Proceedings of the 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV-2025)
DVD Part Number: CFP25ONG-DVD; ISBN: 979-8-3315-1174-6

A BRIEF LITERATURE SURVEY ON CRYPTOGRAPHY MODELS FOR DETECTION OF CYBER ATTACKS IN INTERNET OF THINGS ENABLED SMART CITIES

Ch Sowjanya[1]
Research Scholar
Dept of CSE
RGUKT-Nuzvid
chinni1.sowji@gmail.com

D V Nagarjana Devi[2]
Assistant Professor
Dept of CSE
RGUKT-Nuzvid
devi.duvvuri@rguktn.ac.in

Abstract

Improved infrastructure, more efficient public services, and improved transit systems are all ways in which smart cities use the Internet of Things (IoT) to raise the standard of living for their residents. It is imperative that processes be put in place to meet the varied needs of the use cases as IoT-enabled smart city applications gain popularity. The likelihood of cyber assaults and breaches is rising in tandem with the proliferation of linked gadgets. In order to prevent assaults that could damage citizens and institutions, it is essential to secure these systems. But protecting the IoT environment is no easy task. As smart city infrastructures incorporate more and more IoT devices, there is a pressing need for strong cybersecurity protocols. The safety and efficiency of urban systems are at risk since these devices are open to a variety of cyberattacks. In order to detect outliers brought about by cyberattacks on the IoT in smart cities, this research analyzes numerous cryptography models that provide security to IoT enabled smart gadgets. Improving the security of IoT networks while also protecting user data is a double challenge that the analyzed approached tackles. The need to ensure the secure and dependable functioning of Internet-connected devices is growing in tandem with the quantity of these devices. For the purpose of securing data transmissions on the ever-expanding network of sensors, this research focuses on cryptographic algorithms that can be included in IoT devices. In this paper, the issues of security on networked devices are considered and go over the primary procedures and algorithms that make this technology safe. Because our reliance on the internet of things grows daily, it is important to think about how to improve security-related technologies and algorithms.

Keywords: Cryptography, Cyber Attacks, Internet of Things, Smart Cities, Security, Authentication, Access Control.

1. INTRODUCTION

Many nations are aiming to build smart cities in the near future. Modern technology is the backbone of a smart city, which aims to enhance sustainability, streamline urban services, and provide a better living environment for all [1]. Sensors, communication networks, and data analytics are just a few of the technological systems that it integrates to automate processes, collect and process data, and provide insights that help city officials make better decisions [2]. The goal of implementing technological solutions in urban areas is to create smart cities that are more efficient, environmentally friendly, and safe for residents and visitors alike. The Smart Cities Mission (SCM) has already recognised 100 cities in India as needing improvements to their basic infrastructure and services [3]; these will make the cities better places to live in terms of sustainability, economic diversity, and quality of life. Hardware platforms, communication technologies, and interfaces make up the intricate smart city application pipeline [4].

Interoperability, scalability, security, and resilience are crucial needs for smart city systems due to the use of multiple vendors' components. The proliferation of IoT-enabled apps is a direct result of the many benefits offered by the IoT [5]. Reading up on the IoT, its architecture, and the problems it could answer is a good idea. By automating processes, increasing resource usage, and improving supply chain management, the supply chain industry can save costs

through the use of the IoT [6]. Businesses can use the real-time data it gives to develop individualized consumer services. The IoT is crucial to the efficient management of smart cities. Many factors may be monitored and regulated with the use of IoT devices in smart city applications [7]. These include trash management, traffic management, energy management, air pollution monitoring, and more. Smart traffic control solutions that employ the IoT can alleviate traffic jams and make roads safer for everyone [8]. Energy savings and less light pollution are two additional benefits of smart lighting systems. By utilizing sensors and cameras, public areas can be kept vigilant for any signs of suspicious behavior or possible dangers [9].

