilizing the training services. Here, the assigning of weight varies for the service, and it is represented as $(c_e + k_b) * \left(\frac{g_i + w'}{\prod_{v_x} e'}\right)$. The distribution of access is performed by evaluating the interconnection of three frameworks. BP is used to deploy the synchronization of devices, applications, and services reliably; the interconnection of services is deployed via gradient descent, and when an aberrant service is found, it is denoted as $\sum_{q_0}^{p_v} (\alpha + k_b)$. The identification is carried out for the varying services and analysis of the linked services in the IoT. In this processing, the access is distributed to the authenticated services, and service synchronization is examined. The abnormal services are identified and provide efficient authentication to the user request. The connection and disconnection are derived from establishing communication with end-to-end users. The false rate for the proposed work decreased and promptly provided the authenticated user's security, as offered in Fig. 9.

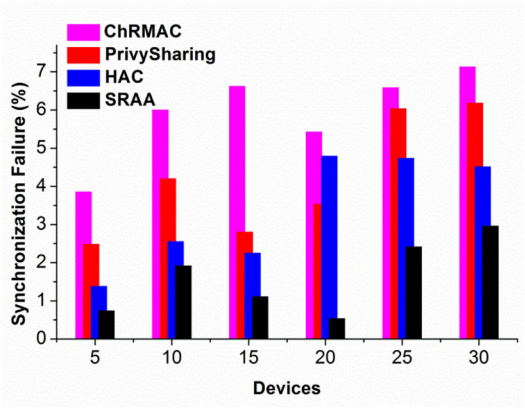

FIGURE 10. Synchronization failure for devices.

C. SYNCHRONIZATION FAILURE

In Fig. 10, the synchronization failure decreases for varying devices and examines the connection among the application, services, and user device, and this connection is computed as $\left(\delta * h'/_{f_w}\right)$. If the communication with the authentic consumers in the assessment is established, distribution has been carried out. The distribution tackles the PDoS attack in the network and is assessed for the authenticated user. The BP method is thus used to sort out the synchronization failures and reliably deploy the access distribution. In this case, the recognition is used to find the connections between the three frameworks and detect the abnormal services. The assessment is formulated to tackle the relative importance bestowed upon the services within the smart city. In this case, the various services that analyze the linked services are improved using the hidden layers. The assigned weight for the user authentication services is updated using gradient descent. The BP is introduced as part of this training. The assigned weights are adjusted if the authentication is altered. As a result, the access is

D. COMPUTATION OVERHEAD

Due to fluctuating access requests and intervals, the authentication process is completed promptly and with minimal computational overhead. Here, the calculation is analyzed regularly using an equation. $(\alpha * \delta) * \left(\frac{p_{v/t_r}}{w'}\right)$. The attackers' identities are used to ensure the verified user's security. The device, application, and service interconnections are analyzed in this computation step. In this case, the error function found by the BP method is deployed using the linked services. The error service is located using the hidden layers, and they are promptly trained accordingly. This end-to-end authentication is used with the training service by allocating weights to the various services. In this case, the IoT's abnormal services are mitigated through recognition of service. Communication with end users is established to guarantee security for the various IoT services. The forward pass is employed by mapping the service and the earlier state to move the service to the upcoming neural state. Various services receive

