IECE Transactions on Sensing, Communication, and Control
http://dx.doi.org/10.62762/TSCC.2024.322898

REVIEW ARTICLE

Next-Generation Technologies for Secure Future Communication-based Social-Media 3.0 and Smart Environment

Archana Kurde[1] **and Sushil Kumar Singh**[1,*]

[1] Department of Computer Engineering, Marwadi University, Rajkot, India

Abstract

Smart Environment is rapidly growing with the inclusion of Artificial Intelligence of Things (AIoT) when it connects to future communication and social media networks. Security and privacy are significant challenges, including data integrity, account hijacking, cybersecurity, and cyberbullying. To mitigate these challenges, Social Media 3.0 is utilized with advanced emerging technologies such as Blockchain, Federated Learning (FL), and others and offers solutions in existing research. This article comprehensively reviews and proposes Next-Generation Technologies for Secure Future Communication Service Scenario for Smart Environment and Social-Media 3.0. We discuss existing attacks with their classification that can threaten the personal information of a Future Communication-based Smart Environment, then offer countermeasure solutions. FL with AIoT is discussed to preserve the privacy and security of smart environment applications with live projects under the implementation of the Dubai Blockchain Strategy, ADEPT, and many more. Blockchain is utilized at the proposed service scenario's edge, fog, and cloud intelligent layers for secure future communication; FL trains local models that aggregate to form global models trained over diverse Smart Environments. Finally, several challenges and open issues of integrating emerging technologies for Smart Environment and Social-Media 3.0 applications and future directions are discussed in the last section.

Keywords: smart environment (SE), blockchain, federated Learning (FL), social media, internet of things (IoT).

1 Introduction

The inclusion of the Internet of Things (IoT) and Artificial Intelligent of Things (AIoT) devices in everyday life have tremendously impacted the everyday lives of humans. The easy access to the sensors and evolving interfaces has made their usage simple for novice users. The sensors keep on sensing physical parameters that are analyzed to make decisions, which results in the actions to be performed by actuators. This ecosystem is rapidly flourishing with increasing access to high-speed internet, reduced hardware costs, sophisticated user interfaces, and the need for self-learning and decision-making systems.

Academic Editor:
Ibrar Hussain

Submitted: 12 October 2024
Accepted: 06 November 2024
Published: 27 November 2024

Vol. 1, **No.** 2, 2024.
10.62762/TSCC.2024.322898

***Corresponding author:**
Sushil Kumar Singh
sushilkumar.singh@marwadieducation.edu.in

Citation
Kurde, A., & Singh, S. K. (2024). Next-Generation Technologies for Secure Future Communication-based Social-Media 3.0 and Smart Environment. *IECE Transactions on Sensing, Communication, and Control*, 1(2), 101–125.

Smart Healthcare (SH), Smart Agriculture (SA), Smart Transportation (ST), Smart Parking (SP), and other areas utilize the growing automation techniques in Smart Environment with Social- Media 3.0. SH integrates security cameras, thermostats, door locking systems, entertainment unit actuators, etc., which ease home appliances' operation and ensure the home's security and safety. Smart Buildings (SB) have lighting control systems, Heating/ Air conditioning, and fire extinguisher systems for energy conservation and protection against hazards [1]. SB is capable of responding according to external climate conditions and transit to the best operating profile. The weather data obtained from the sensor is be used to forecast the weather conditions that are utilized to modify the current operating profile for smooth transitions [97]. Smart transportation includes parking automation, automatic vehicles, real-time traffic updates for on-road vehicles, and many more. Smart Healthcare includes remote monitoring of patients' health, wearable devices, prediction of diseases, tele-diagnosis, and medication [2]. City traffic can be controlled efficiently using autonomous vehicles and smart vehicles that update the traffic controllers with the current traffic scenario, which could make the essential changes in traffic signal scenarios to regulate the traffic accordingly [98]. Smart Agriculture comprises soil and crop monitoring, monitoring for a sprinkling of fertilizers and pesticides, and automatic irrigation systems that enhance the farmers' productivity by reducing their efforts to a considerable extent. The water requirement by different types of soil as per the type of crop and climatic conditions could be monitored, and the data collected can be used to make decisions regarding water supply, the need of fertilizers as per requirement, and harvesting can enhance the crop production and ease the efforts to be done by the farmer [99]. Smart retail inculcates tracking of inventory, automated payment systems, and staff tracking systems to increase retailers' efficiency [3]. A distributed Mall is a concept fusing the characteristics of online shopping and offline stores, geo-located publicity, inventory prediction, product tracking, and relevant and meaningful product recommendations [100]. The various ecosystems forming an intelligent and Smart Environment (SE) are shown in Figure 1.

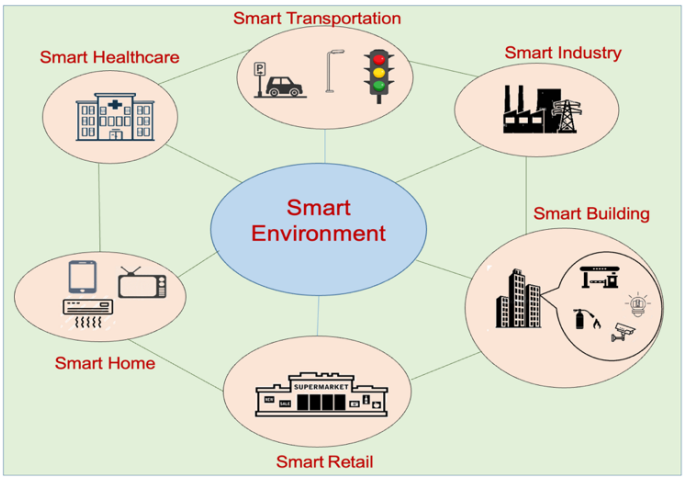

Figure 1. Constituent Ecosystems Forming Intelligent and Smart Environment.

Constituent Components of Smart Environment. All the ecosystems of SE incorporate very sophisticated embedded systems such as cameras, smartphones, smart wearables, air conditioners, safety doors, traffic sensors, and many more, which generate sensitive data that needs to be protected to ensure the individual's privacy. The smart devices have limited computational power, energy constraints, and low storage. Devices with diverse network configurations must collaborate for multiple tasks, with almost no data security mechanisms implemented. Devices with limited energy face the challenge of incorporating advanced data-securing mechanisms due to their high computational requirement and high-power need [4]. Designers need to respect the security and cryptography mechanisms and consider integrating the mechanisms at later phases of development, which can prove hazardous to the safety and security of the individuals and organizations involved in the system.

Vulnerabilities in Smart Environment. The heart of SE is data, which is collected from various sensors that are constituent components of commonly used intelligent appliances such as smartphones and digital cameras. The sensors record sensitive data such as fingerprints, retina scanners, GPS sensors, motion sensors, and thermostats, recording temperature changes along with device location. Smartphones give users access to their private messages, chats, photographs, contacts, confidential messages, and e-mails regarding financial transactions [5]. All this data is accessible to unknown applications installed on the smartphone. The purpose of collecting this data needs to be more evident to the user. All these devices need to stay connected to their peers for communication and to pursue their purpose of existing in the environment. Intruders leverage this liberty of access to sensitive data to encounter cyber-attacks and even steal sensitive data [6].

1.1 Research Motivation

SE incorporates smart embedded systems that sense specific environmental characteristics and physical quantities to generate large amounts of data, which is required to be preprocessed, analyzed, and used by the ecosystem to train models that can be used for making decisions for unknown scenarios. The process involves the communication of heterogeneous objects on a network. The large data generated is often stored on cloud services to support access from remote locations. This complex scenario is often prone to cyber-attacks that get unauthorized access to the data and intrude into the system to affect the decisions taken by the system based on the trained model. Reyna et al. [7] discussed the potential benefits and ways to integrate Blockchain with IoT and discussed the potential applications, associated challenges, and Blockchain platforms specific to IoT. Blockchain has the ability to provide solutions to the privacy of personal data. The use of Blockchain permits access to personal data only upon the owner's approval [8]. Blockchain is the foundation of the implementation of smart ecosystems, namely, 'Dubai Blockchain strategy' at the city level, 'Estonian Blockchain technology' at the country level, 'WWF Blockchain-based seafood traceability', and 'Walmart & IBM food safety solution' at the organization and smart environment level. Blockchain can provide enhanced B2B, B2C, and Government to Citizens (G2C) services by establishing improved transparency, immutable audit logs, enhanced accountability, embedded security, and mutual trust. These characteristics support the bright future of Blockchain for securing futuristic Smart Environments [9]. A Blockchain-based framework, namely SpeedyChain, is proposed in [10] that manages smart city data resiliently, immutably, and in a decentralized manner. The data stored in transactions is decoupled from the block header using a Blockchain-based framework, which allows for the fast addition of data to the blocks.

Privacy-Sharing is a Blockchain-based innovative framework for privacy-preserving and secure IoT data sharing in a smart city environment [11]; the Blockchain network is divided into various channels to preserve data privacy, where every channel consists of a finite number of authorized organizations and process-specific type of data such as smart energy, smart vehicle, smart healthcare and many more. The access control rules are embedded in smart contracts to control user data access within a channel. Private data collection and encryption are carried out to isolate and secure data within a channel.

In the context of data processing and analysis for decision-making, traditional Machine learning algorithms do not preserve user data privacy. Traditional machine learning algorithms collect data from various devices at a central location, which is utilized to train models. Centralized processing can prove to be a threat to the confidentiality of data. In contrast, the federated learning method is a recent development in machine learning. The model is transferred to the device that generates data in federated learning. Thus, the model is trained at the location itself and is responsible for generating the data; it prevents the security threat to data during transmission and sharing with the central processing location [12]. Modern healthcare systems desire to train models for the diagnosis and prediction of disease, but patients' medical data cannot be transferred without confidentiality and trust. Thus, instead of sharing the raw data with the center for the training model, transferring the locally trained model to the center is more feasible to get an accurate model [13]. The inclusion of Blockchain in SE is shown in Table 1, and Table 2 includes the contribution of FL in SE. After that, we proposed a Next-Generation Technologies-enabled Secure Future Communication Service Scenario for Smart Environments and Social-Media 3.0.

1.2 Limitations of the Related Literature

The existing survey concentrating on the convergence of FL and Blockchain Technology does not consider modern consensus algorithms like PoS or PoA. Whereas the conventional consensus PoW is energy intensive [26, 30]. Federated learning is capable of preserving privacy during model training, the privacy and security issues prevailing during data collection also require to be addressed [12]. Device authentication plays a key role when introducing a new node in the network; the architecture must incorporate this factor before introducing a block in the network [46, 47]. The training of the model incorporated at both ends of the Blockchain makes the process time-consuming to reach a consensus and add the final block to the network [37].

1.3 Research Contribution

From 2015 to 2024, the literature studied was published in major publisher databases (IEEE Explore, Springer, ACM Digital Library, ScienceDirect, arxiv—Cornell University, etc.).

The key contributions of this survey are summarized as follows:

- First, a discussion about Blockchain technology for preserving the security and privacy of Smart Environment and data is included.
- Second, federated learning can be applied to training models without compromising the security of SE and SM 3.0 data.
- Next, we describe the Integration of Blockchain and Federated Learning to attain data security and privacy in Social-Media 3.0. After that, we discuss several Social-Media 3.0-related projects using the integration of Blockchain and Federated Learning.
- We proposed a Next Generation Technologies enabled Secure Future Communication Service Scenario for Smart Environments and Social-Media 3.0.
- Finally, the attacks that can compromise the security of SE and SM 3.0 are classified, and several challenges and open issues of integrating FL and Blockchain for Smart Environment and Social-Media 3.0 applications and future directions are included.

1.4 Paper Organization

The rest of the paper consists of Section 2, discussing the role of Blockchain in developing a secure smart environment. Federated learning for local training models is used to preserve privacy among smart modules. The amalgamation of Blockchain and federated learning for a secure smart environment. Section 3 discusses Social-Media 3.0, its security threats, and promising solutions for secure access to Social-Media 3.0 using Blockchain and federated learning. After that, Section 4 comprises open research issues and Future work along with a conclusion.

2 Related Work

In this section, we discuss the preliminary aspects of Blockchain technology and its utilization to ensure the privacy and security of user data in a smart environment. It also includes preliminary aspects of FL and its contribution to retaining user data privacy and security in SE. Integrating Blockchain and federated learning for secure and private data preservation in SE is also discussed.

