JSL, 8(1), Jan 2023: 01-09

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

JOURNAL OF SCIENTIFIC LETTERS
www.jslsci.com

LIGHTWEIGHT ECC-BASED SECURITY AND AI-ENABLED INTRUSION DETECTION FOR RESOURCE-CONSTRAINED SENSOR–CLOUD NETWORKS

Kapila Purohit

Research Scholar, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan

Dr. Sushma Agarwal

Research Supervisor, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan

ABSTRACT

The rapid integration of Internet of Things (IoT) sensors with cloud computing has created efficient platforms for real-time data collection, storage, and intelligent processing. However, resource-constrained sensor devices remain vulnerable to unauthorized access, data interception, impersonation, denial-of-service attacks, and other cyber threats. Conventional cryptographic mechanisms may impose considerable computational, memory, and energy overhead on such devices. This paper proposes a conceptual lightweight security framework that combines Elliptic Curve Cryptography (ECC) with Artificial Intelligence (AI)-enabled intrusion detection for sensor–cloud networks. ECC is employed to provide secure key establishment, authentication, and confidentiality while reducing computational and communication overhead compared with conventional public-key approaches. An AI-based intrusion detection layer is incorporated to identify abnormal traffic patterns and potential attacks using network and behavioral characteristics. The proposed approach establishes a complementary relationship between cryptographic protection and intelligent threat detection. The framework is designed to improve security, energy efficiency, scalability, and communication reliability in heterogeneous sensor–cloud environments.

Keywords: Elliptic Curve Cryptography, Artificial Intelligence, Intrusion Detection, Sensor Networks, Cloud Computing, IoT Security, Lightweight Security, Threat Detection.

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

I. INTRODUCTION

The rapid growth of Internet of Things (IoT) technologies has resulted in the deployment of large numbers of interconnected sensors in healthcare, smart cities, agriculture, industrial automation, transportation, environmental monitoring, and critical infrastructure. These sensors continuously generate information that can be transmitted to cloud platforms for storage, analysis, and decision-making. Sensor–cloud networks therefore provide an effective architecture in which resource-constrained sensing devices can utilize the computational and storage capabilities of remote cloud infrastructures. However, the distributed and heterogeneous nature of these networks introduces significant security challenges. Sensor nodes generally possess limited processing capacity, memory, battery power, and communication bandwidth, making them more difficult to protect using computationally intensive security mechanisms. At the same time, communication channels between sensors, gateways, and cloud servers can be targeted by attackers seeking to compromise confidentiality, integrity, availability, or authenticity.

Traditional security mechanisms frequently rely on conventional public-key cryptography, symmetric encryption, authentication protocols, and centralized intrusion detection systems. Although these approaches can provide substantial protection, their computational and communication requirements may not be appropriate for highly constrained sensor devices. Elliptic Curve Cryptography (ECC) provides an attractive alternative because it can offer strong security with relatively small key sizes. Smaller keys can reduce storage requirements, communication overhead, and computational costs, making ECC particularly suitable for IoT and sensor-oriented environments. ECC can support authentication, digital signatures, and secure key establishment while maintaining an appropriate balance between security and resource utilization. Nevertheless, cryptographic mechanisms primarily protect communications and identities; they cannot independently determine whether legitimate credentials are being used maliciously or whether unusual network behavior represents an emerging attack.

Artificial Intelligence (AI) and machine-learning-based intrusion detection can complement cryptographic protection by analyzing communication patterns and identifying deviations from normal network behavior. AI-enabled intrusion detection systems can examine characteristics such as packet rates, connection frequency, protocol behavior, traffic volume, failed authentication attempts, and node activity. Supervised, unsupervised, and hybrid

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

learning approaches can potentially identify attacks such as denial-of-service, flooding, probing, spoofing, and anomalous behavior. Combining ECC with AI therefore creates a multilayer security architecture in which cryptography protects information and identities while intelligent analytics provide behavioral security.

The objective of this study is to develop a conceptual lightweight security framework for resource-constrained sensor–cloud networks by integrating ECC-based cryptographic mechanisms with AI-enabled intrusion detection. The proposed framework emphasizes security, computational efficiency, energy conservation, communication overhead, scalability, and timely threat identification. Rather than treating cryptographic protection and intrusion detection as independent mechanisms, the framework considers them complementary components of an integrated security architecture. Such an approach can support secure communication while enabling intelligent monitoring of potentially malicious activities across sensor, gateway, and cloud layers.

II. ECC-BASED LIGHTWEIGHT SECURITY ARCHITECTURE FOR SENSOR–CLOUD NETWORKS

Resource limitations represent one of the most important considerations in designing security mechanisms for sensor–cloud networks. Sensor nodes may operate using small batteries and low-power processors while communicating through wireless channels that are exposed to interception and manipulation. A security mechanism that requires excessive computation or frequent transmission of large cryptographic keys can significantly reduce network lifetime. ECC provides an effective foundation for lightweight public-key security because its security can be achieved using comparatively smaller key sizes. This characteristic can reduce the amount of memory required for cryptographic parameters and decrease the communication overhead associated with key exchange and authentication. Consequently, ECC can be positioned at the sensor and gateway layers to establish authenticated and confidential communication with cloud services.