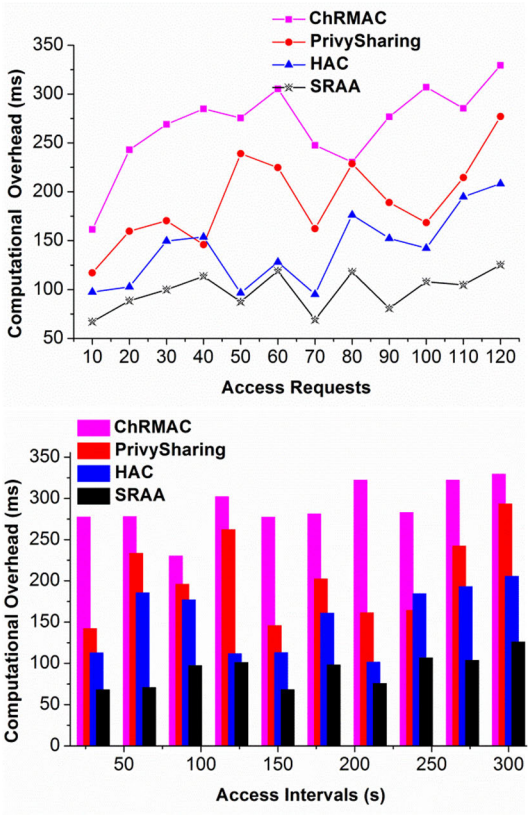

FIGURE 11. Calculation expenses for requests for access and intervals of access.

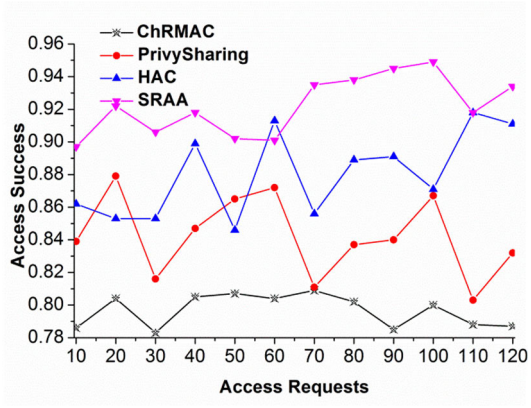

FIGURE 12. Access success for access requests.

varying weights in this method, which takes communication factored in. If reliable communication is established, access distribution happens swiftly. The evaluation generates the authentication, and the calculation overheads are minimized, as shown in Fig. 11.

E. ACCESS SUCCESS

In Fig. 12, when different access requests are made for the devices that use authentication, the success rate of access increases. All three frameworks are synchronized, and the reliability of the interconnection is tested. In this case, security is provided, and normal service is transmitted to the

TABLE 2. Comparison Evaluation of requests for access.

Performance Indicators	Authentication Delay/s	Computation Overhead /ms	Access Success
ChRMAC [20]	2.714	325.4	0.7
PrivySharing [28]	2.38	266.95	0.9
HAC [18]	1.5	190	0.94
SRAA [Proposed]	1.11	104	0.92

Inference: The suggested SRAA increases access success by 9.07% while reducing computation overhead and authentication latency by 15.91% and 20.26%, respectively.

TABLE 3. Comparison of access interval analysis.

Metrics	ChRMAC	PrivySharing	HAC	SRAA
Computation Overhead (ms)	329.30	293.20	205.48	125.822
False Rate	0.081	0.074	0.059	0.0348

Inference: SRAA reduces computation overhead by 18.14% and false rate by 10.96%.

TABLE 4. Device comparative analysis.

Performance Indicators	ChRMAC [20]	PrivySharing [28]	HAC [18]	CNN-KPCA [41]	SRAA [proposed]
Authentication Delay/s	2.72	2.295	2.77	2.87	1.271
Synchronisation Failure (%)	7.13	6.18	4.51	5.76	2.959

Inference: By 15.38% and 8.94%, respectively, SRAA decreases the authenticating duration and synchronization failure.

next neuron state through the forward passed signal. and it is represented as $\left(\frac{f_w * \rho}{\beta(n)}\right) + i' - b' - p_v$. The previous state maps with the pursuing state and gives the result. Thus, the services deployed to synchronize user devices, applications, and services. Here, if the communication is established to the normal services, access is distributed to the user efficiently. This method uses access distribution to deploy the previous state of services and promptly provides security. The error function is addressed and provides the requesting user by equating. $n' * (x_c + w')$. If the authentication is approved for the services, assigning weights is derived to the user, improving synchronization. Here, the abnormal services are detected in the smart city environment and provide authentication to the requested user. In this process, the access success rate is improved and ensures security for the various services.