2.1 Preliminaries

This subsection discussed and elaborated on using Blockchain and FL for a secure Smart Environment and Social-Media 3.0 and utilizing federated learning for training models at distributed nodes.

Blockchain Technology. The centralized data storage used for storing an individual's sensitive financial and personal details in a smart environment has chances of single-point failure, thus proving a threat to the loss of data stolen by outsiders. This scenario gave rise to the need for a decentralized system. Blockchain is a list of records (blocks) Figure 2, which store data publicly and in chronological order. Blockchain is a distributed digital ledger secured by peers connected to a network having access to the ledger. A ledger is a document recording all the transactions carried among any two users. The information stored in blocks is secured using cryptography. Data is validated and accessed by participants on the network bearing the same copy of the ledger. Thus, if one node on the network gets corrupted, the rest of the nodes will come to know immediately and rectify it.

Working of Blockchain. When a sender is willing to transact, he will publish the transaction details on the public Blockchain network. Miners verify the authentication of users; after the verification, the transaction is added to a block and made part of the Blockchain. The transaction occurs as soon as the block is added to the Blockchain. It is the miner's responsibility to verify the sender's and receiver's authenticity and also check the sender has sufficient balance to continue the requested transaction. The ledger across all the nodes is updated with this newly added block. Privacy of all the blocks is preserved by applying hashing on the block. As shown in Figure 3, the transaction detail is represented as a 256-bit hash value in the Merkle root/ Hash root header.

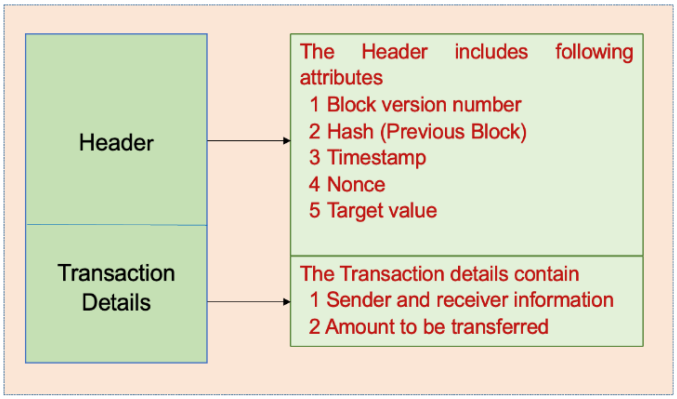

Figure 2. Block Structure Detailed View.

Whenever some changes are made in a block, the hash value of the block changes, as shown in Figure 4. This new value of the block will not match the previous block hash value present in the next block. Thus, the next block will be alerted to some modifications made to the previous block. Hence, the changes can be immediately identified and rectified. Blockchain also includes digital signatures to ensure the message is sent by an authentic person. Users are provided their own private and public keys. The private key is used by the user to control his account, whereas the public key is shared by the user to identify him on the network. This public key is shared on the network for other users to verify the transactions; both the hash values generated, namely value-1 and value-2, are compared; if they match, the sender's identity is approved or else rejected, as depicted in Figure 5.

Proof of Work Consensus Algorithm. Proof of work involves people worldwide (Miners) competing to be the first to add a block to the Blockchain. The miner has to generate a nonce value within the target requirement, so the miner keeps generating hash values that satisfy the condition. Once a minor is able to get a valid hash value, he ignores that on the network. This value can be easily verified by the other participants on the network. The privacy and security preserving characteristic of Blockchain is very beneficial for scenarios like SE, where private and sensitive data to users is to be shared on the network, which can be compromised in the open network access. Thus, utilizing the capabilities of Blockchain will be very favorable to building a secure and privacy-preserving SE. The attempts to integrate Blockchain with SE and its ecosystem are included in Table 2, which includes Research papers on various smart environments published since 2019. Blockchain Used for Smart Environment is shown in Figure 6. The Proof of Work consensus algorithm is quite energy consuming, thus leading to the discovery of other consensus algorithms like Proof of Stake (PoS), Proof of Authority (PoA), Byzantine Fault Tolerance (BFT) Algorithm are as described below.

Proof of Stake (PoS). Nodes on a network contend to become a validator of new blocks to earn the fee. The nodes carry out transactions which are put inside a pool. All the nodes contending to become validators for the next block raise a stake, which is combined with the selection algorithm to identify the validating nodes for the next block. After verification by validator nodes and other nodes in the network, the block is validated, and the fee and stake is received by the validator node. All the nodes do not contend to add blocks to the network, thus saving energy.

Proof of Authority (PoA). This is a permissioned consensus mechanism where validator nodes have proven their authority to act as validator nodes. The validator nodes run software that allows them to put transactions in a block. The reward or fee for adding a block is not in the form of cryptocurrency. Instead, they stake their reputation.

Byzantine Fault Tolerance (BFT) Algorithm. It is a consensus algorithm that proves beneficial when some nodes in the network fail to respond or the response is incorrect. The network has a primary node to behave as a leader, whereas the rest of the nodes are secondary nodes that are backup nodes that help the primary node to reach a consensus. The client sends request to primary node which broadcasts the request to secondary nodes which collectively reach a consensus and inform the primary node about this.

Machine Learning for Training Model. The data collected from various devices installed in Smart Ecosystem is to be used to improve decision-making by predicting future scenarios. This requires a training model based on the collected data; the model training is carried out using various Machine learning techniques such as Supervised Learning, Unsupervised Learning, Reinforcement Learning, and Federated Learning.

Supervised Learning. Supervised learning includes training of models based on labeled data. It is comparatively easier to implement supervised learning and less computationally expensive, but getting labelled data for training is challenging when dealing with real time data collection from sensors present in Smart Environment. Thus proving Supervised learning, a nonfeasible solution for training models using real-time data.

Unsupervised Learning. The availability of labeled training data is an issue when the data is collected from a data-intensive Smart Environment. Thus, training of a model based on unlabeled data is carried out in Unsupervised learning, where features showing similar patterns are grouped to form clusters, and no prior labeling of data is needed. This makes Unsupervised learning a considerable choice when labeled data is not available for training.

Reinforcement Learning. The model is trained by providing rewards for a correct move to appreciate the model's good performance, whereas a penalty for

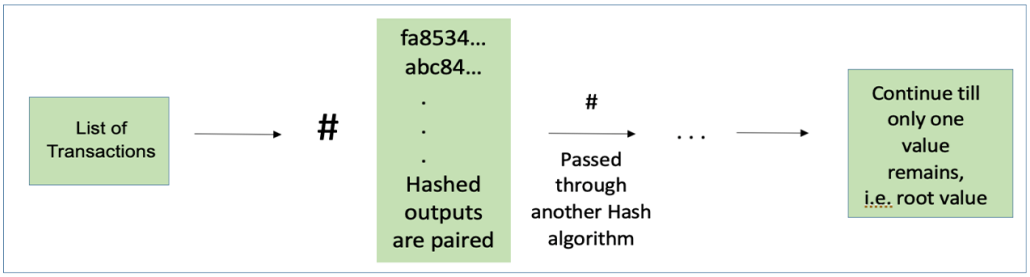

Figure 3. Application of Hashing on Transactions.

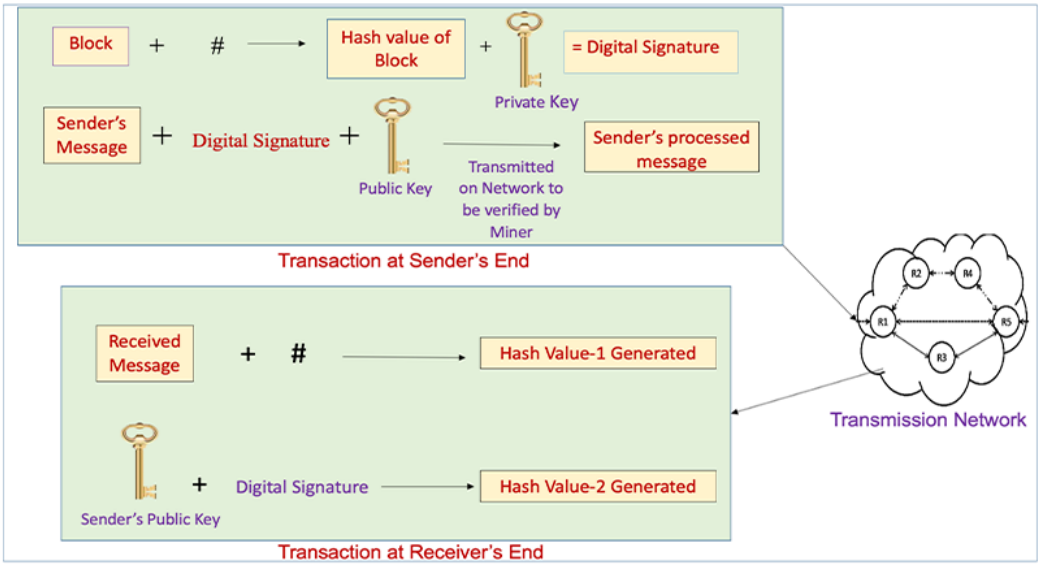

Figure 4. Transactions at Sender's and Receiver's End.

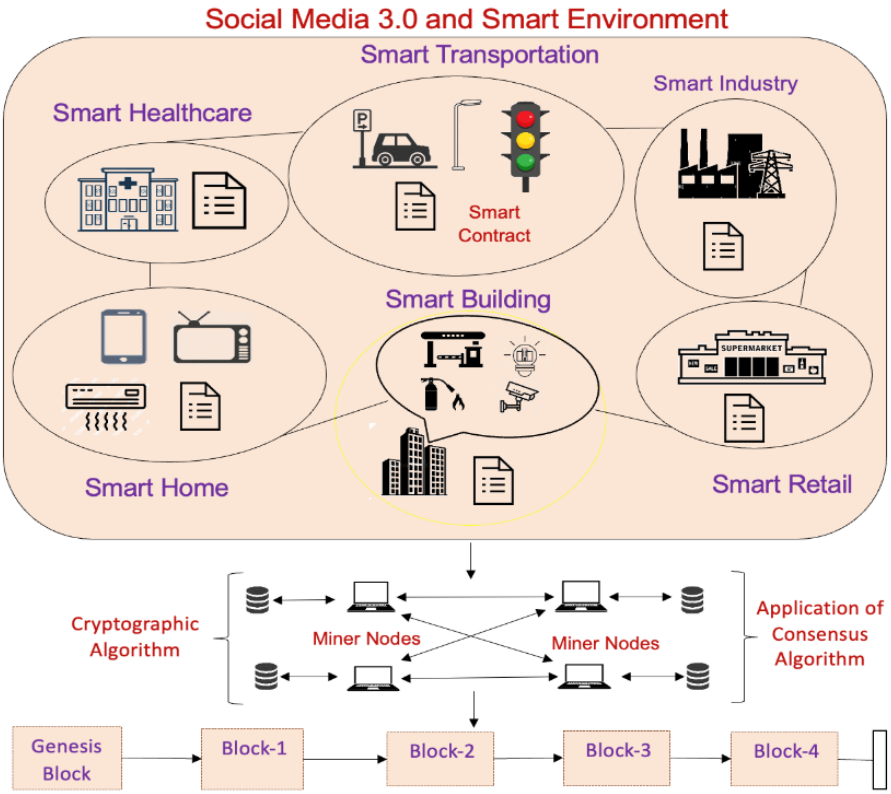

Figure 5. Blockchain Used for Smart Environment.

Table 1. Summary of Blockchain Applications in Smart Environments.