It is vital and tough to incorporate security into smart cities in order to protect confidentiality, integrity, and availability [10]. In smart city applications, IoT devices can be low-cost sensors with limited processing power, memory, and battery life. Cost, deployment location, processing power, and security of IoT devices are often compromised in the sake of efficiency [11]. Another layer of difficulty emerges when users and producers put operational and functional needs ahead of security. Dangers like physical manipulation that causes side-channel assaults and man-in-the-middle attacks are a real possibility with these gadgets [12]. It is possible to violate someone's privacy by taking advantage of security holes in the communication network. The security of users and data might be compromised by APIs that are not up to scratch [13]. When it comes to smart cities in particular, all these concerns highlight how important it is to incorporate security. The correct security controls can only be put in place after extensive testing and evaluation of actual, large-scale smart city installations [14]. Examining node authentication methods, data secrecy, and the usage of secure Application Program Interfaces (APIs) are all part of the physical, network, and application layer security that are part of the security study.

Every day, more and more cyberattacks are being launched. Serious compromises of confidential data may result from this. Concerns about communication security have arisen in response to the exponential growth in the number of internet-connected gadgets [15]. Despite their seemingly innocuous nature, IoT devices have the potential to become mission-critical in the wrong hands. The sharing of passcodes between several devices is a known security vulnerability [16]. Device criticality, measured by their function or the degree to which people may rely on them, determines the nature and severity of the risks associated with them.

Accessibility, integrity, identity, availability, and confidentiality will all take a hit if devices are vulnerable to certain threats [17]. Having this final component on the device is crucial, and it becomes even more so when sending data over the Internet. Accessing the IoT devices through the internet is common, but privacy concerns arise when a third party obtains the passcode. It is important to prevent unauthorized individuals from remotely controlling equipment, as their malicious actions can compromise users' computer and physical security [18]. In most circumstances, a large-scale utilization of communication networks is required, as devices transmit data via the Internet. There is a high risk of compromise for all these communications that travel across public networks [19]. This research details the attacks and the cryptographic methods that stop them in their tracks. Promoting the value of the IoT and the security it offers to the connections established between devices at every stage of data transfer is the goal [20]. By 2020, a great number of gadgets will have internet connectivity, making it critical to reveal how to provide sufficient security on these devices.

From the moment a gadget is installed until the moment it is put into use, security must be a top priority. This means that credentials are required to provide safe access to IoT networks. In order to ensure safe and proper operation, it is essential that the devices have distinct protocols that must be validated [21]. There is a pressing need for security system patches that either lower bandwidth consumption or make attacks more difficult to launch in the event that credentials are stolen. This means that in order for a connected device to get data from another device, it must first identify itself, which can be a challenge for devices with low bandwidth and inconsistent networks [22]. Devices and networks must work together to ensure complete security; the same intelligence that powers them should also enable them to detect and ward off any dangers. An attacker can intercept data via a Man in the Middle attack by posing as the sender of the message and serving as a go-between for the two parties involved, all while being undetected [23]. Some devices employ stripped-down versions of operating systems, which helps keep software expenses down [24]. Because this compromises the security of the entrance doors, which in turn compromises the information transmitted by the devices, it suggests a security concern [25]. Traditional cryptography methods, such homomorphic encryption and preservation, employ expensive procedures that add 30% to processing time and rely on proxies, making them impractical for application in IoT electronic circuits. When dealing with a decent amount of data, it concentrates on partially homomorphic encryption, which offers a high degree of security. This research presents a brief survey on cryptography models that are used for cyber attack detection in IoT devices to enhance Quality of Service (QoS) levels. This research is helpful for the scholars to know the working process and limitations of traditional models so that novel methodologies can be designed that provides better security levels.

2. LITERATURE SURVEY

To ensure trustworthy and practical services in smart city settings, Yu et al. [1] developed SLAP-IoD, a lightweight and secure authentication protocol for the IoT that makes use of a Physical Unclonable Function (PUF). Liang et al. [2] presented PAFR-ABE, an access control scheme that uses attribute-based encryption (ABE) to safeguard EHRs from unauthorized decryption. It addresses the difficulties of user authentication and secret key revocation by offering a solution. At the same time, PAFR-ABE protects users' identities and stops illegal requests for secret keys by ensuring privacy-preserving authentication for users during secret key production. Also, secret key updates are unnecessary for users whose access has not been revoked because PAFR-ABE provides flexible key revocation and recovery.