VIII. CONCLUSION

This article describes a service-based application authentication method that protects against denial of service (PDoS) attacks on IoT-powered apps for smart cities. This method ensures service security by utilizing access control and synchronization verification. The user device, application, and Internet of Things synchronization is verified before access. The changes and anomalies in the synchronization are monitored through BP learning based on decreasing weight factors. By separating service and failed services, a learning process is accomplished. These characteristics define the service's shipment, which is updated often. As a result, the PDoS adversary's deception rate of service response declines. The experimental findings have been implemented, and the suggested SRAA model lowers computation overhead by 18.14% and false rate by 10.96%, access success by 9.07%, authenticating duration by 15.38% and synchronization failure by 8.94% compared to other existing models. It increases access delivery's success rate. However, this study has limitations of scalability issues such as user load and server load balancing. Future BP learning assessments of access control in multi-level application services were anticipated to leverage it. This mainly aims to enhance access control for large-scale applications with simultaneous service answers.

ACKNOWLEDGMENT

The authors express their gratitude to the Centre for Research and Innovation Management (CRIM), Universiti Teknikal Malaysia Melaka (UTeM), for their valuable support in this research.

REFERENCES

[1] H. Yao, P. Gao, J. Wang, P. Zhang, C. Jiang, and Z. Han, "Capsule network assisted IoT traffic classification mechanism for smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7515–7525, Oct. 2019, doi: 10.1109/JIOT.2019.2901348.

[2] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato, "A survey on network methodologies for real-time analytics of massive IoT data and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1457–1477, 3rd Quart., 2017.

[3] M. Tao, K. Ota, and M. Dong, "Locating compromised data sources in IoT-enabled smart cities: A great-alternative-region-based approach," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2579–2587, Jun. 2018, doi: 10.1109/TII.2018.2791941.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[5] D. Bruneo, S. Distefano, M. Giacobbe, A. L. Minnolo, F. Longo, and G. Merlino, "An IoT service ecosystem for smart cities: The #SmartME project," *Internet Things*, vol. 5, pp. 12–33, Mar. 2019.

[6] M. Saadi, M. T. Noor, A. Imran, W. T. Toor, S. Mumtaz, and L. Wuttisittikulkij, "IoT enabled quality of experience measurement for next generation networks in smart cities," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102266.

[7] J.-H. Park, M. M. Salim, J. H. Jo, J. C. S. Sicato, S. Rathore, and J. H. Park, "CIoT-Net: A scalable cognitive IoT based smart city network architecture," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, p. 29, Dec. 2019.

[8] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, "Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city," *IEEE Access*, vol. 7, pp. 54508–54521, 2019, doi: 10.1109/ACCESS.2019.2913438.

[9] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[10] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017.

[11] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018, doi: 10.1109/COMST.2018.2849509.

[12] Q.-V. Pham, F. Fang, V.-N. Ha, M.-J. Piran, M. Le, L.-B. Le, W.-J. Hwang, and Z. Ding, "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art," *IEEE Access*, vol. 8, pp. 116974–117017, 2020, doi: 10.1109/ACCESS.2020.3001277.

[13] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1078–1124, 2nd Quart., 2021, doi: 10.1109/COMST.2021.3062546.

[14] N. Tapas, F. Longo, G. Merlino, and A. Puliafito, "Experimenting with smart contracts for access control and delegation in IoT," *Future Gener. Comput. Syst.*, vol. 111, pp. 324–338, Oct. 2020, doi: 10.1016/j.future.2020.04.020.

[15] M. Amoon, T. Altameem, and A. Altameem, "RRAC: Role based reputed access control method for mitigating malicious impact in intelligent IoT platforms," *Comput. Commun.*, vol. 151, pp. 238–246, Feb. 2020, doi: 10.1016/j.comcom.2020.01.011.

[16] A. Gabillon, R. Gallier, and E. Bruno, "Access controls for IoT networks," *Social Netw. Comput. Sci.*, vol. 1, no. 1, p. 24, Jan. 2020, doi: 10.1007/s42979-019-0022-z.

[17] J.-C. Huang, M.-H. Shu, B.-M. Hsu, and C.-M. Hu, "Service architecture of IoT terminal connection based on blockchain identity authentication system," *Comput. Commun.*, vol. 160, pp. 411–422, Jul. 2020, doi: 10.1016/j.comcom.2020.06.027.