Study (Year)	Category	Definition	Architecture	Blockchain	Smart Environment	Security and Privacy
Rue Zhang et al. [15], 2021	Smart City	Healthcare Blockchain is used to store and/or share medical data securely.	Distributed	•	Healthcare	•
F. Orecchini et al. [16] 2019	Smart Mobility for Renewable energy sources	Innovative technology-based solutions are provided for Smart city where human and social capital interact.	Distributed	•	Automobile	•
Mukherje et al. [17], 2021	Smart City	The quality of life of people within a Smart city are alleviated using latest information and communication technologies (ICT).	Distributed	•	∗Smart citizen; ∗Healthcare; ∗Agriculture; ∗Transportation; ∗Energy utilization; ∗Governance.	•
Jiahui et al. [18], 2021	Smart City	Wireless sensor networks that are certain about the authenticity of server form Smart environment.	Distributed	⊛	Cryptocurrency transactions	•
Paul et al. [19], 2021	Smart City	A variety of sensors such as camera, thermostat, Light Detecting Resistance (LDR) forms building blocks for Smart city.	Layered	⊛	Transactions	•
Wong et al. [20], 2020	Smart City	A smart city with digital and advance technologies to improve living standards, quality of services of their citizens.	Distributed	•	∗Smart logistics; ∗Smart Governance; ∗Smart Mobility.	•
Wanqing et al. [33], 2024	Secure payment Protocol	Intermittent on chain connectivity is made flexible by a Blockchain based offline payment protocol.	Distributed	•	Secure offline payment protocol	•
Zhan et al. [83], 2023	Social Media	A conceptual model based on Blockchain for illustrating business strategy and operations of social media accounts of Firms.	Distributed	•	Crypto economy social media model	•
Sengan et al. [92], 2020	Smart City	A Hybrid method to provide architecture for Cyber Security.	Hybrid	○	Power Supply	•
Singh et al. [93], 2020	Smart City	A Deep Learning-based IoT-oriented infrastructure for a secure smart city.	Distributed	•	∗Smart Industry; ∗Smart Farming.	•
Ali et al. [94], 2020	Smart Vehicle	The proposed framework is beneficial when several flying zone/clusters are present in IoD environment and extends scalability.	Centralized	○	Stolen verifier	⊛

Note: • -> Yes; ○ -> No; ⊛ -> Partially

making an incorrect or bad move. Thus, this motivates the model to make correct decisions by maximizing the rewards gained so far. Thus, reinforcement learning is to be opted for in scenarios where future states are to be predicted.

Federated Learning. The huge data generated by the various components of the smart environment has to be analyzed and used for training models, which in turn make decisions for upcoming inputs. Conventional machine learning algorithms collect the generated data from the source at a single point, and the model is trained using received data. This method of collecting data for training models does not preserve the privacy of information, which could be sensitive data when smart cities environment and other smart environments is under consideration. Due to this limitation of traditional machine learning algorithms,

Table 2. Smart City Environment Projects Developed by Leveraging Blockchain Technology.

Study (Year)	Objective of Project	Services Provided
Dubai Blockchain Strategy 2020 [51]	• Government Efficiency • Industry Creation • International Leadership	• Paperless transaction • Blockchain business registry • Blockchain for electricity • Water billing, etc.
ADEPT 2019 [91]	• Autonomous decentralized peer-to-peer telemetry (ADEPT) where the peers execute the transactions. • Preparation of contract is decentralized manner through peer-to-peer consensus network. • Device coordination is autonomously handled by Consensus ledger.	• Smart Homes • Industrial IoT • Smart Hospitals, etc.
Zug Digital ID 2020 [80]	• uPort's identity model returns ownership of identity to the individual. • Allow users to register their own identity on Ethereum, send and request credentials, sign transactions. • Securely manage keys and data on its open identity system.	• Access to digital government services. • Voting on the presence of fireworks at an upcoming festival. • AirBie is a bike-sharing service.

Federated learning has grabbed the attention to secure the data used for training models. FL decouples data collection and model training, which ensures the security of data collected by avoiding its transmission on a network to be received by a central node, which is responsible for training the model using data received from various sources. Thus, in contrast to the centralized approach of conventional machine learning, a distributed learning mechanism is carried out locally at all the devices generating data.

FL comprises three main components: the data owner or parties, the manager, and the communication-computation framework. The parties can be mobile phones or any smart device generating the raw data [13]. The device trains the local model based on its raw data. This prevents the sharing of data with the server to train the model. All such parties build their own local models using their own datasets for training. These distributed models are then shared with the manager/server to build an aggregated global model. The naive implementation of the above scenario will result in large local models that must be transmitted to the server, which will be a bottleneck for the communication network. To overcome this problem, in the case of large models, the parties need to adopt some methods to reduce the uplink communication cost [14]. Federated learning is classified into three basic types: Horizontal Federated learning, Vertical Federated learning, and federated transfer learning. The nodes having data are stored in matrix form, where data consists of many instances. The sheet's horizontal axis is considered client, whereas the vertical axis represents client characteristics. This facilitates the division of FL based on the partition method [27]. In the Horizontal FL, the data of various nodes have certain similarities but may differ in sample space, i.e. the data collected by a particular sensor of the smartphone has few overlapping features, but the device belongs to different individuals, thus forming separate sample space, shown in Figure 7. In vertical FL there is partial overlapping between samples whereas differing in feature space, i.e. a hospital has patient records based on demographics and another hospital has reports of its patients; thus, the two hospitals can train their own model without sharing their confidential data to the central server responsible for collecting the data from various health care centers. Unlike Horizontal and Vertical Federated learning, the data does not share a resemblance in sample space or feature space. Thus, the major problems are the lack of data labels and poor data quality. Thus, transfer learning enables knowledge to move from one domain to another to obtain good results.

Thus, the application of Federated learning in SE is quite promising, as the main concern in SE is about the privacy and security of confidential personal data, which can get compromised by the adoption of conventional Machine learning methods that are centralized in nature. The distributed nature of Federated learning is suitable for providing personalized interaction experiences to individuals

i.e. personalized recommendation of products in a smart retail system based on the local model trained using the personalized data of the user himself, even without compromising the privacy of the sensitive data that may suffice on use of conventional Machine learning techniques. The literature studied regarding the usage of FL for smart cities incorporates the Research carried out on prominent issues involved in SE and its various ecosystems, which is presented in Table 3, which comprises recent research and those since the SE's inception. Figure 8 shows the contribution of FL in SE. Table 4 discusses projects utilizing federated learning in real-world deployment.

2.2 Integration of Blockchain and Federated Learning for SE

Blockchain has the capability of enhancing security and privacy to train and analyze critical information collected by the nodes of SE. FL has the potential for decentralized collaborative data analysis with minimum response time and cost. Thus, Blockchain can collaborate with FL to build a secure, privacy-preserving SE. The smart vehicular nodes collect their data according to their geographic locations, which are diversified for various nodes per the bio diversities, flora, and fauna. Groups of such nodes in similar geographical locations create their own blocks and maintain a ledger for the collected data. The Blockchain ensures that the blocks formed are introduced by authentic users to testify to the genuineness of the data. After assurance of the authenticity of data, the information stored in the block is used to train the local model, which in turn is aggregated with the rest of the local models at the central server responsible for forming the global model from the aggregated local models. Thus, exploiting Blockchain and FL to achieve a decentralized, secure smart vehicle [28]. The convergence of Blockchain and Federated Learning for SE is shown in Table 5.

3 Secure Access to Social Media 3.0 Using Blockchain and FL

Social media has emerged as the leading means of communicating with friends and family for over a decade. The ease of sharing personal updates and life's whereabouts with our contacts comes with a high cost of compromise in privacy and security threats to the personal data of the user sharing his information on social media. The loss can grow even more if a person shares photos, videos, geographic locations, etc., on social media, unaware of the malicious use of shared information for illegitimate purposes. Apart from this, social media is used for advertisement and publicity by marketers to promote their services or products online to reach their customers based on their past information shared on media. If the individuals sharing their information do not consider the security issues seriously, they become more vulnerable to various threats that put their personal data at risk. Social media platforms like Facebook and Twitter are used to establish social connections and share multimedia data, such as photos and videos, with established contacts. Multimedia sharing networks include YouTube, Instagram, Snapchat, and many more for sharing shortened URLs to share pictures, videos, and live videos to the viewers. It is difficult to find the media shared and its source by looking at its URL. LinkedIn and Pinterest are examples of professional social networking platforms to share their projects/ideas and area of expertise, which allows professionals to share their professional information like the address of their workplace, and email ID, which can be used by intruders to perform personal attacks through email [48].

3.1 Threats due to Attacks and Existing Countermeasures on Social-Media

Threats to social media users can be classified into three categories based on the prevailing time and sophistication of the attack. They can be divided into Primitive, Contemporary, and targeted threats. Primitive threats are those threatening social media since its inception. Contemporary threats employ more sophisticated attacks to access social media users' data, whereas target attacks aim at specific users or groups of users to seek vengeance. Figure 9 shows various attacks causing threats to social media user's data privacy and security, categorized as described above.

Phishing Attack. In a phishing attack, the hacker creates fake website pages that seem identical to the actual website. The URL to this fake website is then shared by fraudulent emails that appear to be sent by an authentic sender. The victim is then lured to give his personal information, including bank account details, government savings numbers, etc. The intruder can further take control of the receiver account to cause severe financial or reputation damage to the social media account holder [54].

Malware. Malware attack refers to using specially designed software to access or damage a computer network or data. It includes viruses, Trojans, ransomware, spyware, etc. The primary goal is

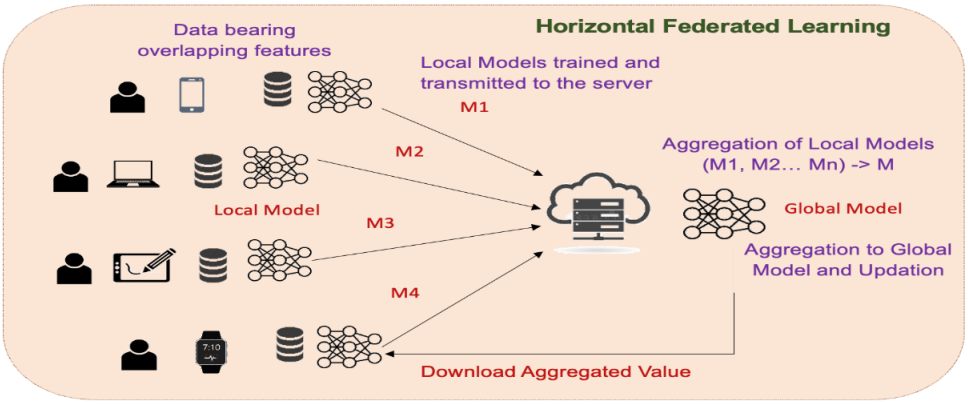

Figure 6. Horizontal FL Training Local and Global Models.

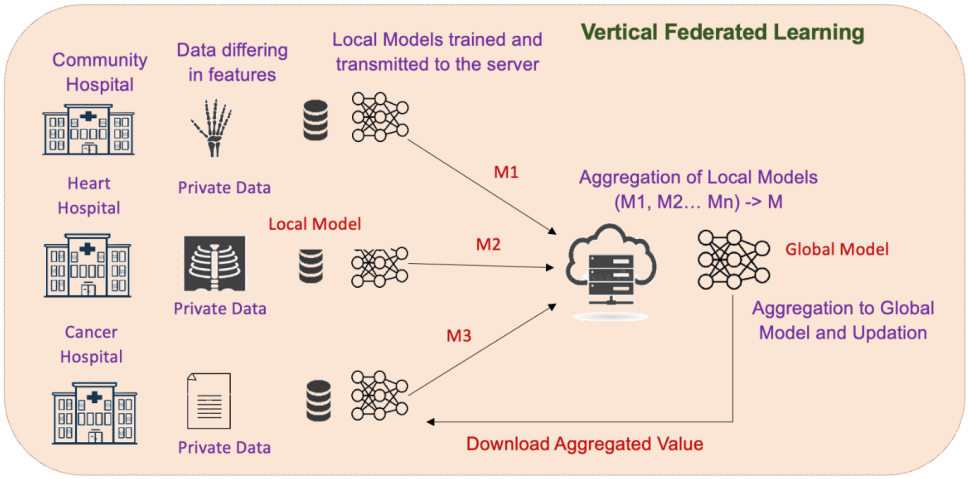

Figure 7. Vertical FL Training Local and Global Models.

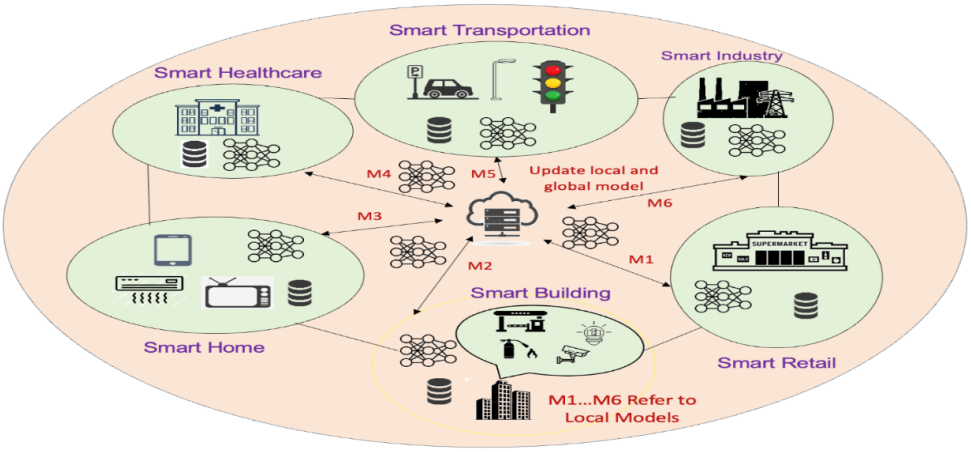

Figure 8. Implementation of Federated Learning in Smart Environment.

to cause harm to the computer system or network of the target by stealing sensitive data or gaining unauthorized access to the network or system of the target. Malware can also be self-replicating worms, which can be embedded in a URL and sent to the target through some dummy website, and the attack can be encountered on click event on the website [52].