The most significant dangers posed by devices linked remotely are the potential compromise of devices and the leakage of sensitive information. Algarniet al. [3] presented a relevant privacy-preserving approach that takes into account various security threats. In order to prevent the aforementioned security breaches, the offered technique is trustworthy for protecting sensitive geosensed data. There have been numerous recent proposals for methods to protect IoD settings; however, some of these have proven to be vulnerable, while others have reduced efficiency. Here, Hussain et al. [4] presented a novel authentication method for drone-user communication that makes use of elliptic curve encryption within a predetermined airspace. In addition to a concise overview of the security features offered by the proposed technique, the author requested that it be tested using the Random oracle approach.

Some of the problems with strong security in IoV that have been discussed in the literature so far include inefficient communication, security without privacy, security that isn't dependable, and long delays caused by security algorithms. In order to solve these problems, Safavat et al. [5] suggested a routing system called ACO-AODV that uses Elliptic Curve Cryptography (ECC) to prevent messages from being spread by suspicious vehicles in the IoV. One part of the proposed protocol uses ECC to map publicly available information like license plates to cryptographic keys; another part uses status message interactions to calculate a trust level; and finally, the third part uses ACO-AODV to secure optimal path selection adaptively based on communication intent, thereby avoiding malicious vehicles.

Liu et al. [6] introduced ECL-AKA, a smart grid technology that improves upon the original certificateless AKA protocol. This protocol's architecture and security model are first described in this article. Afterwards, the full ECL-AKA protocol workflow is presented. To guarantee security and privacy, the majority of the associated work used the Public Key Infrastructure and Certification Revocation Lists (CRLs). Nevertheless, there were a few problems with these efforts, including: 1) the lengthy verification procedure and the large size of CRLs; 2) traceability assaults through the linking of unencrypted Basic Safety Messages (BSMs); and 3) the possibility of an adversary obtaining secret keys from the storage of parked vehicles or RSU. In light of these concerns, Othman et al. [7] offered a physically safe system for authenticating messages that preserve privacy by utilizing PUF and Secret Sharing. Security and privacy are guaranteed by the proposed protocol, even in the face of memory leakage, against passive and aggressive attacks.

Sucasas et al. [8] introduced a new way to build a pseudonym system that doesn't rely on a trusted issuer. To avoid having to assume an honest CA, a group of Smart City service providers use secure multi-party computation (MPC) to mimic the CA. This model described in detail the system that combines an MPC protocol with a signature technique that uses pseudonyms. Verma et al. [9] presented a certificate-based data aggregation (CB-DA) approach that is both efficient and effective. The owner chooses a secret key in the proposed CB-DA method, and that key, together with certificates, is used as a decryption/signing key. Using the Random Oracle Model (ROM), the suggested protocol by Akramet al. [10] offered both official and informal security and is resistant to numerous well-known security vulnerabilities. Compared to other relevant protocols, the suggested protocol offers effective security features and outperforms security performance in terms of communication cost and running time cost.

Tanveer et al. [11] introduced RACP-SG, a new and powerful AC protocol. To complete the AC phase, RACP-SG makes use of elliptic curve encryption, a LWC-based AEAD method called ASCON, and the hash function called ASCON-hash. Additionally, RACP-SG allows for the establishment of a session key (SK) and mutual authentication between a service provider (SEP) and a smart meter (SM) during communication over the public communication channel. Dat et al. [12] break down many industrial IoT situations into their component parts and examined their requirements and logic in order to create a universal model. Using the conditional proxy re-encryption primitive as a foundation, the author outlined potential assaults on several industrial IoT systems and devised a security mechanism to detect and prevent them. Unauthorized users will not be able to access data with the proposed technique.

Pérez et al. [13] presented an encryption system that takes advantage of attribute-based encryption and the lightweight symmetric cryptography under these conditions. Protecting users' privacy without sacrificing scalability or efficiency is the proposal's primary goal in limiting data access to authorized services. The method that was created has been

tested on a real-life smart building situation, and the findings show that it can secure a lot of sensitive data on buildings that are connected to the internet.