The proposed architecture can be organized into four principal layers: the sensor layer, gateway or edge layer, cloud layer, and intelligent security layer. The sensor layer consists of constrained devices responsible for collecting environmental or application-specific information. Each sensor is assigned an ECC-based identity and cryptographic credentials during secure initialization. When a sensor attempts to communicate with a gateway, an

E-mail: editor.jslsci888@gmail.com

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

authentication procedure verifies the legitimacy of the participating entities. ECC-based key establishment can then be used to derive a shared session key. Symmetric encryption may subsequently be used for bulk data transmission because symmetric algorithms generally require fewer computational resources than public-key operations. This hybrid arrangement allows ECC to perform computationally heavier operations only where necessary, while efficient symmetric encryption protects continuous data streams.

The gateway or edge layer can serve as an intermediary between constrained sensors and cloud infrastructure. This layer is particularly important because it can perform computationally demanding security functions that would otherwise consume significant sensor resources. The gateway can authenticate sensor nodes, manage session keys, aggregate data, perform preliminary security checks, and forward validated information to the cloud. ECC-based digital signatures or authentication codes can be employed to establish trust between devices and gateways. Secure key renewal mechanisms can further limit the consequences of key compromise. By shifting selected security operations toward the gateway, the proposed architecture reduces the computational burden imposed on individual sensor nodes while maintaining end-to-end security objectives.

At the cloud layer, authenticated sensor data can be stored and processed using scalable computing resources. Cloud servers can maintain security logs, authentication histories, device profiles, and network-level monitoring information. However, the cloud should not be treated as inherently trustworthy. Secure communication between the gateway and cloud should therefore use authenticated cryptographic channels. Data integrity mechanisms can detect unauthorized modification during transmission, while encryption can reduce the risk of disclosure. Access-control policies can determine which applications or cloud services are authorized to access specific categories of sensor information. The architecture can additionally incorporate secure logging so that security-related events can be traced and analyzed.

The principal advantage of the proposed ECC-based architecture is its emphasis on balancing security with resource consumption. Performance evaluation should consider metrics such as encryption and authentication time, energy consumption, memory requirements, communication overhead, packet-processing delay, and successful authentication rate. A useful design objective is to minimize resource consumption while satisfying predefined security requirements. ECC does not eliminate computational costs; scalar multiplication and

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

other elliptic-curve operations still require processing resources. Therefore, implementation choices, curve selection, hardware acceleration, key management, and protocol optimization remain important. Lightweight implementations should also minimize unnecessary cryptographic operations and avoid repeated authentication exchanges where secure session continuity can be maintained.

The ECC layer alone, however, cannot identify every form of malicious behavior. An attacker may obtain legitimate credentials, compromise a vulnerable node, generate abnormal traffic using an authenticated identity, or exploit application-level weaknesses. For this reason, the proposed framework integrates behavioral monitoring with cryptographic protection. Security events generated during authentication and communication can be supplied to an intelligent analysis module. The combination enables the system to determine not only whether a communication participant is cryptographically legitimate but also whether its behavior is consistent with expected network patterns. This layered approach can improve resilience against both conventional communication attacks and sophisticated behavioral threats while preserving the lightweight characteristics required by resource-constrained networks.

III. AI-ENABLED INTRUSION DETECTION AND INTELLIGENT THREAT ANALYSIS

AI-enabled intrusion detection provides the behavioral security component of the proposed sensor–cloud framework. Traditional rule-based intrusion detection systems generally depend on predefined signatures or manually constructed rules. Such systems can be effective against previously recognized attacks but may struggle to detect new or modified attack patterns. Machine-learning techniques provide an alternative by learning relationships between network characteristics and security events. In a sensor–cloud environment, relevant features may include packet frequency, packet size, communication duration, protocol type, source and destination behavior, authentication failures, retransmission rates, connection patterns, and changes in node activity. These characteristics can be analyzed to establish a behavioral profile for normal network operation.

The proposed AI module can employ a layered detection strategy. At the sensor or gateway level, lightweight anomaly indicators can identify unusual behavior without requiring extensive computation. More complex analysis can be transferred to the edge or cloud

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

environment. Supervised learning algorithms can be trained using labeled datasets containing normal and malicious traffic, enabling classification of known attack categories. Algorithms such as decision trees, random forests, support vector machines, and neural networks can be considered depending on the computational environment and required accuracy. When labeled attack data are limited, unsupervised or semi-supervised approaches can identify deviations from established normal behavior. This is particularly valuable for detecting previously unseen or evolving attacks.

A significant challenge in AI-based intrusion detection is the resource requirement associated with model training and inference. Large deep-learning models may achieve strong classification performance but can be unsuitable for constrained sensor devices. Therefore, the proposed architecture can separate model training from lightweight inference. Training can be conducted in the cloud using extensive historical datasets, while optimized models can be deployed at gateways or edge devices for rapid detection. Feature selection and model compression can further reduce inference requirements. The system can also adopt periodic model updates so that detection capabilities evolve as new attack patterns emerge. Such an arrangement creates a balance between the computational resources available in the cloud and the low-latency requirements of edge security.