Spam. A spam attack includes flooding a user or network with undesired messages in order to induce malware. These messages can be disruptive for the user, which may push the network to its bottleneck, or the inbox may reach its maximum limit, thus disrupting the normal behavior of the network that may lead to failure of the network or crash of the server when unable to handle the flooded messages. These messages can contain suspicious URLs, viruses, or

Table 3. Summary of Blockchain Applications in Smart Environments.

Study (Year)	Category	Definition	Architecture	Smart Environment	Security and Privacy
Qiang et al. [21], 2021	Sales	Federated learning keeps the private training data confidential by enabling multiple parties to collaboratively train their own machine learning model and share the model to server.	Decentralized	Smart Retail	•
Abdullatif et al. [31], 2022	Smart vehicle	Semi-supervised FL approach called FedSem handles the problem of unlabelled data in smart cities while preserving privacy and increasing data utilization.	Distributed	Traffic signal detection	○
Zhaohua et al. [22], 2022	Smart City	IoT sensors are included in smart city to collect data which can be utilized in various fields such as resource allocation and communication.	Distributed	∗visual detection; ∗Finance.	•
Raed et al. [23], 2022	Smart Building	Federated learning based Federated stacked long short-time memory model is trained on time series data generated by IoT sensors.	Decentralized	∗Lighting control; ∗water management.	•
Zhaohui et al. [24], 2022	6G	FL facilitates resource allocation or behaviour prediction in a distributed manner for wireless networks.	Distributed	∗Interference cancelation; ∗network control; ∗resource allocation; ∗user grouping.	•
Xumin et al. [25], 2021	Smart Parking lot	In FedParking, each PLO trains a shared LSTM model to forecast available parking spaces by the local data while preserving the training data privacy.	Distributed	∗Parking space estimation; ∗incentive mechanism.	•
Xiaoming et al. [35], 2023	Smart City	Traffic flow within smart city is predicted by capturing long and short spatiotemporal features and the correlation of near spatial dependency.	Distributed	Traffic prediction	•
Syed et al. [36], 2024	Smart City	A model for scheduling heterogeneous workloads and recommending resources for eHealth edge-cloud connectivity.	Distributed	Healthcare recommending	•

Note: • ->Yes; ○ ->No

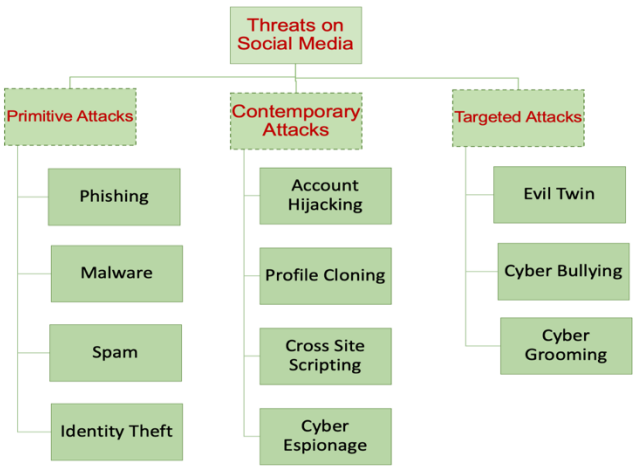

Figure 9. Various Attacks Prevailing Threats on Social Media.

malware capable of collecting the target's personal information, which could be exploited to cause further harm [59].

Identity theft. Identity theft includes accessing someone's personal information and credentials to commit fraud. Using account hijacking, the attacker gets access to a user's account by using any of the primitive attacks discussed above. The assailant uses someone else's identity, like a social security number or mobile number, to pretend to be someone else and get in contact with the target to gain access to his friend list and demand confidential information from them to encounter similar attacks on them [60].

Account Hijacking. Account Hacking refers to unauthorized access to a legitimate user through any of the conventional attacks to gain access to the

Table 4. Projects Developed by Leveraging Federated Learning.

Project (Year)	Objective of Project	Services Provided
Google GBoard [107], 2023	• Predictive text and autocorrect features	• Google's Keyboard app improves text prediction without collecting personal data.
Siri [108], 2023	• Refine models without sharing personal data with central server	• Voice command • Smart Home Applications • Music and media controls
NVIDIA Clara [109], 2022	• Train AI models on medical imaging data from different hospitals	• Radiology • Pathology • Drug discovery

actual user's personal information with the intention of asking for ransom on the pretext of surrendering the hacked account access without causing further harm to the information and access of the account [70].

Profile Cloning. In profile cloning, the attacker creates a duplicate profile of a certain account to dodge the contacts of the original account holder and introduce malware in their network or system. The attacker makes it difficult to distinguish between the original and fake profiles [61]. Using the fake profile created, the attacker can tarnish the image of the profile holder, spread fake rumors, and leak morphed pictures or videos of the authentic user.

Cross-site Scripting. Cross-site scripting attacks are carried out on web applications by embedding malicious scripts in the content that is to be delivered to users. When the user comes in contact with the script, the embedded malicious script executes on the browser to carry out actions such as stealing cookies, session tokens,, and other data [62]. The countermeasures for the attacks discussed in Table 6 are described in Table 7.

Cyber Espionage. Cyber espionage is the act of spying on sensitive data such as military data, highly confidential government affairs, foreign and political policies of a country, etc. China's APT10 is an attack that steals intellectual and Government confidential data worldwide. This is a quite critical and harmful attack that may affect the foreign affairs and political terms of countries involved in the incident.

Evil Twin. Evil Twin attack is also called Cyber impersonation, where the hacker mimics a social media account to get through the account holder's friends and take advantage of being their friend. The attacker sets an illegitimate Wi-Fi access point, thus gaining the victim's trust to promote sharing personal and confidential data on the network, assuming it to be safe to transmit crucial information like login credentials, emails, browsing history, and social media accounts [49].

Cyberbullying. Cyberbullying is continuous harassment of the target by sending emails or social media posts containing embarrassing or personal pictures or videos of the target to bully and disturb the mental peace of the target [48]. The prime threat is its capability to threaten a large number of victims simultaneously and at any time. The involvement of intimate information of the victim may restrict the victim from filing a complaint or seeking help.

Cyber Grooming. Cyber grooming refers to building emotional and intimate relations with the victim through intimate information that can be easily acquired from children or adolescents, which can be used to threaten or blackmail the victim in the near future. The groomer attempts to isolate the victim from his friends and relatives, thus pretending to perfuse the void and taking advantage by gaining access to intimate information of the victim, which could be used to further exploit the victim [63].

One or more such attacks can be carried out simultaneously to create a further threatening situation for the victim. Thus, social media requires more attention from researchers for security and privacy preservation. Social media 3.0 is a promising alternative enriched by the capabilities of IoT devices that give users immense liberty to access social media through various devices. This increased accessibility to social media requires using AI tools

Table 5. Convergence of Blockchain and Federated Learning for Social Environment.

Study (Year)	Category	Definition	Architecture	Security and Privacy
Chai et al. [28], 2015	Smart Vehicle	A framework by which vehicles learn environmental data and share the learnt knowledge with each other.	Distributed	•
Zhen et al. [29], 2023	Smart City	Function encryption, Blockchain, differential privacy, edge computing, and asynchronous communication are used to enhance data communication processing capability of smart city.	Decentralized	•
Zhao et al. [30], 2022	Smart Home	The system facilitates smart home appliance manufacturers to build a model using data from customers' home appliances to improve their service and products.	Decentralized	•
Sharnil et al. [12], 2023	Smart City	Smart cities empower people to manage resources through enabling technologies such as the IoT, Big data, FL, etc.	Decentralized collaborative learning	•
Otuom et al. [32], 2022	IoT	An adaptive, network trustworthiness and secure framework to determine trust values of end devices belonging to various networks.	Distributed	•
Konstantinos [34], 2021	IoT	The Industrial IoT based smart city network traffic is classified to identify anomalies due to Advanced Persistent Threat (APT) attacks.	Distributed	•
Yuanhang et al. [37], 2021	Smart Transportation	The miners verify model updates of distributed vehicles to prevent updates of unreliable model and then stored on the Blockchain.	Decentralized	•
Komal et al. [38], 2023	Smart Healthcare	A decentralized privacy-preserving framework for healthcare monitoring at home.	Decentralized	•
Ferheen et al. [39], 2021	Smart Vehicle	A solution for vehicles where they compete to become a relay node (miner) by processing the proposed Proof-of-Federated-Learning (PoFL) consensus.	Distributed	•
Zhanpeng et al. [40], 2022	IoT	Malicious devices and model tempering is prevented from malicious server using a secure global aggregation algorithm.	Distributed	○
Liu et al. [41], 2021	Smart Vehicle	In order to reduce the communication overhead and computation cost of vehicles, a cooperative privacy-preserving framework is introduced.	Distributed	•
Rong et al. [42], 2022	Edge Computing	A two-order aggregation calculation to solve the overhead of synchronization problems and the reliability of shared data is enhanced.	Distributed	•
Yuzheng et al. [43], 2021	Committee Consensus	BFLC is a decentralized, federated learning framework to avoid the influence of malicious central servers or malicious nodes.	Distributed	•
Yunlong et al. [44], 2021	Smart Network	To formulate the resource sharing task as a combinational optimization problem, a deep reinforcement learning-based algorithm is proposed.	Distributed	•
Weishan et al. [45], 2020	Hotel Air Conditioning System	A platform architecture for failure detection in IIoT, which enables verifiable integrity of client data.	Distributed	•
Sana et al. [46], 2019	IoT	The model updates are shared with the central node using the proposed framework.	Distributed	•
Gaofeng et al. [47], 2020	Heavy Haul Railway	The agents owning data are distributed among whom asynchronous collaborative machine learning approach is implemented.	Distributed	•

Note: • -> Yes; ○ -> No.

Table 6. Security attacks prevailing threats on social media 3.0.