Vinoth et al. [14]proposed a multifactor authenticated key agreement mechanism for IIoT, which would allow authorized users to remotely access sensing devices while also protecting transmitted data from hostile attacks. To authenticate users in an IIoT setting, the system makes use of passwords, biometrics, and smart cards. To facilitate the negotiation of a secure session key between the user and several sensing devices, the author used secret-sharing technology and the Chinese remainder theorem to build a group key among valid sensing devices.

Researchers still face challenges when deploying Flying Ad Hoc Networks (FANETs) to guarantee message integrity, non-repudiation, authenticity, and authorization for information transmission in these areas. Due to its dynamic topology changes, the FANET is more sophisticated and susceptible to adversaries' many attacks when it comes to drone technology. So far, in order to establish the utmost trust before launching a drone into an IoD environment, a regulated layered network architecture is required. This will ensure that only authorized drones can securely interact with one another and with the ground control station (GCS). An attacker can potentially capture data from an open network channel and utilize it for their own malicious purposes; even a little breach in security can have a significant impact on communication. In such a delicate setting, it is essential to use extreme caution while authenticating both identities and messages. To that end, Janet al. [15] developed an Elliptic Curve Cryptographic (ECC)–based authentication technique for the IoT that makes use of FANET and is thus verifiably safe.

Tanveer et al. [16] provided REAS-TMIS, a novel AKE scheme for telecare MIS that is both effective and efficient in terms of resources. It make use of a hash function and authenticated encryption with associative data (AEAD). IoT devices with limited resources can communicate securely using AEAD methods. Because of these AEAD qualities, REAS-TMIS is efficient with resources. As an added bonus, REAS-TMIS eliminates the computationally costly operations of elliptic curve point multiplication and chaotic map. Furthermore, after the user's identity has been validated, REAS-TMIS enables the session key (SK) establishment functionality, which allows for future encrypted communication between MS and users. Using the well-established random oracle model, the author confirmed that SK is secure. In addition, REAS-TMIS is demonstrated to be secure by the implementation of Scyther-based security corroboration, and its resilience against various security assaults is demonstrated through the execution of informal security analysis.

De Ree et al. [17] introduced the DECENT scheme, a decentralized and efficient key management system. In self-organizing, dense, and dynamic network environments, this technique offers secure multi-hop communication. Network nodes can cooperate to carry out critical management tasks by using threshold secret sharing mechanisms, which make them serve as a distributed trusted third party (TTP). First, DECENT has a special self-healing feature that allows it to recover from network compromise on its own. Second, there are rules for selecting a suitable security threshold for any deployment scenario that ensures decentralized key management services can be offered while maximizing security.

Luo et al. [18] suggested a communication protocol that reduces resource consumption by utilizing a symmetric key-based method. This system offered ultra-lightweight encryptions that are both effective and efficient in protecting data transmissions. To withstand key reset and device capture attempts, this protocol generates symmetric keys and delegated them using a chaotic system, the Logistic Map. To examine the protocol's security features, the author used a semantic model. In order to ensure runtime efficacy, the author additionally assessed the resource consumption.

In the realm of trade finance, there has been a great deal of interest in blockchain-based smart legal contracts due to their status as legally binding executable contracts. However, there is a privacy disclosure issue because all transaction data is publicly viewable when the contract is placed on an open and transparent blockchain network. Our solution to this issue is a revamped framework for privacy-protecting smart legal contracts that incorporates new steps for creating, deploying, and carrying out these contracts. The contract conditions declare and safeguard the sensitive transaction data in this design. The compiler can use these phrases to build executable code for smart contracts by linking them to specified cryptographic algorithms. Yin, et al. [19] build a new dual-mode identity-based broadcast encryption (DM-IBBE) scheme to suit specific-purpose or generic-purpose privacy by employing exclusive encryption mode or selective encryption mode, respectively, as established cryptographic algorithms. It was demonstrated that the DM-IBBE system satisfies the decisional Diffie-Hellman assumption for semantic security.