The AI component should interact with the ECC security layer rather than operating independently. For example, repeated authentication failures, unusual key-establishment requests, sudden changes in packet transmission, and unexpected communication with unknown destinations can become features for the intrusion detection model. If the AI system detects a high-risk anomaly, the gateway can temporarily restrict the affected node, increase authentication requirements, terminate suspicious sessions, or alert the cloud security administrator. Cryptographic events can therefore provide valuable contextual information for behavioral analysis. Conversely, the intrusion detection system can assist cryptographic management by identifying nodes whose credentials may have been compromised. This interaction creates a dynamic security mechanism that combines identity-based protection with behavior-based detection.

Performance evaluation of the proposed AI-enabled security mechanism should consider detection accuracy, precision, recall, F1-score, false-positive rate, false-negative rate, detection latency, and computational overhead. High accuracy alone is insufficient because excessive false alarms can overwhelm administrators and consume network resources.

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

Similarly, a low false-positive rate is not useful if the system fails to identify serious attacks. Therefore, evaluation should consider a balanced set of security and performance metrics. The framework can be tested against representative threats such as denial-of-service, distributed denial-of-service, packet injection, spoofing, selective forwarding, probing, and compromised-node behavior. Comparative analysis with conventional rule-based intrusion detection and non-ECC security mechanisms can demonstrate the benefits of the integrated architecture.

Privacy is another important consideration in AI-enabled monitoring. Network traffic used for model development may contain sensitive information about users, devices, locations, or operational processes. Centralizing all security data in the cloud may create additional privacy risks. Privacy-preserving learning mechanisms, secure aggregation, anonymization, and federated learning can therefore be incorporated into future versions of the architecture. Federated learning, for example, can allow participating gateways to train local models and share model updates rather than transferring all raw traffic data to a central server. Combining such approaches with ECC-based authentication can provide stronger protection for both communication and learning processes. The resulting framework can support a more adaptive security environment in which cryptographic protection, intelligent detection, and privacy preservation operate together.

IV. CONCLUSION

The increasing deployment of sensor–cloud networks has created significant opportunities for intelligent monitoring, automation, and data-driven services, but it has simultaneously expanded the attack surface of resource-constrained devices. Conventional security mechanisms may impose substantial computational, memory, and communication requirements on sensor nodes. This study proposed a lightweight security framework based on the integration of Elliptic Curve Cryptography and AI-enabled intrusion detection to address these challenges. ECC provides a suitable foundation for authentication, key establishment, digital signatures, and secure communication because it can provide strong public-key security using relatively compact cryptographic parameters.

The proposed architecture distributes security responsibilities across sensors, gateways, cloud infrastructure, and intelligent security modules. Sensor devices can perform lightweight cryptographic operations, while gateways can undertake more demanding authentication,

E-mail: ***editor.jslsci888@gmail.com***

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

monitoring, and security-management tasks. Symmetric encryption can be combined with ECC to protect continuous data transmission efficiently. Secure communication, key management, access control, and integrity verification collectively contribute to improving the resilience of sensor–cloud communication against interception, impersonation, and unauthorized modification.

AI-enabled intrusion detection complements ECC by addressing threats that cannot be identified through cryptographic authentication alone. Machine-learning models can analyze traffic characteristics, authentication events, and behavioral patterns to identify anomalies and potential attacks. Cloud-based model training combined with lightweight edge inference provides a practical approach for resource-constrained environments. The framework can also be extended with privacy-preserving learning, federated learning, and adaptive model updating to address emerging security and privacy requirements.

Future research should validate the proposed framework through real-world sensor deployments and comprehensive simulation experiments. Comparative evaluations should examine energy consumption, computational overhead, communication latency, detection accuracy, false-positive rate, scalability, and resilience against multiple attack types. Further investigation is also required into optimized ECC implementations, lightweight AI models, adaptive key management, and privacy-preserving machine learning. Overall, the integration of lightweight ECC with intelligent intrusion detection offers a promising direction for developing secure, efficient, scalable, and adaptive sensor–cloud networks.

V. REFERENCES

N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

V. S. Miller, “Use of elliptic curves in cryptography,” in *Advances in Cryptology—CRYPTO ’85 Proceedings*, Springer, 1986, pp. 417–426.

D. J. Bernstein, “Curve25519: New Diffie-Hellman speed records,” in *Public Key Cryptography—PKC 2006*, Springer, 2006, pp. 207–228.

R. H. Weber, “Internet of Things—New security and privacy challenges,” *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

Online ISSN: 2456-1495
CODEN (USA): JSLOBJ

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

M. Abomhara and G. M. Køien, "Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015.

N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in *2015 Military Communications and Information Systems Conference*, IEEE, 2015, pp. 1–6.

R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

A. A. Diro and N. Chilamkurti, "Leveraging LSTM networks for cybersecurity in IoT," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1742–1754, 2022.