Attack	Study (Year)	Affecting Platform	Technology Used	Description of Work Done	Security Solution Provided
Phishing	Wen et al. [53], 2023	Ethereum	Graph based technology	A graph-based feature extension method is used to build phishing detection framework.	•
	Zheng et al. [55], 2023	Ethereum	Graph based technology	Transaction evolution graphs are used to learn the feature of evolving behaviour to obtain a dynamic graph classifier.	•
	Huang et al. [56], 2024	Ethereum	Graph Neural Network	Feature augmentation is used to learn and present a graph level presentation by taking mean of the top n features.	•
	Valecha et al. [57], 2021	email	Machine learning models using Persuasion cues	Three machine learning models, with relevant gain persuasion cues, loss persuasion cues, and combined gain and loss persuasion cues respectively.	•
Malware	Faruk et al. [52], 2021	-	Artificial Intelligence	The emphasis is on detection and prevention of naïve user from malware using AI techniques	○
	Ojha et al. [64], 2021	Wireless Sensor Network	Mathematical Model	The quarantine and vaccination techniques are aggregated to obtain the equilibrium points of the proposed mathematical model.	•
	Zhao et al. [65], 2021	Android	Function call graph	Structural attack against graph based Android malware detection techniques, which addresses the inverse-transformation problem between feature-space attacks and problem-space attacks.	○
Spam	Rao et al. [59], 2021	Social Network	Machine learning and Deep learning	Feature selection/extraction is done using dimensionality reduction techniques, whereas social spam and spammer detection is done by various machine learning and deep learning techniques.	○
	Wang et al. [66], 2021	email	Game model	An evolutionary game model between an attacker and defender and establish replicator dynamics equations.	⊛
	Saad et al. [67], 2021	Blockchain memory pool	Hiking mining prices	For deducing prioritization mechanism, a set of countermeasures that utilize fee, age and size (namely , Contra-F, Contra-A, and Contra-S) are used.	•
Identity Theft	Haber et al. [60], 2021	Identity Governance	Cyber Kill Chain model	The identity governance is done using the Cyber Kill chain model using Infiltration, exploitation, exfiltration.	⊛
	Bilge et al. [68], 2009	Social Network	Automated identity theft	A forged profile is created automatic in a network where the victim is not yet registered and a friend of the victim is contacted who is registered on both networks.	○
Account Hijacking	Alterkav et al. [70], 2021	Social Network	Metalearning ML algorithm	Social media account's hijacking is verified by a novel framework for authorization.	•
Profile Cloning	Punkamol et al. [61], 2020	Social Network	K-nearest neighbours ML algorithm	The account cloning in online social networks is detected using a framework having three parts: Twitter Crawler, Attribute Extractor, and Cloning Detector.	•
Cross Site Scripting	Alsaffar et al. [62], 2022	-	Internet program	Improve available internet functions for preventing XSS assaults by creating a programme that detects XSS vulnerabilities by completely mapping internet applications.	•
	Ayeni et al. [71], 2018	Web applications	Fuzzy logic	The framework uses fuzzy logic to detect classic XSS weaknesses.	•
	Marashdih et al. [72]	Web applications	Static analysis	An algorithm is defined to improve the static analysis outcomes regarding XSS vulnerability detection.	•
Cyber Espionage	Rivera et al. [73], 2022	-	Espionage as a Service	The model considers two main aspects: first, the technical aspect driven by the rapid advance of ICT and the software engineering level used by cyber-criminals to create sophisticated malware.	○
	Bederna et al. [74], 2022	-	Botnet	The real-life cyber espionage capability of proposed Botnet architecture, APT28 group activities and the VPNFilter Botnet is demonstrated.	○
Evil Twin	Shrivastava et al. [75] 2020	SDN enable Wi-Fi	Access point algorithm	The distribution of IP-prefix by LAP is utilized to detect and mitigate evil twin attack.	•
	Agarwal et al. [76], 2018	802.11 Wi-Fi Network	IDS Sniffer	The proposed IDS sniffs the association request frame, if only one response is obtained there is no attack and if there are two responses, there is a Evil Twin attack.	•
Cyber Bullying	Kopecký et al. [77] 2017	Teachers	Online questionnaire	A research on cyber bullying targeting primary and secondary school teachers is carried by a polling conducted through online questionnaire.	○
	Zambrano et al. [78], 2021	Twitter	Machine learning	The modelling of different stages or seasons of a lifecycle of cyberbullying associated with social engineering is determined that will allow identifying patterns of malicious behaviour online.	•
Cyber Grooming	Haider et al. [79], 2018	Social network	Data mining, Machine learning	A detection phase utilising automated methods to identify and classify attacks, conduct digital forensic investigations.	⊛
	Rybnicek et al. [80], 2013	Facebook	Facebook Watchdog	A research agenda for a Facebook Watchdog application that detect the cyberbullying, stalking and online grooming.	•
	Zambrano et l. [81], 2019	Social engineering	Machine learning	A Latent Dirichlet Allocation (LDA) to determine the stages of attack detected using a linear model trained on a database of real cyberpedophile chats.	•

Note: • ——-> Yes ○ ——> No ⊛ ——> Partially

Table 7. Security attacks and proposed solutions in various environments.

Study (Year)	Attack	Environment	Proposed Solution
Wen et al. [53], 2023	Phishing	Ethereum	• Phishing detection framework using feature engineering. • Four phishing hiding framework and greedy method are combined.
Zheng et al. [55], 2023	Phishing	Ethereum	• A dynamic graph classifier learning evolving behaviour from transaction evolution graphs. • TEGDetector catches both the spatial and temporal evolutions of transactions.
Huang et al. [56], 2024	Phishing	Ethereum	• Node features are augmented using structure features, transaction features, and interaction intensity. • Key information is retained and introduction of noise is reduced using a graph-level representation.
Valecha et al. [57], 2021	Phishing	Email	• Gain, loss, and combined persuasion cues are used to train three machine learning models.
Ojha et al. [64], 2021	Malware	Wireless Sensor Network	• Quarantine and vaccination techniques are aggregated to form a mathematical model. • Calculation of cut-off limit of node density and communication radius determines the extent of malware.
Wang et al. [66], 2021	Spam	Email	• An evolution game model is proposed for multiple attackers and defenders.
Saad et al. [67], 2021	Spam	Blockchain memory pool	• Memory pools and Blockchain-based cryptocurrencies are targeted by a new form of attack. • A countermeasure is proposed to optimize mempool size and minimize the effects of DoS attacks caused by spam transactions.
Haber et al. [60], 2021	Identity Theft	Identity Governance	• A permission-controlled DLT is proposed to store account and identity information.
Alterkav et al. [70], 2021	Account Hijacking	Social Network	• Features from a Twitter-based dataset are analyzed using the XGBoost algorithm. • A framework is proposed to verify hijacking of social media accounts due to human error.
Punkamol et al. [61], 2020	Profile Cloning	Social Network	• User profiles, friend and follower networks, and posting behaviours are analyzed to detect account cloning in online social networks.
Alsaffar et al. [62], 2022	Cross Site Scripting	-	• Locating extraordinary XSS vulnerabilities using environment-friendly algorithms. • Pre-approved XSS vulnerability scanning generates a complete internet resource map.
Ayeni et al. [71], 2018	Cross Site Scripting	Web applications	• Classic XSS weaknesses are detected using a method based on fuzzy logic.
Marashdih et al. [72]	Cross Site Scripting	Web applications	• An algorithm is proposed to improve static analysis for detecting XSS vulnerabilities.
Shrivastava et al. [75], 2020	Evil Twin	SDN enable Wi-Fi	• "EvilScout," an evil twin detection and mitigation framework, utilizes information on IP-prefix distribution by the LAP.
Agarwal et al. [76], 2018	Evil Twin	802.11 Wi-Fi Network	• The proposed IDS sniffs the association request frame to identify Evil Twin attacks.
Zambrano et al. [78], 2021	Cyber Bullying	Twitter	• Topic modeling is used to train a cyberbullying life cycle model. • Stages of attacks are conceptualized based on criteria associated with computer attacks.
Haider et al. [79], 2018	Cyber Grooming	Social Network	• Identification and classification of attacks are done using automated methods. • Digital forensic investigation is carried out.
Rybnicek et al. [80], 2013	Cyber Grooming	Facebook	• A Facebook Watchdog application detects cyberbullying, stalking, and online grooming.
Zambrano et al. [81], 2019	Cyber Grooming	Social Engineering	• Latent Dirichlet Allocation (LDA) determines attack stages from a database of real cyberpedophile chats.

Table 8. Security attacks with their occurrence in real-world.

Attack Name	Details of Attack	Impact of Attack
Phishing Attack	Google Docs in 2017 [101]	OAuth authentication granting access to millions of Google accounts to the attacker.
Malware	WannaCry ransomware attack in 2017 [102]	2,00,000 Computers around 150 countries lost their data.
Spam	Spamhaus in 2013 [103]	DDoS attack peaking at 300 Gbps disrupting their operations.
Cross Site Scripting	Samy Worm Attack in 2005 [104]	Infected over 1 Million MySpace profiles creating endless loops.
Cyber Bullying	Amanda Todd in 2012 [105]	Attacker got access to personal information of Amanda and shared it with her contacts.
Identity Theft	Equifax Data Breach [106]	Attacker got access to social security numbers and other details of 147 million people.

and Blockchain technology that ensures access to social media by the authentic user only and gives a tough challenge to hackers who carry various attacks on social media networks. DP-BFL is a differentially private Blockchain-based explainable FL framework harnessing the power of the evolving social media 3.0 networks. The framework is able to defend against limited malicious attacks, which may need to be improved when dealing with targeted attacks. Contemporary attacks are employed to get access to the victim's social media account [50].

3.2 Next-Generation Technologies-enabled Secure Future Communication Service Scenario

In this subsection, we propose a Next-Generation Technologies-enabled Secure Future Communication Service Scenario for Social-Media 3.0 and Smart Environment. An overview of the proposed service scenario is shown in Figure 10, and it consists of four intelligent layers: connection intelligence, edge intelligence, fog intelligence, and cloud intelligence. Details of all Intelligent layers are as follows with step by step:

- **Connection Intelligent Layer**: In this layer, various AIoT sensors and social media 3.0-related devices are available, which are utilized in smart environment applications such as smart homes, smart parking, smart transportation, smart vehicular networks, and others $\{SCA_1, SCA_2, SCA_3, ...\}$. This layer basically has two objectives: data collection, which is done by an IoT sensor and smart media 3.0, and device authentication. When any IoT sensor device is leveraged in a smart environment application, it is first verified and validated by specified application administrators with certificate-based mutual authentication. Identity information is stored in the Blockchain ledger after verifying and validating the AIoT sensor devices and social media 3.0 devices. Then, the generated data is transferred to the second layer.

- **Edge Intelligent Layer**: At this layer, various base stations are available to process the data of the smart environment application with leverages emerging next-generation technologies such as Federated Learning, Blockchain, 6G, and Digital Twin at the second layer (edge intelligent layer) and use ML-based Virtual and Distributed Ledger Model. Digital Twin is utilized to provide a virtual environment for Smart Environment applications. The local model takes the input from IoT sensor devices and outputs the gradient values. This output is transferred as 6G communication to the Global Model. At this layer, we can optimize data with an ML-based Virtual Model of a smart environment, and high-priority data can communicate to the upper layer via 6G.

- **Fog Intelligent Layer**: At this layer, we use a global model with Blockchain technology for data aggregation and authentication. After aggregating the gradient values of all local models, they are transferred to the Blockchain network, and they are verified and validated with advanced consensus algorithms of Blockchain Technology, such as Proof of Authentication, Proof of Availability, and others. After getting the authenticate gradient values of the smart environment application data, it is downloaded by all local models with 6G. Then, this smart environment data is transferred to the cloud intelligent layer.

- **Cloud Intelligent Layer**: We leveraged Distributed Hash Table-based Decentralized data centers at the cloud intelligent layer. Various data centers are connected to each other in a distributed manner and store smart environment applications' data intelligently. With the help of DHT, we can offer secure and decentralized storage. After that, we can use Deep Learning

for futuristic prediction of Smart Environment Applications data.

Social media 3.0 comprises modern social-engaging platforms like Twitter and Instagram, which provide many options for adding content about your interests and the activities you are involved in in your day-to-day life. Apart from that, the profiles include some private information that should not be disclosed to strangers who may, in turn, benefit from the sensitive information to harm the account holder. Also, many advertising agencies use the individual's information, such as his likes or dislikes and areas of interest, unauthorized access of SM accounts, whereas we propose to use federated learning to train the models used to provide a customized platform experience to the account holder. Instead of sending the raw data recorded, we will train a local model to be sent to a server where a Global model will be formed after aggregating many such local models received from various nodes. Blockchain for the security of the SM account, as the information to be added to the SM account will be verified by the miners against the proof of work consensus algorithm, ensuring the authenticity of the individual trying to add the information to the said account. This approach restricts the during transmission. All such outsiders may cause harm to the account holder as they have access to the private information of the individual. Thus, we propose the use of to provide personalized suggestions regarding some products or services. For this recommendation, they train a model by sending data to a centralized location, which makes the data prone to various cyber-attacks encountered on the network during transmission. All such outsiders may cause harm to the account holder as they have access to the private information of the individual. Thus, we propose the use of Blockchain for the security of the SM account, as the information to be added to the SM account will be verified by the miners against the proof of work consensus algorithm, ensuring the authenticity of the individual trying to add the information to the said account. This approach restricts the unauthorized access of SM accounts, whereas we propose to use federated learning to train the models used to provide a customized experience of the platform to the account holder. Instead of sending the raw data recorded, we will train a local model to be sent to a server where a Global model will be formed after aggregating many such local models received from various nodes.

4 Open Research Issues and Future Work

The user data generated by SE is vulnerable to security and privacy breaches. Also, the involvement of social media accessed through nodes forming a SE further worsens the situation. This scenario provokes research in the security and privacy of social media networks in SE against sophisticated attacks, including contemporary and targeted attacks. The competence of Blockchain technology and Federated learning can be employed to detect and defend the SM from newly prevailing attacks when connected to SE. In the future, we will analyze the data shared by SM networks in SE and methods of exploiting the collected data to pursue security and privacy breaches. We will also introduce a framework to defend and detect possible attacks on SE nodes connected to SM networks. Table 7 includes open research challenges with their proposed solutions.