The advent of GPS-enabled IoT devices has revolutionized our lives by collecting the whereabouts and whenabouts of installed objects for the purpose of enhancing location-based services. Data privacy and security has been a hot topic recently, particularly in relation to outsourcing to third parties. The availability and confidentiality of data that is outsourced have been addressed through the proposal of multiple dynamic searchable symmetric encryption (DSSE) algorithms. Unfortunately, neither the security nor the efficiency of the current methods are up to par. Li et al. [20] presented SES-ESTD, a technique for secure and efficient search over encrypted spatiotemporal data, which uses enhanced asymmetric scalar-product preserving encryption and a limited pseudo-random function to overcome this

difficulty. High retrieval efficiency, forward security, and content privacy are all achieved by this scheme. Proof of forward security and content privacy is provided by a rigorous security study of SES-ESTD. Also, compared to other systems, SES-ESTD has lower compute and storage overheads, according to comprehensive studies. Crucially, compared to current forward secure spatiotemporal DSSE systems, SES-ESTD achieves retrieval speeds of milliseconds for millions of data points, which is 2.85 times quicker.

3. DISCUSSIONS

With the proliferation of Smart Cities and the widespread use of IoT, the integration of these technologies has emerged as an exciting new area, albeit one fraught with difficulties, chief among them security concerns [27]. Authentication is a major effort to fix these problems. Several advantages, such as a high data transfer rate and dependable communications even in the event of a central server failure, can be introduced by enabling direct device-to-device communications instead of solely device-to-service connections [28]. It is more challenging to design secure protocols that can offer a sustainable deployment in practice due to the resource limitation nature of IoT devices. This research provides a brief literature survey on security models using cryptography that provide authentication and access control with cyber attack detection in smart cities. This research analyzed numerous models and foundelliptic curve cryptosystem as the best cryptography model with better security levels and with less complex operations.

The elliptic curve cryptosystem was created in the nineteenth century by Victor Miller and Neil Kobiltz. This method is similar to public key cryptography like RSA. The difficulty of the Elliptic Curve Discrete Logarithm Problem determines the security strength of ECC. The computational efficiency of ECC is higher than that of RSA exponentiation because it uses scalar multiplication, which incorporates point doubling and adding operations. The attacker faces challenges in understanding and cracking the security key due to the complexity of ECC. Using only 160 bits of key length, ECC achieves the same level of security as RSA, which uses a 1024 bit key. The result is that it works great with devices that are limited in resources, such as mobile phones and smart cards.The algebraic structure of elliptic curves over finite fields is the foundation of ECC, a form of public-key encryption. Due to the reduced demand on hardware resources and memory for storage, as well as the associated reduced computational cost, a smaller key size is preferable. Furthermore, ECC is becoming more trusted by the cryptologist community as RSA questions get easier to solve with quantum computing. IoT devices typically have limited resources but need a high degree of security; thus, ECC Cryptography is a good fit for this setting.

Each and every system relies on authentication in some way. To safeguard them from potential threats, it is one of the security features. This procedure aids in ensuring that only authorized users are able to access a system. Numerous studies and research have focused on various IoT-specific solutions because this is such a crucial procedure. In reality, the point of proposing an authentication protocol is to offer a method for ensuring that only authorised objects can connect to and communicate with each other in a given system. Only then can we set up secure channels to allow objects to communicate without fear of identity theft. In addition to complex cryptographic techniques, there are alternative approaches that have been proposed for security. Another approach involves key-based management and rating-based authentication, which aims to avoid the high computational cost of cryptographic operations. To overcome the limitations of the traditional models and to design innovative and novel methods for improving the security levels, this research also provides suggestions to academicians and scholars to designa strong IoT node authentication model using Dual Key Authentication model using asymmetric cryptography model with strong access control mechanisms in smart city application, to implement a Node Behavior based cyber attacks detection model to avoid malicious actions in the IoT network for enhancing the security levels in smart cities using light weight cryptography model key distribution. An effective strong cryptography models using Enhanced Elliptic Curve Cryptography is also required for implementing secure data transmission in smart cities that performs secured encryption and decryption model. There is a need to design an efficient big data processing model for secured cloud storage with access control mechanism and attack detection model for enhancing the security levels. Finally, comparative analysis of proposed models with traditional models can be performed to prove that the proposed models performance levels are high.