[18] M. Wazid, A. K. Das, V. Bhat K, and A. V. Vasilakos, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102496, doi: 10.1016/j.jnca.2019.102496.

[19] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019, doi: 10.1016/j.sysarc.2018.12.005.

[20] P. Zhang, J. Liu, Y. Shen, H. Li, and X. Jiang, "Lightweight tag-based PHY-layer authentication for IoT devices in smart cities," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3977–3990, May 2020, doi: 10.1109/JIOT.2019.2958079.

[21] W. Feng, Y. Qin, S. Zhao, and D. Feng, "AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS," *Comput. Netw.*, vol. 134, pp. 167–182, Apr. 2018, doi: 10.1016/j.comnet.2018.01.039.

[22] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/ACCESS.2019.2905846.

[23] R. Nakanishi, Y. Zhang, M. Sasabe, and S. Kasahara, "IOTA-based access control framework for the Internet of Things," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Paris, France, Sep. 2020, pp. 87–95, doi: 10.1109/BRAINS49436.2020.9223293.

[24] S. Qi, X. Yang, J. Yu, and Y. Qi, "Blockchain-aware rollbackable data access control for IoT-enabled digital twin," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 11, pp. 3517–3532, Nov. 2023, doi: 10.1109/JSAC.2023.3310061.

[25] M. Hamad, A. Finkenzeller, H. Liu, J. Lauinger, V. Prevelakis, and S. Steinhorst, "SEEMQTT: Secure end-to-end MQTT-based communication for mobile IoT systems using secret sharing and trust delegation," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3384–3406, Feb. 2023, doi: 10.1109/JIOT.2022.3221857.

[26] M. Dammak, S.-M. Senouci, M. A. Messous, M. H. Elhdhili, and C. Gransart, "Decentralized lightweight group key management for dynamic access control in IoT environments," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 3, pp. 1742–1757, Sep. 2020, doi: 10.1109/TNSM.2020.3002957.

[27] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller, "Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications," *IEEE Access*, vol. 3, pp. 1503–1511, 2015.

[28] B. Chen, L. Liu, and H. Ma, "HAC: Enable high efficient access control for information-centric Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10347–10360, Oct. 2020, doi: 10.1109/JIOT.2020.2989361.

[29] K. C. Yadav, "Smart HAC system," in *Proc. Int. Conf. Circuit, Power Comput. Technol. (ICCPCT)*, Nagercoil, India, Mar. 2016, pp. 1–4, doi: 10.1109/ICCPCT.2016.7530117.

[30] S. Behrad, E. Bertin, S. Tuffin, and N. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," *Future Gener. Comput. Syst.*, vol. 108, pp. 46–61, Jul. 2020, doi: 10.1016/j.future.2020.02.014.

[31] Y. Chen, Y. Sun, N. Lu, and B. Wang, "Channel-reserved medium access control for edge computing based IoT," *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102500, doi: 10.1016/j.jnca.2019.102500.

[32] S. Belguith, N. Kaaniche, M. Hammoudeh, and T. Dargahi, "PROUD: Verifiable privacy-preserving outsourced attribute based SignCryption supporting access policy update for cloud assisted IoT applications," *Future Gener. Comput. Syst.*, vol. 111, pp. 899–918, Oct. 2020, doi: 10.1016/j.future.2019.11.012.

[33] C. Cicconetti, M. Conti, and A. Passarella, "Uncoordinated access to serverless computing in MEC systems for IoT," *Comput. Netw.*, vol. 172, May 2020, Art. no. 107184, doi: 10.1016/j.comnet.2020.107184.

[34] D. Wang, Y. Qu, Y. Fu, Y. Yang, and Q. Chen, "A non-orthogonal random access scheme based on NB-IoT," *Wireless Pers. Commun.*, vol. 111, no. 4, pp. 2625–2639, Apr. 2020, doi: 10.1007/s11277-019-07006-5.

[35] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Comput.*, vol. 23, no. 3, pp. 2067–2087, Sep. 2020, doi: 10.1007/s10586-020-03058-6.