4.1 Privacy Preservation

Privacy is one of the major concerns in SE, where all the nodes are connected to the outside world through the internet, and this may compromise the privacy of confidential data of those in contact with the nodes. Blockchain, which is an end-to-end encryption, can prove to be a promising solution to this problem [82, 83]. Currently, very few attempts have been made to utilize Blockchain for social media privacy preservation. As the cost of the Proof of Work (PoW) consensus algorithm is quite high and tedious, there is a need to solve this trade-off between the cost and reward paid to the miner. The performance of these two solutions in the presence of SE is to be analyzed to ensure the privacy of the personal data of the users using Social media in coordination with SE.

4.2 Centralization

The centralization of all the user data has proven to be a huge threat to the failure of single-point problems and a risk to the security of the private data at the central unit dealing with the consolidated data. Security attacks at a single point are quite easy for the attacker to carry out and get access to the data; this issue needs attention when SE is considered with nodes having access to SM. Thus, centrally training models can threaten the security of the central node responsible for training the model. This gives rise to the need to adopt Federated learning, which allows the training of local modes at the nodes, gathering data, and then transmitting their trained local model to the central server instead of the raw data. Thus, avoiding the transmission of raw data solves the problem of

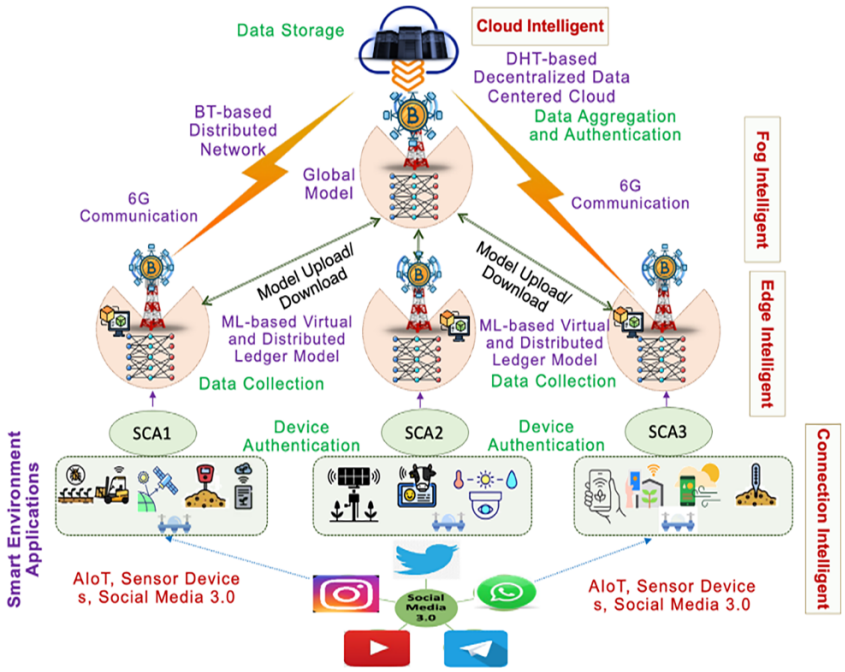

Figure 10. Overview of Next-Generation Technologies-enabled Secure Future Communication Service Scenario.

centralization. Application of Federated learning in SM can prove promising for those training their models from the data gathered from SM accounts of users for recommendation systems and personalized advertising agencies without compromising the privacy of their customers present over SM [84].

4.3 Trust Management

Building the SM account holders' trust and retaining it for their continuation in using the platform required many factors to be considered to build a trustworthy platform that can be relied upon when users' private data is in the picture. It requires the implementation of multiple technologies like end-to-end encryption, Blockchain, Federated learning, SHA-3 hashing, SDN, Graph classifiers for detecting possible threats, and IDPS that continuously scan the system for potential threats that try to intrude and steal the data of the SM accounts.

4.4 Cyberbullying

Cyberbullying has been in existence since the very beginning of electronic communication, and with the development of more involving and alluring SM platforms, it has grown to become one of the most feared threats to the personal data of users. The contemporary attacks discussed in Section 3 can severely affect the trust and reliance of a user on the SM platform, thus adversely affecting the businesses of this platform and questioning the platform's credibility. Thus, a sophisticated SDN capable of detecting potential hackers seeking access to private data using various attacks must be built. SDN using more advanced machine learning technologies to identify the attacks, such as deep learning and federated learning, can be devised to identify any attack encountered [85]. Integration of such SDN in SE, specifically for SM-enabled nodes, is a big point of concern for the researchers.

4.5 Authentication and Access Control

The primary method of gaining access to the victim's SM account is to get the victim's credentials to surpass the account's initial authentication phase. This method is the basic method of getting access of the victim's account without any alarm driven for breaching of security layers. Thus, the authentication phase of the account is to be inculcated with new techniques involving modern biometric authentication technologies such as face recognition, retina scanning, fingerprint, scanners, RFID, etc. [86, 87]. Following authentication, further layers of security for acquiring deeper access to the account must be set up using access control mechanisms like Role-based access control, Attribute-based access control [88], and many more.

4.6 Data Security

Data security is the foundation of a safe SM platform as gaining more users is the key to the increase in users of the platform, which is directly proportional to the security features provided by the platform, which will gain the confidence of the users to create and access the

Table 9. Possible Solutions for Challenges to the Security of Social Media and Smart Environment.

Possible Solutions	Privacy Preservation	Centralization	Trust Management	Cyberbullying	Authentication and Access Control	Data Security	Regulatory Compliance	Real-Time Monitoring
End-to-End Encryption	✓		✓		✓	✓		
Channelized Blockchain	✓		✓		✓	✓		✓
SHA-3 Hashing	✓		✓			✓		
Federated Learning	✓	✓				✓		
SDN			✓	✓	✓	✓		
Graph Classifier	✓		✓	✓	✓			
SDLC							✓	
DLT		✓			✓			✓
IDPS			✓		✓			✓

accounts on such platforms. Thus, secured delivery of their sent messages, restricting unauthorized access to their account through human prevailed errors and also through advertising agencies gaining access to the account holder's personal information on the pretext of studying his likes or dislikes, hobbies, friends, and locations is of utmost concern. End-to-end encryption, Blockchain, and SHA-3 Hashing algorithms are promising solutions to these issues. Whereas Federated learning promises decentralized model training to ensure private data security. SDN and Graph classifiers are more sophisticated solutions for premium accounts belonging to known figures that are mostly on target of the attackers to peep inside the personal lives of well-known social figures and political personals [82–84].

4.7 Regulatory Compliance

Privacy preservation and maintaining the security of the system and data involved in the system is a continuous process to be done during the entire life cycle of software development. The development of every module passes through certain phases during the entire life cycle, where the developer can easily determine the possible attacks that could be carried on that particular module. The prior knowledge of these potential threats can be used to implement security measures during the development phases itself. These precautionary measures can lead to secure software development that could detect certain attacks on its own when commercially launched to give services to end users. Thus, privacy-preserving and secure software with its built-in SDN can prevent software users from possible attacks. Thus, security measures inculcated in SDLC are a promising solution to embed Regulatory compliance in SDLC [89].

4.8 Real-Time Monitoring

Security breaches and malicious activities have become highly frequent and continuous activities carried out by hackers worldwide 24×7. This makes SM accounts more prone as they provide personal and confidential data of the account holder along with his hobbies, professional and personal activities, and geographic locations. In this scenario, it becomes necessary to continuously monitor the SM accounts to detect ongoing attacks on the accounts. Blockchain is a distributed ledger technology where the blocks are added to the chain only after the approval of all the participants in the network; this makes it difficult for an attacker to modify any block, as every change in the block is notified to all the network participants. Miners worldwide work around the clock to provide proof of work consensus to the network, which makes the Blockchain a preferable solution to the need for real-time monitoring [82]. Distributed ledger technology can be used to store information in a decentralized format, which can diminish the attack at a single point. Fake news and deepfakes can be identified using DLT earlier and removed from SM to avoid circulating such fake information [90, 95, 96, 110–114]. Intrusion detection and prevention are also necessary for real-time network surveillance to identify and prevent potentially harmful attacks on SM [115–118].

5 Conclusion

In this article, we reviewed and proposed Next-Generation Technologies for Secure Future Communication Service Scenario for Smart Environment and Social-Media 3.0. A certificate-based mutual authentication mechanism is utilized at the first intelligent layer for IoT sensor device authentication. Federated Learning is leveraged at the second and third intelligent layers for privacy preservation of the smart environment's data, and the virtual environment is offered by digital twin technology at the second layer. Blockchain networks store identity information of all IoT sensor devices in a smart environment, and an advanced consensus algorithm is used for data or gradient values of global model authentication. After authentication of the gradient values, the local model downloaded these values and transferred smart environment application data to the cloud intelligent layer for decentralized storage via the Distributed Hash Table. 6G communication offers high-definition connectivity for Smart Environments. The utilization of Federated Learning for local models trained at heterogeneous Smart Ecosystems aggregated to form global model enhances security by forbidding transmission of raw data from various devices incorporated within the network. The use of Blockchain for authentication prevents unauthorized access to the information communicated within the network by illegitimate users. In the future, we will evaluate the proposed service scenario for Smart Environment and Social Media 3.0 with advanced version Algorithms and methodology of emerging next-generation technologies.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

This research was supported by the Research Seed Grant funded by the Marwadi University, Rajkot, Gujarat (MU/R&D/22- 23/MRP/FT13).

References

[1] Chin, J., Callaghan, V., & Allouch, S. B. (2019). The Internet-of-Things: Reflections on the past, present and future from a user-centered and smart environment perspective. *Journal of Ambient Intelligence and Smart Environments*, 11(1), 45-69.

[2] Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE consumer electronics magazine*, 5(3), 60-70. [CrossRef]

[3] Pantano, E., & Timmermans, H. (2014). What is smart for retailing?. *Procedia Environmental Sciences*, 22, 101-107. [CrossRef]

[4] Ikrissi, G., & Mazri, T. (2021). IOT-based Smart Environments: State of the art, security threats and solutions. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 46, 279-286.

[5] Popescul, D., & Genete, L. D. (2016). Data security in smart cities: challenges and solutions. *Informatica Economică*, 20(1).

[6] Patrono, L., Atzori, L., Šolić, P., Mongiello, M., & Almeida, A. (2020). Challenges to be addressed to realize Internet of Things solutions for smart environments. *Future generation computer systems*, 111, 873-878. [CrossRef]

[7] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, 88, 173-190. [CrossRef]

[8] Theodorou, S., & Sklavos, N. (2019). Blockchain-based security and privacy in smart cities. In *Smart cities cybersecurity and privacy* (pp. 21-37). Elsevier. [CrossRef]

[9] Majeed, U., Khan, L. U., Yaqoob, I., Kazmi, S. A., Salah, K., & Hong, C. S. (2021). Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *Journal of Network and Computer Applications*, 181, 103007. [CrossRef]

[10] Michelin, R. A., Dorri, A., Steger, M., Lunardi, R. C., Kanhere, S. S., Jurdak, R., & Zorzo, A. F. (2018, November). SpeedyChain: A framework for decoupling data from blockchain for smart cities. In *Proceedings of the 15th EAI international conference on mobile and ubiquitous systems: Computing, networking and services* (pp. 145-154). [CrossRef]

[11] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, 88, 101653. [CrossRef]

[12] Pandya, S., Srivastava, G., Jhaveri, R., Babu, M. R., Bhattacharya, S., Maddikunta, P. K. R., ... & Gadekallu, T. R. (2023). Federated learning for smart cities: A comprehensive survey. *Sustainable Energy Technologies and Assessments*, 55, 102987. [CrossRef]

[13] Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., ... & He, B. (2021). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*, 35(4), 3347-3366. [CrossRef]

[14] Konečný, J. (2016). Federated Learning: Strategies for Improving Communication Efficiency. *arXiv preprint arXiv:1610.05492*. [CrossRef]

[15] Zhang, R., Xue, R., & Liu, L. (2021). Security and privacy for healthcare blockchains. *IEEE Transactions on Services Computing*, 15(6), 3668-3686. [CrossRef]

[16] Orecchini, F., Santiangeli, A., Zuccari, F., Pieroni, A., & Suppa, T. (2019). Blockchain technology in smart city: A new opportunity for smart environment and smart mobility. In *Intelligent Computing & Optimization* 1 (pp. 346-354). Springer International Publishing.