4. CONCLUSION

A key factor in the rise of smart cities in the last several years has been the broad use of IoT applications. The IoT enables various technologies, communications, and applications in a smart city to improve the quality of life for its residents, as well as the efficiency and effectiveness of the city's service providers. However, cyberattacks and dangers are only going to become more common as smart city networks expand. Threats and attacks can reach the IoT devices in a smart city network through the sensors that connect them to huge cloud servers. As a result, methods to safeguard IoT devices from assaults like these must be developed. The IoT has quickly established itself as a crucial component of the Internet's future with its applications in smart homes, smart cities, and other areas. The IoT is unlike any technology that has come before it, and as a result, it poses new security challenges.

Once a device's control server approves it for system integration, the server will assist the device in authenticating with other devices. After both devices have successfully authenticated, they will be able to interact independently of their server. Information contained in embedded devices nowadays may be sensitive and should not be exposed because most of them have sensors to detect changes in the actual world. The integration of various forms of privacy protection into the authentication process offers opportunities to enhance protocol's security, particularly for IoT devices with limited resources. Given this, the question of what data can be transferred between devices once authentication is complete is an essential one that needs more research. This research is helpful for the scholars to know the working process and limitations of traditional models so that novel methodologies can be designed that provides better security levels. In future, hydrid cryptography models can be designed for the development of strong security models in smart cities.

REFERENCES

[1] S. Yu, A. K. Das, Y. Park and P. Lorenz, "SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments," in IEEE Transactions on Vehicular Technology, vol. 71, no. 10, pp. 10374-10388, Oct. 2022, doi: 10.1109/TVT.2022.3188769.

[2] X. Liang, Y. Liu and J. Ning, "An Access Control Scheme With Privacy-Preserving Authentication and Flexible Revocation for Smart Healthcare," in IEEE Journal of Biomedical and Health Informatics, vol. 28, no. 6, pp. 3269-3278, June 2024, doi: 10.1109/JBHI.2024.3391218.

[3] F. Algarni, M. A. Khan, W. Alawad and N. B. Halima, "P3S: Pertinent Privacy-Preserving Scheme for Remotely Sensed Environmental Data in Smart Cities," in IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 16, pp. 5905-5918, 2023, doi: 10.1109/JSTARS.2023.3288743.

[4] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan and N. Kumar, "Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones," in IEEE Systems Journal, vol. 15, no. 3, pp. 4431-4438, Sept. 2021, doi: 10.1109/JSYST.2021.3057047.

[5] S. Safavat and D. B. Rawat, "On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart Cities," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5050-5059, Aug. 2021, doi: 10.1109/TITS.2020.3008361.

[6] Z. Liu, C. Hu, C. Ruan, P. Hu, M. Han and J. Yu, "An Enhanced Authentication and Key Agreement Protocol for Smart Grid Communication," in IEEE Internet of Things Journal, vol. 11, no. 12, pp. 22413-22428, 15 June15, 2024, doi: 10.1109/JIOT.2024.3381379.

[7] W. Othman, M. Fuyou, K. Xue and A. Hawbani, "Physically Secure Lightweight and Privacy-Preserving Message Authentication Protocol for VANET in Smart City," in IEEE Transactions on Vehicular Technology, vol. 70, no. 12, pp. 12902-12917, Dec. 2021, doi: 10.1109/TVT.2021.3121449.

[8] V. Sucasas, A. Aly, G. Mantas, J. Rodriguez and N. Aaraj, "Secure Multi-Party Computation-Based Privacy-Preserving Authentication for Smart Cities," in IEEE Transactions on Cloud Computing, vol. 11, no. 4, pp. 3555-3572, Oct.-Dec. 2023, doi: 10.1109/TCC.2023.3294621.

[9] G. K. Verma, P. Gope, N. Saxena and N. Kumar, "CB-DA: Lightweight and Escrow-Free Certificate-Based Data Aggregation for Smart Grid," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 2011-2024, 1 May-June 2023, doi: 10.1109/TDSC.2022.3169952.