[36] B. Lu, L. Wang, J. Liu, W. Zhou, L. Guo, M.-H. Jeong, S. Wang, and G. Han, "LaSa: Location aware wireless security access control for IoT systems," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 748–760, Jun. 2019, doi: 10.1007/s11036-018-1088-x.

[37] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for risk-based access control model for IoT," *Internet Things*, vol. 6, Jun. 2019, Art. no. 100052, doi: 10.1016/j.iot.2019.100052.

[38] H. F. Atlam, R. J. Walters, G. B. Wills, and J. Daniel, "Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT," *Mobile Netw. Appl.*, vol. 26, no. 6, pp. 2545–2557, Dec. 2021, doi: 10.1007/s11036-019-01214-w.

[39] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101653, doi: 10.1016/j.cose.2019.101653.

[40] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernández-Campusano, "A context-aware privacy-preserving method for IoT-based smart city using software defined networking," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101470, doi: 10.1016/j.cose.2019.02.006.

[41] J. B. Awotunde, T. Gaber, L. V. N. Prasad, S. O. Folorunso, and V. L. Lalitha, "Privacy and security enhancement of smart cities using hybrid deep learning-enabled blockchain," *Scalable Comput., Pract. Exper.*, vol. 24, no. 3, pp. 561–584, Sep. 2023.

JAMIL ABEDALRAHIM JAMIL ALSAYAYDEH (Member, IEEE) received the degree in computer engineering and the M.S. degree in computer systems and networks from Zaporizhzhia National Technical University, Ukraine, in 2009 and 2010, respectively, and the Ph.D. degree in engineering sciences, with a specialization in automation of control processes, from the National Mining University, Ukraine, in 2014. Since 2015, he has been a Senior Lecturer with the Department of Electronics and Computer Engineering Technology, Faculty of Electrical and Electronic Engineering Technology, Universiti Teknikal Malaysia Melaka (UTeM). He is also a Research Member with the Center for Advanced Computing Technology. He has supervised bachelor's and master's students. His research interests include formal methods, simulation, the Internet of Things, computing technology, artificial intelligence, and machine learning: computer architecture, algorithms, and applications. He is the author/coauthor of more than 43 research publications in his research, which were cited by more than 95 documents. He actively publishes research articles and receives grants from the government and private sectors, universities, and international collaboration. He is a member of the Board of Engineers Malaysia (BEM). He is also a reviewing member of various reputed journals.

IRIANTO received the master's degree, in 2009, and the Ph.D. degree in applied and computational statistics from Universiti Putra Malaysia, in April 2021. Since graduation, he started to teach at several universities in Indonesia. From 2012 to 2021, he was a Lecturer with the Faculty of Engineering Technology, Universiti Teknikal Malaysia Melaka. In 2021, he was an Assistant Professor with American International University, Kuwait. Since 2022, he has been an Assistant Professor with Rabdan Academy and Zayed Military University, United Arab Emirates. His research interests include applied mathematics and multivariate statistical process control.

MOHANAD FAEQ ALI received the bachelor's degree in computer science from the Faculty of Computer Science, Baghdad College of Economic Sciences University, and the master's degree in computer science (internetworking) and the Ph.D. degree in IoT cyber security from the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM).

MOHAMMED NASSER MOHAMMED AL-ANDOLI received the B.Sc. degree in computer information systems from Mutah University, Jordan, in 2011, the M.Sc. degree in computer science from the Jordan University of Science and Technology, Jordan, in 2016, and the Ph.D. degree in information technology from Multimedia University, Malaysia, in 2022. He is currently a Senior Lecturer with the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM). His main research interests include malware analysis, complex network analysis, machine learning, high-performance computing, deep learning, and parallel computing.

SAFARUDIN GAZALI HERAWAN is currently a Senior Lecturer with Bina Nusantara University, Jakarta, Indonesia. He is the author/coauthor of more than 80 research publications which are cited by more than 290 documents. His current research interests include automotive engineering, renewable energy, and heat recovery technologies.