[17] Mukherjee, P., Barik, R. K., & Pradhan, C. (2021). A comprehensive proposal for blockchain-oriented smart city. *Security and Privacy Applications for Smart City Development*, 55-87.

[18] Chen, J., Gan, W., Hu, M., & Chen, C. M. (2021). On the construction of a post-quantum blockchain for smart city. *Journal of information security and applications*, 58, 102780. [CrossRef]

[19] Paul, R., Ghosh, N., Sau, S., Chakrabarti, A., & Mohapatra, P. (2021). Blockchain based secure smart city architecture using low resource IoTs. *Computer Networks*, 196, 108234. [CrossRef]

[20] Wong, P. F., Chia, F. C., Kiu, M. S., & Lou, E. C. (2022). Potential integration of blockchain technology into smart sustainable city (SSC) developments: a systematic review. *Smart and Sustainable Built Environment*, 11(3), 559-574. [CrossRef]

[21] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2), 1-19. [CrossRef]

[22] Zheng, Z., Zhou, Y., Sun, Y., Wang, Z., Liu, B., & Li, K. (2022). Applications of federated learning in smart cities: recent advances, taxonomy, and open challenges. *Connection Science*, 34(1), 1-28. [CrossRef]

[23] Sater, R. A., & Hamza, A. B. (2021). A federated learning approach to anomaly detection in smart buildings. *ACM Transactions on Internet of Things*, 2(4), 1-23. [CrossRef]

[24] Yang, Z., Chen, M., Wong, K. K., Poor, H. V., & Cui, S. (2022). Federated learning for 6G: Applications, challenges, and opportunities. Engineering, 8, 33-41. [CrossRef]

[25] Huang, X., Li, P., Yu, R., Wu, Y., Xie, K., & Xie, S. (2021). FedParking: A federated learning based parking space estimation with parked vehicle assisted edge computing. IEEE Transactions on Vehicular Technology, 70(9), 9355-9368. [CrossRef]

[26] Li, D., Luo, Z., & Cao, B. (2022). Blockchain-based federated learning methodologies in smart environments. *Cluster Computing*, 25(4), 2585-2599.

[27] Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. Computers & Industrial Engineering, 149, 106854. [CrossRef]

[28] Chai, H., Leng, S., Chen, Y., & Zhang, K. (2020). A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(7), 3975-3986. [CrossRef]

[29] Kuang, Z., & Chen, C. (2023). Research on smart city data encryption and communication efficiency improvement under federated learning framework. *Egyptian Informatics Journal*, 24(2), 217-227. [CrossRef]

[30] Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., ... & Liu, Y. (2020). Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet of Things Journal*, 8(3), 1817-1829. [CrossRef]

[31] Albaseer, A., Ciftler, B. S., Abdallah, M., & Al-Fuqaha, A. (2020, June). Exploiting unlabeled data in smart cities using federated edge learning. In *2020 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 1666-1671). IEEE. [CrossRef]

[32] Otoum, S., Al Ridhawi, I., & Mouftah, H. (2021). Securing critical IoT infrastructures with blockchain-supported federated learning. *IEEE Internet of Things Journal*, 9(4), 2592-2601.[CrossRef]

[33] Jie, W., Qiu, W., Koe, A. S. V., Li, J., Wang, Y., Wu, Y., & Li, J. (2023). A Secure and Flexible Blockchain-Based Offline Payment Protocol. *IEEE Transactions on Computers*. [CrossRef]

[34] Demertzis, K. (2021). Blockchained federated learning for threat defense. *arXiv preprint arXiv:2102.12746*. [CrossRef]

[35] Yuan, X., Chen, J., Yang, J., Zhang, N., Yang, T., Han, T., & Taherkordi, A. (2022). Fedstn: Graph representation driven federated learning for edge computing enabled urban traffic flow prediction. *IEEE Transactions on Intelligent Transportation Systems*, 24(8), 8738-8748. [CrossRef]

[36] Ahmed, S. T., & Jeong, J. (2024). Heterogeneous Workload based Consumer Resource Recommendation Model for Smart Cities: eHealth Edge-Cloud Connectivity Using Federated Split Learning. *IEEE Transactions on Consumer Electronics*. [CrossRef]

[37] Qi, Y., Hossain, M. S., Nie, J., & Li, X. (2021). Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Generation Computer Systems*, 117, 328-337. [CrossRef]

[38] Farooq, K., Syed, H. J., Alqahtani, S. O., Nagmeldin, W., Ibrahim, A. O., & Gani, A. (2022). Blockchain federated learning for in-home health monitoring. *Electronics*, 12(1), 136. [CrossRef]

[39] Ayaz, F., Sheng, Z., Tian, D., & Guan, Y. L. (2021). A blockchain based federated learning for message dissemination in vehicular networks. *IEEE Transactions on Vehicular Technology*, 71(2), 1927-1940. [CrossRef]

[40] Yang, Z., Shi, Y., Zhou, Y., Wang, Z., & Yang, K. (2022). Trustworthy federated learning via blockchain. *IEEE Internet of Things Journal*, 10(1), 92-109. [CrossRef]

[41] Liu, H., Zhang, S., Zhang, P., Zhou, X., Shao, X., Pu, G.,

& Zhang, Y. (2021). Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. *IEEE Transactions on Vehicular Technology*, 70(6), 6073-6084. [CrossRef]

[42] Wang, R., & Tsai, W. T. (2022). Asynchronous federated learning system based on permissioned blockchains. *Sensors*, 22(4), 1672. [CrossRef]

[43] Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z., & Yan, Q. (2020). A blockchain-based decentralized federated learning framework with committee consensus. *IEEE Network*, 35(1), 234-241. [CrossRef]

[44] Lu, Y., Huang, X., Zhang, K., Maharjan, S., & Zhang, Y. (2020). Blockchain and federated learning for 5G beyond. *IEEE Network*, 35(1), 219-225. [CrossRef]

[45] Zhang, W., Lu, Q., Yu, Q., Li, Z., Liu, Y., Lo, S. K., ... & Zhu, L. (2020). Blockchain-based federated learning for device failure detection in industrial IoT. *IEEE Internet of Things Journal*, 8(7), 5926-5937. [CrossRef]

[46] Awan, S., Li, F., Luo, B., & Liu, M. (2019, November). Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (pp. 2561-2563). [CrossRef]

[47] Hua, G., Zhu, L., Wu, J., Shen, C., Zhou, L., & Lin, Q. (2020). Blockchain-based federated learning for intelligent control in heavy haul railway. *IEEE Access*, 8, 176830-176839. [CrossRef]

[48] Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5), 2157-2177.

[49] Etuh, E., & Bakpo, F. S. (2022). Social Media Networks Attacks and their Preventive Mechanisms: A Review. *arXiv preprint arXiv:2201.03330*. [CrossRef]

[50] Salim, S., Turnbull, B., & Moustafa, N. (2021). A blockchain-enabled explainable federated learning for securing internet-of-things-based social media 3.0 networks. *IEEE Transactions on Computational Social Systems*. [CrossRef]

[51] Dubai Blockchain Policy. (2022). *DIGITAL DUBAI*. https://www.digitaldubai.ae/docs/default source/publications/ dubaiblockchainpolicy.pdf?sfvrsn=4a4bb396_4

[52] Faruk, M. J. H., Shahriar, H., Valero, M., Barsha, F. L., Sobhan, S., Khan, M. A., ... & Wu, F. (2021, December). Malware detection and prevention using artificial intelligence techniques. In *2021 IEEE international conference on big data (big data)* (pp. 5369-5377). IEEE. [CrossRef]

[53] Wen, H., Fang, J., Wu, J., & Zheng, Z. (2022). Hide and seek: An adversarial hiding approach against phishing detection on ethereum. *IEEE Transactions on Computational Social Systems*, 10(6), 3512-3523. [CrossRef]

[54] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, 76, 139-154.

[55] Zheng, H., Ma, M., Ma, H., Chen, J., Xiong, H., & Yang, Z. (2023). Tegdetector: a phishing detector that knows evolving transaction behaviors. *IEEE Transactions on Computational Social Systems*. [CrossRef]

[56] Huang, H., Zhang, X., Wang, J., Gao, C., Li, X., Zhu, R., & Ma, Q. (2024). PEAE-GNN: Phishing Detection on Ethereum via Augmentation Ego-Graph Based on Graph Neural Network. *IEEE Transactions on Computational Social Systems*. [CrossRef]

[57] Valecha, R., Mandaokar, P., & Rao, H. R. (2021). Phishing email detection using persuasion cues. *IEEE transactions on Dependable and secure computing*, 19(2), 747-756. [CrossRef]

[58] Duman, S., Büchler, M., Egele, M., & Kirda, E. (2023). PellucidAttachment: Protecting users from attacks via e-mail attachments. *IEEE Transactions on Dependable and Secure Computing*, 21(3), 1342-1354. [CrossRef]

[59] Rao, S., Verma, A. K., & Bhatia, T. (2021). A review on social spam detection: Challenges, open issues, and future directions. *Expert Systems with Applications*, 186, 115742. [CrossRef]

[60] Haber, M. J., & Rolls, D. (2019). *Identity attack vectors: implementing an effective identity and access management solution*. Apress.

[61] Punkamol, D., & Marukatat, R. (2020, March). Detection of account cloning in online social networks. In *2020 8th International Electrical Engineering Congress (iEECON)* (pp. 1-4). IEEE. [CrossRef]

[62] Alsaffar, M., Aljaloud, S., Mohammed, B. A., Al-Mekhlafi, Z. G., Almurayziq, T. S., Alshammari, G., & Alshammari, A. (2022). Detection of Web Cross-Site Scripting (XSS) Attacks. *Electronics*, 11(14), 2212. [CrossRef]

[63] Muñoz, F., Isaza, G., & Castillo, L. (2020, June). Smartsec4cop: smart cyber-grooming detection using natural language processing and convolutional neural networks. In *International Symposium on Distributed Computing and Artificial Intelligence* (pp. 11-20). Cham: Springer International Publishing.

[64] Ojha, R. P., Srivastava, P. K., Sanyal, G., & Gupta, N. (2021). Improved model for the stability analysis of wireless sensor network against malware attacks. *Wireless Personal Communications*, 116(3), 2525-2548.

[65] Zhao, K., Zhou, H., Zhu, Y., Zhan, X., Zhou, K., Li, J., ... & Luo, X. (2021, November). Structural attack against graph based android malware detection. In *Proceedings of the 2021 ACM SIGSAC conference on computer and communications security* (pp. 3218-3235). [CrossRef]

[66] Wang, M., & Song, L. (2021). Efficient defense strategy against spam and phishing email: An evolutionary game model. *Journal of Information Security and Applications*, 61, 102947. [CrossRef]

[67] Saad, M., Kim, J., Nyang, D., & Mohaisen, D. (2021). Contra-∗: Mechanisms for countering spam attacks on blockchain's memory pools. *Journal of Network and Computer Applications*, 179, 102971. [CrossRef]

[68] Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009, April). All your contacts are belong to us: automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web* (pp. 551-560). [CrossRef]

[69] Daraghmi, E., Jayousi, S., Daraghmi, Y., Daraghmi, R., & Fouchal, H. (2024). Smart Contracts for Managing the Agricultural Supply Chain: A Practical Case Study. *IEEE Access*. [CrossRef]

[70] Alterkavı, S., & Erbay, H. (2021). Design and analysis of a novel authorship verification framework for hijacked social media accounts compromised by a human. *Security and Communication Networks*, 2021(1), 8869681. [CrossRef]

[71] Ayeni, B. K., Sahalu, J. B., & Adeyanju, K. R. (2018). Detecting Cross-Site Scripting in Web Applications Using Fuzzy Inference System. *Journal of Computer Networks and Communications*, 2018(1), 8159548. [CrossRef]

[72] Marashdih, A. W., Zaaba, Z. F., Suwais, K., & Mohd, N. A. (2019). Web application security: An investigation on static analysis with other algorithms to detect cross site scripting. *Procedia Computer Science*, 161, 1173-1181. [CrossRef]

[73] Rivera, R., Pazmiño, L., Becerra, F., & Barriga, J. (2022). An analysis of cyber espionage process. In *Developments and Advances in Defense and Security: Proceedings of MICRADS 2021* (pp. 3-14). Springer Singapore.

[74] Bederna, Z., & Szadeczky, T. (2020). Cyber espionage through Botnets. *Security Journal*, 33(1), 43-62.