[10] M. W. Akram et al., "A Secure and Lightweight Drones-Access Protocol for Smart City Surveillance," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 10, pp. 19634-19643, Oct. 2022, doi: 10.1109/TITS.2021.3129913.

[11] M. Tanveer, A. U. Khan, N. Kumar, A. Naushad and S. A. Chaudhry, "A Robust Access Control Protocol for the Smart Grid Systems," in IEEE Internet of Things Journal, vol. 9, no. 9, pp. 6855-6865, 1 May1, 2022, doi: 10.1109/JIOT.2021.3113469.

[12] L. Fang, H. Zhang, M. Li, C. Ge, L. Liu and Z. Liu, "A Secure and Fine-Grained Scheme for Data Security in Industrial IoT Platforms for Smart City," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7982-7990, Sept. 2020, doi: 10.1109/JIOT.2020.2996664.

[13] S. Pérez et al., "A Lightweight and Flexible Encryption Scheme to Protect Sensitive Data in Smart Building Scenarios," in IEEE Access, vol. 6, pp. 11738-11750, 2018, doi: 10.1109/ACCESS.2018.2801383.

[14] R. Vinoth, L. J. Deborah, P. Vijayakumar and N. Kumar, "Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3801-3811, 1 March1, 2021, doi: 10.1109/JIOT.2020.3024703.

[15] S. U. Jan, I. A. Abbasi, F. Algarni and A. S. Khan, "A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET," in IEEE Access, vol. 10, pp. 95321-95343, 2022, doi: 10.1109/ACCESS.2022.3204271.

[16] M. Tanveer, A. U. Khan, A. Alkhayyat, S. A. Chaudhry, Y. B. Zikria and S. W. Kim, "REAS-TMIS: Resource-Efficient Authentication Scheme for Telecare Medical Information System," in IEEE Access, vol. 10, pp. 23008-23021, 2022, doi: 10.1109/ACCESS.2022.3153069.

[17] M. De Ree, G. Mantas, J. Rodriguez and I. E. Otung, "DECENT: Decentralized and Efficient Key Management to Secure Communication in Dense and Dynamic Environments," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 7, pp. 7586-7598, July 2023, doi: 10.1109/TITS.2022.3160068.

[18] X. Luo et al., "A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment," in IEEE Access, vol. 8, pp. 67192-67204, 2020, doi: 10.1109/ACCESS.2020.2978525.

[19] H. Yin, Y. Zhu, G. Guo and W. C. -C. Chu, "Privacy-Preserving Smart Contracts for Confidential Transactions Using Dual-Mode Broadcast Encryption," in IEEE Transactions on Reliability, vol. 73, no. 2, pp. 1090-1103, June 2024, doi: 10.1109/TR.2023.3328146.

[20] Z. Li, J. Ma, Y. Miao, X. Wang, J. Li and C. Xu, "Enabling Efficient Privacy-Preserving Spatiotemporal Location-Based Services for Smart Cities," in IEEE Internet of Things Journal, vol. 11, no. 3, pp. 5288-5300, 1 Feb.1, 2024, doi: 10.1109/JIOT.2023.3305605.

[21] V. L. Narayana, S. Bhargavi, D. Srilakshmi, V. S. Annapurna and D. M. Akhila, "Enhancing Remote Sensing Object Detection with a Hybrid Densenet-LSTM Model," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 264-269, doi: 10.1109/IC2PCT60090.2024.10486394.

[22] Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for prediction of covid-19. Traitement du Signal, Vol. 40, No. 4, pp. 1689-1696. https://doi.org/10.18280/ts.400437

[23] Lakshman Narayana, V., Lakshmi Patibandla, R.S.M., Pavani, V., Radhika, P. (2023). Optimized Nature-Inspired Computing Algorithms for Lung Disorder Detection. In: Raza, K. (eds) Nature-Inspired Intelligent Computing Techniques in Bioinformatics. Studies in Computational Intelligence, vol 1066. Springer, Singapore. https://doi.org/10.1007/978-981-19-6379-7_6.

[24] Lakshman Narayana, V., C.R. Bharathi. (2023). Efficient route discovery method in MANETs and packet loss reduction mechanisms. International Journal of Advanced Intelligence Paradigms, 2023 Vol.25 No.1/2. 10.1504/IJAIP.2023.130818.

[25] V. L. Narayana, S. Sirisha, G. Divya, N. L. S. Pooja and S. A. Nouf, "Mall Customer Segmentation Using Machine Learning," 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022, pp. 1280-1288, doi: 10.1109/ICEARS53579.2022.9752447.

[26] J. D. Michler, A. Josephson, T. Kilic and S. Murray, "Privacy protection measurement error and the integration of remote sensing and socioeconomic survey data", J. Develop. Econ., vol. 158, pp. 1-25, 2022.

[27] Konatam, S., Nalluri, S., Malyala, M. M., Daiya, H., Kumar, V. N., & Raju, K. S. (2024). A Random Forest-Based Method for Effective and Robust Detection of Wormhole Attacks in Wireless Sensor Networks. International Conference on Intelligent Computing and Communication, 461–476.

[28] Nalluri, S., Malyala, M. M., Kandagiri, H., & Kandagiri, K. K. (2025). Emission Minimization Through IoT-Integrated Intelligent Transportation System. In Urban Mobility and Challenges of Intelligent Transportation Systems (pp. 579–598). IGI Global Scientific Publishing.

[29] S. Jalayer, A. Sharifi, D. Abbasi-Moghadam, A. Tariq and S. Qin, "Modeling and predicting land use land cover spatiotemporal changes: A case study in Chalus Watershed Iran", IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens., vol. 15, pp. 5496-5513, 2022.

[30] S. Sodagari, "Trends for mobile IoT crowdsourcing privacy and security in the Big Data era", IEEE Trans. Technol. Soc., vol. 3, no. 3, pp. 199-225, Sep. 2022.

[31] F. Zhao et al., "Night-time light remote sensing mapping: Construction and analysis of ethnic minority development index", Remote Sens., vol. 13, no. 11, 2021.

[32] Q. Luo, D. Yu, Y. Zheng, H. Sheng and X. Cheng, "Core-GAE: Toward generation of IoT networks", IEEE Internet Things J., vol. 9, no. 12, pp. 9241-9248, Jun. 2022.

[33] J. Li et al., "Delayed packing attack and countermeasure against transaction information based applications", Inf. Sci., vol. 652, Jan. 2024.

[34] M. H. Ullah and J.-D. Park, "Distributed energy trading in smart grid over directed communication network", IEEE Trans. Smart Grid, vol. 12, no. 4, pp. 3669-3672, Jul. 2021.

[35] Y. Su, Y. Li, J. Li and K. Zhang, "LCEDA: Lightweight and communication-efficient data aggregation scheme for smart grid", IEEE Internet Things J., vol. 8, no. 20, pp. 15639-15648, Oct. 2021.

[36] Q. Yang, R. Lu, C. Rong, Y. Challal, M. Laurent and S. Wang, "Guest editorial the convergence of blockchain and IoT: Opportunities challenges and solutions", IEEE Internet Things J., vol. 6, no. 3, pp. 4556-4560, Jun. 2019.

[37] H. M. S. Badar, S. Qadri, S. Shamshad, M. F. Ayub, K. Mahmood and N. Kumar, "An identity based authentication protocol for smart grid environment

using physical uncloneable function", IEEE Trans. Smart Grid, vol. 12, no. 5, pp. 4426-4434, Sep. 2021.

[38] J. Wang, L. Wu, K.-K. R. Choo and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure", IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 1984-1992, Mar. 2020.

[39] P. Mall, R. Amin, A. K. Das, M. T. Leung and K.-K. R. Choo, "PUF-based authentication and key agreement protocols for IoT WSNs and smart grids: A comprehensive survey", IEEE Internet Things J., vol. 9, no. 11, pp. 8205-8228, Jun. 2022.

[40] S. Hu et al., "Provably secure ECC-based authentication and key agreement scheme for advanced metering infrastructure in the smart grid", IEEE Trans. Ind. Informat., vol. 19, no. 4, pp. 5985-5994, Apr. 2023.