[75] Shrivastava, P., Jamal, M. S., & Kataoka, K. (2020). EvilScout: Detection and mitigation of evil twin attack in SDN enabled WiFi. *IEEE Transactions on Network and Service Management*, 17(1), 89-102. [CrossRef]

[76] Agarwal, M., Biswas, S., & Nandi, S. (2018). An efficient scheme to detect evil twin rogue access point attack in 802.11 Wi-Fi networks. *International Journal of Wireless Information Networks*, 25, 130-145.

[77] Kopecký, K., & Szotkowski, R. (2017). Cyberbullying, cyber aggression and their impact on the victim–The teacher. *Telematics and informatics*, 34(2), 506-517. [CrossRef]

[78] al-Khateeb, H. M., & Epiphaniou, G. (2016). How technology can mitigate and counteract cyber-stalking and online grooming. *Computer Fraud & Security*, 2016(1), 14-18. [CrossRef]

[79] Rybnicek, M., Poisel, R., & Tjoa, S. (2013, October). Facebook watchdog: a research agenda for detecting online grooming and bullying activities. In *2013 IEEE International Conference on Systems, Man, and Cybernetics* (pp. 2854-2859). IEEE. [CrossRef]

[80] Young, A., & Verhulst, S. (2020). Zug Digital ID: Blockchain Case Study for Government Issued Identity. Consensys. https://consensys.io/blockchain-use-cases/government-and-the-public-sector/zug

[81] Zambrano, P., Torres, J., Tello-Oquendo, L., Jácome, R., Benalcazar, M. E., Andrade, R., & Fuertes, W. (2019). Technical mapping of the grooming anatomy using machine learning paradigms: An information security approach. *IEEE Access*, 7, 142129-142146. [CrossRef]

[82] Zhan, Y., Xiong, Y., & Xing, X. (2023). A conceptual model and case study of blockchain-enabled social media platform. Technovation, 119, 102610. [CrossRef]

[83] Basem, O., Ullah, A., & Hassen, H. R. (2022). Stick: an end-to-end encryption protocol tailored for social network platforms. *IEEE Transactions on Dependable and Secure Computing*, 20(2), 1258-1269. [CrossRef]

[84] Zhou, X., Liang, W., Ma, J., Yan, Z., Kevin, I., & Wang, K. (2022). 2D federated learning for personalized human activity recognition in cyber-physical-social systems. *IEEE Transactions on Network Science and Engineering*, 9(6), 3934-3944. [CrossRef]

[85] Krishnan, P., Jain, K., Jose, P. G., Achuthan, K., & Buyya, R. (2021). SDN enabled QoE and security framework for multimedia applications in 5G networks. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 17(2), 1-29. [CrossRef]

[86] Wati, V., Kusrini, K., Al Fatta, H., & Kapoor, N. (2021). Security of facial biometric authentication for attendance system. *Multimedia Tools and Applications*, 80(15), 23625-23646.

[87] Mbarek, B., Ge, M., & Pitner, T. (2020). An efficient mutual authentication scheme for internet of things. *Internet of things*, 9, 100160. [CrossRef]

[88] El Sibai, R., Gemayel, N., Bou Abdo, J., & Demerjian, J. (2020). A survey on access control mechanisms for cloud computing. *Transactions on Emerging Telecommunications Technologies*, 31(2), e3720. [CrossRef]

[89] Kempe, E., & Massey, A. (2021, September). Perspectives on regulatory compliance in software engineering. In *2021 IEEE 29th International Requirements Engineering Conference (RE)* (pp. 46-57). IEEE. [CrossRef]

[90] Fraga-Lamas, P., & Fernandez-Carames, T. M. (2020). Fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. *IT professional*, 22(2), 53-59. [CrossRef]

[91] Cohn, J. M., Finn, P. G., Nair, S. P., Panikkar, S. B., & Pureswaran, V. S. (2019). US Patent No. 10,257,270.

[92] Sengan, S., Subramaniyaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., & Ravi, L. (2020). Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public

data-smart network. *Future generation computer systems*, 112, 724-737. [CrossRef]

[93] Singh, S. K., Jeong, Y. S., & Park, J. H. (2020). A deep learning-based IoT-oriented infrastructure for secure smart city. *Sustainable Cities and Society*, 60, 102252. [CrossRef]

[94] Ali, Z., Chaudhry, S. A., Ramzan, M. S., & Al-Turjman, F. (2020). Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles. *IEEE Access*, 8, 43711-43724. [CrossRef]

[95] Park, J. H., Yotxay, S., Singh, S. K., & Park, J. H. (2024). PoAh-Enabled Federated Learning Architecture for DDoS Attack Detection in IoT Networks. *Human-Centric Computing And Information Sciences*, 14. [CrossRef]

[96] Singh, S. K., Azzaoui, A. E., Choo, K. K. R., Yang, L. T., & Park, J. H. (2023). Articles A Comprehensive Survey on Blockchain for Secure IoT-enabled Smart City beyond 5G: Approaches, Processes, Challenges, and Opportunities. *Hum.-Centric Comput. Inf. Sci*, 13, 51. [CrossRef]

[97] Al Dakheel, J., Del Pero, C., Aste, N., & Leonforte, F. (2020). Smart buildings features and key performance indicators: A review. *Sustainable Cities and Society*, 61, 102328. [CrossRef]

[98] Fantin Irudaya Raj, E., & Appadurai, M. (2022). Internet of things-based smart transportation system for smart cities. In *Intelligent Systems for Social Good: Theory and Practice* (pp. 39-50). Singapore: Springer Nature Singapore.

[99] Sinha, B. B., & Dhanalakshmi, R. (2022). Recent advancements and challenges of Internet of Things in smart agriculture: A survey. *Future Generation Computer Systems*, 126, 169-184. [CrossRef]

[100] Bourg, L., Chatzidimitris, T., Chatzigiannakis, I., Gavalas, D., Giannakopoulou, K., Kasapakis, V., ... & Zaroliagis, C. (2023). Enhancing shopping experiences in smart retailing. *Journal of Ambient Intelligence and Humanized Computing*, 1-19.

[101] Mohamed, G., Visumathi, J., Mahdal, M., Anand, J., & Elangovan, M. (2022). An effective and secure mechanism for phishing attacks using a machine learning approach. *Processes*, 10(7), 1356. [CrossRef]

[102] Aljaidi, M., Alsarhan, A., Samara, G., Alazaidah, R., Almatarneh, S., Khalid, M., & Al-Gumaei, Y. A. (2022, November). NHS WannaCry ransomware attack: technical explanation of the vulnerability, exploitation, and countermeasures. In *2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)* (pp. 1-6). IEEE. [CrossRef]

[103] Thangavel, S., & Kannan, S. (2022). Detection and trace back of low and high volume of distributed denial-of-service attack based on statistical measures. *Concurrency and Computation: Practice and Experience*, 34(8), e5428. [CrossRef]

[104] Wang, D., Webb, S., Lee, K., Caverlee, J., & Pu, C. (2023). Granular computing system vulnerabilities: Exploring the dark side of social networking communities. In *Granular, Fuzzy, and Soft Computing* (pp. 239-250). New York, NY: Springer US.

[105] Aisya, N. R. (2024). Cyberbullying: The Silent Epidemic of The Digital Age. *Journal of World Science*, 3(6), 691-697. [CrossRef]

[106] Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the capital one data breach: Critical lessons learned. *ACM Transactions on Privacy and Security*, 26(1), 1-29. [CrossRef]

[107] Suliman, M., & Leith, D. (2023, September). Two models are better than one: Federated learning is not private for google gboard next word prediction. In *European Symposium on Research in Computer Security* (pp. 105-122). Cham: Springer Nature Switzerland.

[108] Farahani, B., Tabibian, S., & Ebrahimi, H. (2023). Towards A Personalized Clustered Federated Learning: A Speech Recognition Case Study. *IEEE Internet of Things Journal*. [CrossRef]

[109] Brecko, A., Kajati, E., Koziorek, J., & Zolotova, I. (2022). Federated learning for edge computing: A survey. *Applied Sciences*, 12(18), 9124. [CrossRef]

[110] Singh, S. K., Kumar, M., Khanna, A., & Virdee, B. (2024). Blockchain and FL-based secure architecture for enhanced external Intrusion detection in smart farming. *IEEE Internet of Things Journal*. [CrossRef]

[111] Usman, M. T., Khan, H., Singh, S. K., Lee, M. Y., & Koo, J. (2024). Efficient deepfake detection via layer-frozen assisted dual attention network for consumer imaging devices. *IEEE Transactions on Consumer Electronics*. [CrossRef]

[112] Kumar, M., Singh, S. K., & Kim, S. (2024). Predictive Analytics for Mortality: FSRNCA-FLANN Modeling Using Public Health Inventory Records. *IEEE Access*. [CrossRef]

[113] Singh, S. K., Kumar, M., Tanwar, S., & Park, J. H. (2024). GRU-based digital twin framework for data allocation and storage in IoT-enabled smart home networks. *Future Generation Computer Systems*, 153, 391-402. [CrossRef]

[114] Jeremiah, S. R., Ha, J., Singh, S. K., & Park, J. H. ArticlesPrivacyGuard: Collaborative Edge-Cloud Computing Architecture for Attribute-Preserving Face Anonymization in CCTV Networks. [CrossRef]

[115] Khan, H., Ullah, I., Shabaz, M., Omer, M. F., Usman, M. T., Guellil, M. S., & Koo, J. (2024). Visionary vigilance: Optimized YOLOV8 for fallen person detection with large-scale benchmark dataset. *Image and Vision Computing*, 149, 105195. [CrossRef]

[116] Ullah, I., Ali, F., Khan, H., Khan, F., & Bai, X. (2024). Ubiquitous computation in internet of vehicles for human-centric transport systems. *Computers in Human Behavior*, 161, 108394. [CrossRef]

[117] Khan, H., Jan, Z., Ullah, I., Alwabli, A., Alharbi,

F., Habib, S., ... & Koo, J. (2024). A deep dive into AI integration and advanced nanobiosensor technologies for enhanced bacterial infection monitoring. *Nanotechnology Reviews*, 13(1), 20240056. [CrossRef]

[118] Singh, S. K., Lee, C., & Park, J. H. (2022). CoVAC: A P2P smart contract-based intelligent smart city architecture for vaccine manufacturing. *Computers & Industrial Engineering*, 166, 107967. [CrossRef]

Archana Kurde is currently Research Scholar in the Department of Computer Engineering at Marwadi University, Rajkot, Gujarat, India, and is pursuing a Ph.D. under the supervision of Dr. Sushil Kumar Singh from the same university. She is interested in IoT, Blockchain and Smart Environment.

Sushil Kumar Singh (Member, IEEE) is an Associate Professor in the Department of Computer Engineering at Marwadi University, Rajkot, India. He received Ph.D. degree from Seoul National University of Science and Technology, Seoul, South Korea. He received M.Tech. Degree in Computer Science and Engineering from Uttarakhand Technical University, Dehradun, India. He also received an M.E. degree in Information Technology from Karnataka State University, Mysore, India. He has also been the lab leader of the UCS Lab at the Department of Computer Science Engineering, Seoul National University of Science and Technology, Seoul, South Korea. He has received the Best Lab Leadership Award from UCS Lab for 2019-2021. He is selected in Top 2% Scientist for the (2023-2024) year as per the list compiled by Stanford University and published by Elsevier. He has more than 12 years of experience teaching in the field of computer science. He has published Four Books: Computer C Programming, Cyber Security, Big Data Analytics, and Mobile Computing. He has also published many high-quality papers (Q1, Top 10% JCR Rank) in international journals and conferences. He has already delivered international lectures in many countries. His research interests include Blockchain, Artificial Intelligence, Big Data, Internet of Things, Smart City Security, and Cyber-Physical Systems. He is an Associate/ Guest Editor in the Human-centric Computation and Information Sciences (HCIS) Journal, IEEE Journal of Biomedical and Health Informatics (IEEE JBHI) Journal, IGI Global Publication, and Wiley Scrivener Publication. He is a reviewer of the IEEE Wireless Communication Magazine, IEEE SYSTEMS, IEEE Internet of Things, FGCS, TETT, EXSY, JISA, Computer Network, MDPI, CIE, HCIS, JIPS, Computing (COMP), Multimedia Tools & Applications, and SCIS Journal. He also organizes the Research Activities Club, which promotes quality research activities among young researchers at Marwadi University, Rajkot, Gujarat, India. (Email: sushilkumar.singh@marwadieducation.edu.in)